FRAUD EXAMINERS MANUAL

1. Big Picture Summary

The **Fraud Examiners Manual** is the **core body of knowledge** for the CFE exam. It explains **what fraud is, why it happens, how it is committed, how it is detected, how it is investigated, and how it is prevented**.

The unifying theme across all sections is this:

Fraud is intentional, patterned behavior that occurs when pressure, opportunity, and rationalization converge—and it leaves identifiable financial, behavioral, and control-based traces.

Every topic in the Manual ultimately trains you to **think like a fraud examiner**, not just memorize schemes.

---

2. Must-Know Points (HIGH PRIORITY)

These are **non-negotiable knowledge areas** for the CFE exam:

- Fraud is **intentional misrepresentation or misuse**, not error.
- The **Fraud Tree** classifies occupational fraud into:
    - Asset Misappropriation
    - Corruption
    - Financial Statement Fraud
- The **Fraud Triangle** explains *why* fraud occurs:
    - Pressure
    - Opportunity
    - Rationalization
- **Financial statement fraud is the least common but most costly**.
- **Asset misappropriation is the most common but least costly**.
- **Management override** is central to many major frauds.
- Revenue recognition, estimates, and timing are **high-risk fraud areas**.
- **Cash flow does not lie**—profits without cash are a major red flag.
- Fraud examination follows a **structured methodology**; it is not a witch hunt.
- **Prevention is cheaper and more effective than detection**.

---

3. Key Concepts and Explanations

A. Occupational Fraud & the Fraud Tree

Definition (Core):
Occupational fraud is the use of one's job for personal enrichment through the deliberate misuse of an employer's assets or resources.

Three Major Categories (Fraud Tree):

1. **Asset Misappropriation** – stealing or misusing assets
2. **Corruption** – abuse of power for personal gain
3. **Financial Statement Fraud** – intentional misstatement of financial reports

Why this matters:
Most exam questions test your ability to **classify scenarios accurately**, not recall long lists.

B. Fraud Triangle (Cressey)

Fraud almost always requires **all three elements**:

1. **Pressure**
    - Financial problems
    - Unrealistic performance targets
    - Personal or family stress
2. **Opportunity**
    - Weak internal controls
    - Management override
    - Poor oversight
3. **Rationalization**
    - "I'm just borrowing"
    - "I deserve this"
    - "Everyone does it"

Why this matters:

- Removing **any one** reduces fraud risk.
- Frequently tested in **scenario-based questions**.

C. Accounting Concepts (Foundation of Fraud)

Fraud examiners must understand how transactions flow through records.

Core Equation:

Assets = Liabilities + Equity

Because accounting uses **double-entry**, fraud **always affects at least two accounts**.

Accrual vs Cash Accounting

- GAAP/IFRS require **accrual accounting**
- Fraud often exploits **timing differences**

Financial Statements

- Income statement shows performance
- Balance sheet shows position
- **Cash flow statement shows reality**

Critical Insight:

Sustained profits with weak operating cash flows = **red flag**

D. Financial Statement Fraud (MOST TESTED)

Definition:
Intentional misstatement or omission in financial statements to deceive users.

Who commits it:

- Senior management (CEO, CFO)
- Those with override authority

Direction of manipulation:

- Usually overstate assets/revenue
- Understate expenses/liabilities
- Sometimes reversed (e.g., tax fraud)

Five Core Financial Statement Fraud Schemes (HIGH PRIORITY)

1. **Fictitious Revenues**
    - Recording sales that never occurred
    - Often offset by fake or uncollectible A/R
2. **Timing Differences (Income Smoothing)**
    - Recording revenue too early
    - Deferring expenses improperly

3. **Improper Asset Valuation**
    - Inventory inflation
    - Overstated receivables
    - Inflated fixed assets or goodwill
4. **Concealed Liabilities & Expenses**
    - Omitting obligations
    - Capitalizing expenses improperly
5. **Improper Disclosures**
    - Hiding related-party transactions
    - Side agreements not disclosed

Why this matters:
Most major scandals involve **multiple schemes simultaneously**.

E. Asset Misappropriation

Most common fraud category

Cash Schemes

- **Skimming** – cash stolen before recording
- **Cash larceny** – cash stolen after recording

Disbursement Schemes

- Billing fraud
- Payroll fraud (ghost employees)
- Expense reimbursement fraud
- Check and electronic payment tampering

Key control theme:

Separation of duties

F. Corruption

Includes:

- Bribery
- Kickbacks

- Illegal gratuities
- Economic extortion
- Conflicts of interest

Key challenge:
Corruption often benefits **both sides**, making detection harder.

G. Identity Theft, Cyberfraud, and Data Theft

Core ideas:

- Fraud increasingly exploits **technology and human behavior**
- Insider threats are as dangerous as external hackers

Patterns:

- Phishing, vishing, smishing
- Account takeovers
- Malware and ransomware

H. Fraud Examination & Investigation

Fraud Examination Is Not an Audit

Typical stages:

1. Predication
2. Planning
3. Evidence collection
4. Interviews
5. Reporting

Evidence Types

- Documentary
- Testimonial
- Physical

Key principle:

Preserve evidence integrity (chain of custody).

I. Fraud Prevention & Deterrence

Focuses on **reducing opportunity and rationalization**.

Key tools:

- Fraud risk assessments
- Corporate governance
- Codes of ethics
- Tone at the top
- Ongoing monitoring and analytics

Important distinction:
Fraud prevention is proactive; audits are largely reactive.

---

4. Important Terms and Definitions

- **Occupational Fraud** – job-related fraud against employer
- **Fraud Triangle** – pressure, opportunity, rationalization
- **Fraud Tree** – classification system
- **Skimming vs Cash Larceny** – before vs after recording
- **Channel Stuffing** – pushing excess inventory to inflate revenue
- **Income Smoothing** – shifting profits between periods
- **Management Override** – circumvention of controls
- **Predication** – reasonable basis to investigate
- **Chain of Custody** – documented control of evidence

---

5. Comparisons and Distinctions

Skimming vs Cash Larceny

- Skimming: before recording
- Larceny: after recording

Audit vs Fraud Examination

- Audit: reasonable assurance
- Fraud exam: proof of wrongdoing

Asset Misappropriation vs Financial Statement Fraud

- AM: common, smaller losses
- FSF: rare, catastrophic losses

Error vs Fraud

- Error: unintentional
- Fraud: intentional

---

6. Memory Hooks

- **Fraud Triangle = P-O-R**
- **FSF = 5 Schemes**: FIT-CI
  (Fictitious, Improper timing, asset Valuation, Concealed liabilities, Improper disclosure)
- **Cash rule**: Profit without cash = suspect
- **Controls mantra**: Separate, Rotate, Supervise

---

7. Likely Exam / High-Yield Points

If this shows up on the exam, remember:

- Fraud ≠ mistake
- Management is often the perpetrator
- Fraud usually spans **multiple periods**
- Most schemes leave **accounting inconsistencies**
- Prevention is often **control-based, not detective**

Common traps:

- Assuming auditors guarantee fraud detection
- Treating rationalization as observable evidence
- Ignoring cash flows

---

8. Quick Recall Sheet (Last-Minute Review)

- Fraud is **intentional**
- Three fraud types: AM, Corruption, FSF
- Fraud Triangle: Pressure + Opportunity + Rationalization
- FSF = least common, most costly

- Five FSF schemes
- Cash flow is key
- Controls fail → opportunity rises
- Prevention beats detection

OPTIONAL ENHANCEMENTS

Recall Questions

1. Why is financial statement fraud often long-lasting?
2. How does skimming differ from cash larceny?
3. Why are estimates high-risk fraud areas?
4. How does management override weaken controls?
5. Why is rationalization hard to observe?

Flashcards (Sample)

- **Q:** What makes fraud different from error?
  A: Intentional deception
- **Q:** Most common fraud?
  A: Asset misappropriation
- **Q:** Most costly fraud?
  A: Financial statement fraud
- **Q:** Key cash flow red flag?
  A: Profits without operating cash
- **Q:** Purpose of fraud risk assessment?
  A: Identify and reduce fraud risk proactively

1-Minute Review

Fraud is intentional misuse or misstatement. It occurs when pressure, opportunity, and rationalization align. Most fraud is asset misappropriation, but financial statement fraud causes the greatest damage. Accounting knowledge, control awareness, and examiner judgment are essential.

5-Minute Review

Focus on the Fraud Tree, Fraud Triangle, five financial statement fraud schemes, cash flow analysis, separation of duties, management override, and fraud examination methodology. Always think in patterns, not isolated acts.

Financial Statement Fraud & Asset Misappropriation (Cash Receipts & Disbursements)

---

1. Big Picture Summary

This material explains **how financial statement fraud and cash-based asset misappropriation are committed, concealed, detected, and prevented**.

The unifying idea is:

Fraud succeeds not because transactions are complex, but because controls fail, entries are manipulated, and omissions leave no immediate trail.

The chapter trains you to:

- Recognize **patterns**, not isolated errors
- Follow **money flows and timing differences**
- Detect **what is missing**, not just what is misstated

---

2. Must-Know Points (HIGH PRIORITY)

- **Concealed liabilities and expenses** are one of the *easiest* financial statement frauds to commit.
- **Omissions are harder to detect** than misstatements because they leave **no audit trail**.
- Improper capitalization **inflates current income** but depresses future income.
- **Cash flow analysis is critical** — profits without operating cash = red flag.
- Financial statement fraud often involves:
    - Management override
    - Subjective estimates
    - Related-party transactions
- **Skimming vs cash larceny** depends entirely on *when* cash is stolen.
- **Skimming is off-book** → harder to detect.
- **Cash larceny is on-book** → leaves an audit trail.
- **Ratio analysis** is a screening tool, not proof.
- **Prevention focuses on pressure, opportunity, rationalization** (Fraud Triangle).

---

3. Key Concepts and Explanations

A. Concealed Liabilities and Expenses (Financial Statement Fraud)

Definition:
Understating liabilities or expenses to artificially inflate profits.

Why it matters:
Every peso (or dollar) of omitted expense increases **pretax income by the same amount**.

Common Methods (HIGH PRIORITY)

1. **Omitting liabilities or expenses**
    - Vendor invoices ignored
    - Judgments or legal claims not recorded
    - Debits postponed to future periods
2. **Improper capitalization**
    - Costs expensed vs capitalized based on management intent
    - Shifts expenses from current period → future periods
3. **Undisclosed warranty & return liabilities**
    - Failure to accrue predictable costs
    - Different GAAP vs IAS treatment but same fraud logic

Key Insight

Missing transactions are harder to detect than wrong ones because nothing points to their absence.

Detection Techniques

- Review **post-balance-sheet transactions**
- Analyze **accounts payable movements**
- Examine **expense trends**
- Perform **physical searches** for unposted invoices
- Conduct **targeted interviews**

B. Improper Capitalization vs Improper Expensing

Capitalization Rule:

- Costs that **extend useful life or increase value** → capitalize
- Ordinary repairs → expense immediately

Fraud Effect:

- Capitalizing expenses → **overstates assets & income**
- Expensing capital items → **understates income (often tax-motivated)**

C. Improper Disclosures

Financial statements must include **all material information needed to avoid misleading users**.

Common disclosure fraud areas:

- Contingent liabilities
- Subsequent events
- Related-party transactions
- Management fraud
- Accounting changes

Failure type:

- Non-disclosure
- Misleading disclosure
- Incomplete footnotes

D. Red Flags of Financial Statement Fraud (EXAM FAVORITE)

HIGH-YIELD RED FLAGS

- Profit growth without cash flow
- Management domination
- Aggressive estimates
- Unusual margin improvement
- Shrinking reserves
- Rapid growth vs peers
- Complex or unusual transactions near period-end
- Related-party transactions not fully disclosed

---

4. Important Terms and Definitions

- **Concealed liabilities** – obligations omitted from records

- **Improper capitalization** – recording expenses as assets
- **Contingent liability** – obligation dependent on future events
- **Skimming** – theft before recording
- **Cash larceny** – theft after recording
- **Lapping** – using one receipt to cover another
- **Fraud risk factor** – condition increasing likelihood of fraud
- **Vertical analysis** – common-size statements
- **Horizontal analysis** – period-over-period change
- **Ratio analysis** – relationship between accounts

---

5. Comparisons and Distinctions

Skimming vs Cash Larceny

Skimming	Cash Larceny
Before recording	After recording
No audit trail	Audit trail exists
Harder to detect	Easier to detect

Capitalizing vs Expensing

Capitalize	Expense
Delays cost recognition	Immediate cost
Inflates current profit	Reduces income now

Omission vs Misstatement

Omission	Misstatement
Harder to detect	Easier to test
Leaves no trail	Leaves evidence

---

6. Memory Hooks

- **CLE** – Concealed Liabilities = *Criminally Lazy Easiest*
- **Before = Skimming / After = Larceny**
- **CAP it now → PAY later** (capitalization timing)
- **Cash > Profit** (cash tells truth)
- **VHR** (Vertical, Horizontal, Ratios)

---

7. Likely Exam / High-Yield Points

If tested, remember:

- Concealed liabilities increase income **1:1**
- Omitted items are **fraud even if recorded later**
- Skimming = off-book
- Lapping requires **control over posting**
- Ratio analysis **indicates**, not proves
- Fraudsters rely on:
    - Trust
    - Poor separation of duties
    - Override authority

Common traps

- Assuming auditors guarantee detection
- Focusing only on overstated expenses
- Ignoring timing and omissions
- Treating ratios as conclusive evidence

---

8. Quick Recall Sheet (Last-Minute)

- Fraud = intentional
- Missing liabilities → higher profits
- Capitalize wrongly → inflate income
- Skimming = before records
- Larceny = after records
- Ratios = red flags, not proof

- Cash flow exposes lies
- Controls fail → fraud thrives

OPTIONAL ENHANCEMENTS

Recall Questions

1. Why are omissions harder to detect than false entries?
2. How does improper capitalization affect future earnings?
3. Why is skimming considered off-book fraud?
4. When does lapping become impossible?
5. Why is cash flow analysis critical?

Flashcards

- **Q:** Skimming occurs when?
  A: Before recording
- **Q:** Best indicator of concealed liabilities?
  A: Negative operating cash flows
- **Q:** Improper disclosures usually involve?
  A: Contingencies, events, related parties
- **Q:** Ratio analysis limitation?
  A: Misses immaterial frauds
- **Q:** Most effective fraud deterrent?
  A: Strong internal controls + tone at top

1-Minute Review

Financial statement fraud thrives on omissions, timing tricks, and weak disclosure. Skimming occurs before cash hits the books; larceny after. Ratios point you where to look—cash tells you where to dig.

5-Minute Review

Focus on concealed liabilities, capitalization abuse, skimming vs larceny, lapping mechanics, ratio anomalies, and management override. Always analyze cash flows and timing differences first.

Financial Statement Fraud & Asset Misappropriation (Cash Receipts & Disbursements)

---

1. Big Picture Summary

This document explains **how fraudsters manipulate financial statements and steal cash**, **how those schemes are concealed**, **how fraud examiners detect them**, and **how organizations prevent them**.

The unifying theme is:

Fraud does not succeed because accounting is complex—it succeeds because controls break down, trust is abused, and transactions are intentionally omitted, altered, or misclassified.

The material trains you to think like a **fraud examiner**, not an accountant:

- Follow **timing**, **cash**, and **relationships**
- Look for **what is missing**, not just what is wrong
- Understand **why concealment techniques evolve**

---

2. Must-Know Points (HIGH PRIORITY)

- **Concealed liabilities and expenses** are one of the **easiest and most dangerous** financial statement frauds.
- **Omissions are harder to detect than misstatements** because they leave **no audit trail**.
- Improper capitalization **inflates current income** but **depresses future income**.
- **Negative operating cash flow with reported profits is a major red flag**.
- Financial statement fraud almost always involves **management override**.
- **Skimming vs cash larceny depends entirely on timing** (before vs after recording).
- **Skimming = off-book fraud** (harder to detect).
- **Cash larceny = on-book fraud** (audit trail exists).
- **Lapping is a concealment technique**, not a primary theft method.
- **Analytical procedures (ratios, trends)** indicate *where* to look, not proof of fraud.
- **Separation of duties** is the single most important fraud deterrent.

---

3. Key Concepts and Explanations

A. Financial Statement Fraud: Concealed Liabilities & Expenses

Core Idea:
Understating liabilities or expenses artificially inflates earnings **peso-for-peso**.

Why this scheme is attractive to fraudsters

- Requires **less effort** than creating fake revenue
- Often justified as “temporary”

- Easier to rationalize
- Harder to detect

Three Primary Methods (HIGH PRIORITY)

1. **Omitting liabilities and expenses**
    - Ignoring vendor invoices
    - Not recording judgments or litigation
    - Delaying recognition intentionally
2. **Improper capitalization**
    - Expensing vs capitalizing based on intent, not substance
    - Shifts expenses to future periods
3. **Failure to record warranty & return liabilities**
    - Under-accruing predictable future costs

Key Insight:

Recording an expense later **does not cure the fraud** in the current period.

Detection of Omitted Liabilities

- Review **post-balance-sheet transactions**
- Analyze accounts payable flows
- Conduct **physical searches** for unrecorded invoices
- Perform **targeted interviews**

B. Capitalizing vs Expensing Costs

Rules

- Repairs → expense
- Improvements that increase value or life → capitalize

Fraud Mechanics

- Improper capitalization:
    - Overstates assets
    - Overstates income now

    - Understates income later
- Improper expensing:
    - Often tax-motivated
    - Smooths future earnings

Exam Insight:
Questions test **timing effects**, not journal entries.

C. Improper Disclosures

Financial statements must include **all material information needed to avoid misleading users**.

Common disclosure fraud areas:

- Contingent liabilities
- Subsequent events
- Management fraud
- Related-party transactions
- Accounting changes
- Stock option backdating

Key Principle:

Partial or misleading disclosure = fraud.

D. Red Flags of Financial Statement Fraud

HIGH-YIELD RED FLAGS

- Profits without cash
- Aggressive estimates
- Shrinking reserves
- Margin growth beyond peers
- Management dominance
- Complex period-end transactions
- Related-party transactions
- Repeated “immaterial” justifications

E. Financial Statement Analysis as a Detection Tool

Analysis does **not prove fraud**—it **points where to dig**.

Core tools:

- **Vertical analysis** – relationships within one period
- **Horizontal analysis** – changes over time
- **Ratio analysis** – relationships between accounts

Rule of thumb:
Large dollar changes matter more than percentages.

Key Ratios & Fraud Signals (EXAM FAVORITES)

- **Current ratio** ↓ → possible embezzlement
- **Quick ratio** ↓ → fictitious A/R or overstated assets
- **A/R turnover** ↓ → fictitious sales
- **Inventory turnover** ↑ abnormally → inventory theft
- **Debt-to-equity** ↑ → concealed liabilities
- **Profit margin** unusually high → understated expenses
- **Asset turnover** ↓ → improper capitalization

F. Interviews in Financial Statement Fraud

Who is central: CEO and CFO
Why: They control estimates and override controls

Key Interview Principles

- Ask questions, not accusations
- One person at a time
- Non-threatening approach
- Start broad → end direct
- Hypothetical questions first
- Always ask executives directly if they committed fraud

Exam Insight:
Failure to ask direct fraud questions = serious professional weakness.

G. Prevention of Financial Statement Fraud

Built around **Fraud Triangle reduction**

Reduce Pressure

- Avoid unrealistic targets
- Remove structural obstacles

Reduce Opportunity

- Strong internal controls
- Segregation of duties
- Oversight and monitoring

Reduce Rationalization

- Ethical tone at top
- Clear policies
- Consistent consequences

---

4. Important Terms and Definitions

- **Concealed liabilities** – obligations omitted from records
- **Improper capitalization** – recording expenses as assets
- **Skimming** – theft before recording (off-book)
- **Cash larceny** – theft after recording (on-book)
- **Lapping** – using later receipts to cover earlier theft
- **Shrinkage** – physical inventory < perpetual inventory
- **Contingent liability** – obligation dependent on future event
- **Management override** – bypassing established controls

---

5. Comparisons and Distinctions

Skimming vs Cash Larceny

Skimming	Cash Larceny
Before recording	After recording
Off-book	On-book

No audit trail	Audit trail exists
Harder to detect	Easier to detect

Capitalizing vs Expensing

Capitalize	**Expense**
Defers expense	Immediate hit
Boosts current income	Reduces income now
Risk of future reversal	Cleaner earnings

Ratio Analysis vs Proof

Ratio Analysis	**Proof**
Screening tool	Evidence
Indicates risk	Confirms fraud

---

6. Memory Hooks

- **CLE** → Concealed Liabilities = *Criminally Lazy & Easy*
- **Before book = Skimming**
- **After book = Larceny**
- **Cash tells truth**
- **V-H-R** → Vertical, Horizontal, Ratios
- **Pressure talks, controls stop**

---

7. Likely Exam / High-Yield Points

If this appears on the exam, remember:

- Omissions > misstatements
- Fraud often spans **multiple periods**
- Analytical anomalies → start point only
- Lapping hides theft, doesn't create it

- Executives must be questioned directly
- Improper disclosures alone can constitute fraud

Common traps

- Treating ratio changes as proof
- Confusing skimming with larceny
- Ignoring timing effects
- Forgetting management's role

---

8. Quick Recall Sheet (Last-Minute Scan)

- Fraud = intentional
- Missing liabilities inflate income
- Capitalization shifts earnings forward
- Skimming before books
- Larceny after books
- Ratios flag, evidence proves
- Cash flow exposes lies
- Controls fail → fraud thrives

OPTIONAL ENHANCEMENTS

Recall Questions

1. Why are omissions harder to detect than misstatements?
2. How does improper capitalization affect future earnings?
3. Why is skimming considered off-book fraud?
4. When does lapping become unsustainable?
5. Why must CEOs be asked direct fraud questions?

Flashcards

- **Q:** Most dangerous FSF method?
  A: Concealed liabilities
- **Q:** Skimming leaves what trail?
  A: No direct trail

- **Q:** Best cash fraud indicator?
  A: Cash flow inconsistency
- **Q:** What precedes most FSF?
  A: Management pressure
- **Q:** Best deterrent?
  A: Strong internal control + ethics

1-Minute Review

Financial statement fraud relies on omissions, timing, and control failures. Skimming occurs before recording; larceny after. Ratios point, cash confirms, controls prevent.

5-Minute Review

Focus on concealed liabilities, improper capitalization, skimming vs larceny, lapping mechanics, key ratios, executive interviews, and Fraud Triangle prevention.

PART I – ASSET MISAPPROPRIATION: FRAUDULENT DISBURSEMENTS

1. Electronic Payment Fraud

Common Concealment Methods

- Altering bank statements
- Miscoding transactions
- Using shell companies with similar names
- Relying on lack of reconciliation

Key Preventive Controls

- Strict **segregation of duties** (create → approve → release → reconcile)
- **No payment personnel** should reconcile bank statements
- Daily reconciliation and monitoring
- Strong access controls (passwords, MFA, automatic deactivation)

Bank Security Tools

- ACH blocks and filters
- Positive Pay (ACH)
- Dual authorization & transaction limits
- Multifactor authentication

✅ **CFE tip:** Expect questions distinguishing **internal controls vs. bank-provided controls**.

---

2. Billing Schemes (Most Common Fraudulent Disbursement)

A. Shell Company Schemes

Characteristics

- No real operations, employees, or economic value
- Set up by employee or via relative
- Used to submit fictitious or inflated invoices

Common Red Flags

- Vendor address = employee / relative address
- PO box–only vendors
- Newly created vendors with high billings
- Employee self-approval of invoices

Core Control Weakness Exploited

- Lack of separation between **vendor setup, PO approval, invoice approval**

B. Nonaccomplice Vendor Schemes (Pay-and-Return)

Methods

- Paying invoices twice
- Paying wrong vendor
- Overpaying vendor and intercepting refunds

✅ **Exam clue:** Vendor is *not* aware—employee manipulates the process.

C. Personal Purchases with Company Funds

Variants

- False invoices
- Mischaracterized purchases
- Use of company credit cards

Typical Red Flags

- Mixed personal and business items
- Deliveries sent to home addresses
- Employee approves own expenses

---

3. Detection of Billing Schemes

Primary Methods

- Analytical review (purchases vs. sales trends)
- Data analytics:
    - Vendors ↔ employees with same address
    - One-time or unusual charges
- Statistical sampling
- Vendor complaints

Sample Audit Focus

- 3-way match (PO–RR–Invoice)
- Duplicate invoice checks
- Vendor master file review

PART II – PAYROLL FRAUD SCHEMES

1. Ghost Employees

Definition

A person on payroll who does not actually work for the organization.

Four Required Elements

1. Added to payroll
2. Timekeeping/wage data created
3. Paycheck issued
4. Payment delivered to fraudster

Key Red Flags

- Duplicate addresses or bank accounts
- No tax withholdings
- Similar names (e.g., John Doe vs. John Doer)

---

2. Falsified Hours & Salary

How It Happens

- Overstated hours
- Unauthorized rate increases

Approval Manipulation

- Forged supervisor approval
- Collusion with supervisor
- Reliance on negligent supervisor

✅ **Classic exam setup:** "Supervisor routinely approves timecards without review."

---

3. Commission Schemes

Two Ways to Inflate Pay

1. Overstate sales
2. Inflate commission rate

Red Flags

- Disproportionate commissions
- High write-offs of A/R linked to one salesperson
- Fictitious customers

---

4. Payroll Fraud Prevention

- Separate HR, payroll, distribution, reconciliation
- Independent payroll distribution
- Periodic payroll audits
- Match HR records ↔ payroll list

PART III – EXPENSE REIMBURSEMENT SCHEMES

1. Mischaracterized Expenses

- Personal expenses claimed as business
- Vague or missing business purpose

2. Overstated Expenses

- Altered receipts
- "Invoice swapping" (buy high → return → submit receipt)

3. Fictitious Expenses

- Fake receipts (software-generated, blank receipts)
- Expenses never incurred

4. Multiple Reimbursements

- Same expense claimed multiple times
- Credit card **plus** reimbursement

Best Detection Method ✅ **Detailed review of expense reports** + employee schedules

---

PART IV – INVENTORY & OTHER ASSETS

1. Misuse vs. Theft

- **Misuse**: borrowing without intent to steal
- **Theft**: permanent deprivation

2. Inventory Theft Methods

- Larceny (no records manipulation)
- False sales
- False shipments
- Asset requisition abuse

3. Concealment Techniques

- Forced inventory reconciliations
- Fictitious sales & A/R
- Write-offs (obsolete, scrap)
- Physical padding (empty boxes)

4. Detection Tools

- Perpetual vs. physical inventory comparison
- Trend analysis (COGS vs. sales)
- Statistical sampling of receiving & shipping docs

PART V – CORRUPTION (HIGH-IMPACT EXAM AREA)

1. Core Forms

Type	Key Feature
Bribery	Payment to influence decision
Kickback	Share of proceeds
Illegal gratuity	Reward *after* decision
Economic extortion	"Pay or else"
Conflict of interest	Undisclosed personal interest

---

2. Kickbacks

- Overbilling most common mechanism
- Usually attacks **purchasing function**

✅ **Distinction to remember**

- Shell company → **Asset misappropriation**
- Real company owned by employee → **Conflict of interest**

---

3. Detection of Corruption

Primary Method

- Tips (most common detection source)

Red Flags

- Vendors repeatedly winning bids
- Extravagant employee lifestyle
- PO boxes, shared addresses
- Poor procurement documentation

---

4. Proving Corrupt Payments

On-Book

- Fictitious payables
- Overbilling
- Ghost employees

Off-Book

- Cash payments
- Unrecorded sales
- Focus on **point of receipt**

FINAL CFE EXAM QUICK HITS

- **Most common asset misappropriation:** Billing schemes
- **Most powerful control:** Segregation of duties
- **Best fraud detection method overall:** Tips
- **Payroll fraud hardest to detect:** Ghost employees (esp. with direct deposit)
- **Conflict vs. Billing:** Ownership interest determines classification

CFE High-Yield Summary & Examination Notes

Topics Covered

- Conflicts of Interest (COI)
- Corruption Schemes
- Theft of Data & Intellectual Property
- Corporate Espionage
- Insider Threats
- Identity Theft
- Financial Institution Fraud (Intro)

1️⃣ Conflicts of Interest (COI)

Core Definition (Exam-Critical)

A **conflict of interest** exists when an individual's **personal interest interferes—or appears to interfere—with their duty of loyalty to the employer** [Fraud Exam...rs Manual4 | PDF]

Major COI Schemes

Scheme	Description	Key Red Flag
Turnaround / Flip Sales	Employee buys asset first, resells to employer at inflated price	Same-day buy/sell, unusual pricing
Underselling	Employer sells below market to related party	Margin erosion

Write-off Sales	Credit memos used to eliminate receivables	Excessive reversing entries
Delayed Billing	Favoring clients by delaying invoicing	Chronic aged receivables
Business Diversion	Employee siphons customers to own business	Lost customers, side business
Resource Diversion	Employer funds used to build employee's future business	Related future employment

Disclosure Risks

- Failure to disclose **related-party transactions** is one of the **most serious frauds** [Fraud Exam...rs Manual4 | PDF]
- **Appearance of conflict** ≈ almost as damaging as actual conflict

---

2️⃣ Detecting Conflicts of Interest

Primary Detection Methods (CFE Favorite)

- Tips & complaints (most common)
- Vendor ↔ employee address matching
- Vendor master file vs employee master file
- Exit interviews
- Interviews with procurement staff
- Family disclosure requirements [Fraud Exam...rs Manual4 | PDF]

Classic COI Red Flags

- Unusual vendor favoritism
- Employee lifestyle beyond means
- Undisclosed relationships
- Vendor details matching employee data
- Inferior products accepted without challenge

3️⃣ Prevention & Governance

Preventive Controls

- Clear COI policy + annual disclosures
- Ethical tone at the top

- Regular employee education
- Monitoring of disclosed relationships [Fraud Exam...rs Manual4 | PDF]

ISO 37001 – Anti-Bribery (Exam Tip)

ISO 37001 focuses on **proportionate, risk-based anti-bribery controls**, including:

- Policy
- Training
- Risk assessments
- Due diligence
- Financial/commercial controls [Fraud Exam...rs Manual4 | PDF]

4️⃣ Theft of Data & Intellectual Property

CIA Triad (Must-Memorize)

- **Confidentiality**
- **Integrity**
- **Availability** [Fraud Exam...rs Manual4 | PDF]

Intellectual Property Includes

- Trade secrets
- Source code
- R&D data
- Pricing strategies
- Customer information

5️⃣ Competitive Intelligence vs Espionage

Legitimate	Illegal
Open-source research	Covert, illegal methods
Public filings	Wiretapping
Industry reports	Social engineering
Ethical codes (SCIP)	Insider recruitment

Corporate espionage = illegal, covert acquisition for business advantage [Fraud Exam...rs Manual4 | PDF]

6️⃣ Corporate Espionage – Methods

Information Sources

- Open-source intelligence (OSINT)
- Dumpster diving
- Surveillance (physical & technical)
- Human intelligence
- Transactional intelligence
- Social engineering [Fraud Exam...rs Manual4 | PDF]

Social Engineering (High-Yield)

4 phases:

1. Gather intelligence
2. Choose tactic
3. Build trust
4. Elicit information

Common tactics:

- Pretexting
- Phishing / spear-phishing
- Shoulder surfing
- Reverse social engineering

7️⃣ Insider Threats

Insider Categories

Type	Description
Traitors	Abuse legitimate access
Zealots	Ideology-driven
Spies	Planted operatives
Browsers	Curious snoopers

Well-intentioned	Careless users [Fraud Exam...rs Manual4 | PDF]

Motivations

- Financial gain
- Revenge
- Ego
- Ideology
- Opportunity

CERT Top Controls (Memorize)

- Insider threat program
- HR + IT coordination
- Focus on high-value assets
- Monitor ingress/egress
- Baseline normal behavior

Identity Theft

Definition

Wrongful acquisition and use of personal data for fraud or deception, typically for economic gain [Fraud Exam...rs Manual4 | PDF]

Key Types

- **Traditional** (account takeover, true-name fraud)
- **Synthetic** (real + fabricated data)
- Financial
- Criminal
- Medical
- Tax
- Employment
- Business identity theft

Common Methods

- Dumpster diving
- Phishing / vishing / smishing

- Malware
- Mail theft
- Address changes
- Skimming

🏦 Financial Institution Fraud (Intro)

Embezzlement Schemes

- False accounting entries
- Suspense accounts
- Unauthorized withdrawals
- Dormant account abuse
- Skimming irregular receivables [Fraud Exam...rs Manual4 | PDF]

Detection Red Flags

- Missing documents
- Out-of-sequence checks
- Abnormal reconciliations
- Excessive write-offs
- Suspense accounts

🔑 CFE Exam Memory Anchors

- **COI = duty of loyalty**
- **Most COI detected via tips**
- **Appearance matters**
- **CIA triad**
- **OSINT ≠ espionage**
- **Social engineering exploits human nature**
- **Insiders are highest data risk**
- **Synthetic identity theft = hardest to detect**

Financial Institution Fraud • Mortgage Fraud • Payment Fraud • Insurance Fraud

---

1. Big Picture Summary

This document explains **how fraud manifests across financial institutions**, focusing on **mortgages, new accounts, wire transfers, payment systems, and insurance**.

The unifying idea is:

Financial institution fraud thrives at scale, speed, and complexity—where incentives, technology, and weak verification intersect.

Across all topics, the **recurring examiner mindset** is:

- Follow **who controls information**
- Focus on **origination stages**
- Identify **collusion**
- Watch **speed, volume, and complexity**
- Assume fraud increases where **verification lags execution**

---

2. Must-Know Points (HIGH PRIORITY)

- **Mortgage fraud adapts to economic cycles** (booms, recessions, relief programs).
- **Inflated or "made-as-instructed" appraisals** are a cornerstone of mortgage fraud.
- **Straw borrowers** are central to many mortgage schemes.
- **New accounts are the highest-risk accounts** (first 90 days).
- **Wire transfer fraud can destroy a firm instantly**.
- **Separation of duties is the single most powerful control**.
- **Payment fraud has shifted from card-present to card-not-present (CNP)**.
- **Fraud displacement is real**: controls in one area push fraud elsewhere.
- **Insurance fraud exists in underwriting, claims, agents, and policyholders**.
- Basel, FATF, STRs, and operational risk frameworks underpin financial crime defenses.

---

3. Key Concepts and Explanations

A. Fraudulent Appraisals (Mortgage Foundation Fraud)

What it is

Manipulating assumptions in appraisals to inflate or deflate property value.

Common Manipulations

- Unrealistic vacancy/expense assumptions
- Inflated income, absorption, or selling prices
- Influencing or colluding with appraisers

Why it matters

The appraisal drives loan amount, loss severity, and downstream fraud potential.

Uses of Fraudulent Appraisals

- Approving marginal loans
- Rolling over bad loans
- Concealing losses
- Criminal profit

Red Flags (EXAM FAVORITE)

- New or unapproved appraiser
- Excessive appraisal fees
- Invalid comparables
- Unsupported market assumptions

Detection Logic

Always reconcile the appraisal to:

- Leases
- Comparable sales
- Absorption rates
- Residual values
- Capitalization rates

B. Mortgage Industry Structure (Exam Framework)

Key Parties (Know Roles)

- **Mortgagor** – borrower

- **Mortgagee** – lender
- **Broker / Agent** – intermediary
- **Loan officer** – sales
- **Underwriter** – credit risk
- **Appraiser** – valuation
- **Investor** – secondary market

Structural Risk Insight

The **secondary market** divorces origination from long-term risk → fraud risk increases.

C. Why Mortgage Fraud Persists

Contributing Factors

- Commission-driven incentives
- Lender competition
- High loan volumes
- Subprime lending
- Technology & e-processing
- New/unregulated players

Classic exam logic:
Pressure + speed + commission = fraud opportunity.

D. Core Mortgage Fraud Schemes (HIGH PRIORITY)

1. Builder Bailout

- Unsold inventory
- Inflated appraisals
- Undisclosed incentives
- Straw borrowers
- Loans stay current briefly, then default

Key exam test:
👉 *Disclosure = legality*. Undisclosed incentives = fraud.

---

2. Air Loans

- Nonexistent properties
- Fully fabricated documents
- Early payment default
- Massive losses
- High collusion

---

3. Identity Fraud vs Identity Theft

Identity Fraud	Identity Theft
Misrepresent data	Assume entire identity
Credit manipulation	Asset theft (home)

---

4. Fraudulent Sale / Second Lien

- Forged deeds
- Free-and-clear properties
- Identity assumption
- Inflated appraisal
- 100% proceeds stolen

---

5. Foreclosure Rescue Scams

- **Phantom-help** – fees, no help
- **Lease-back** – deed stolen

---

6. Short Sale Fraud

- Facilitator scams
- Straw buyers
- Reverse staging
- Hidden relationships (non-arm's-length)

---

7. Property Flipping vs Flopping

Flipping	Flopping
Inflate second sale	Deflate first sale
Normal market abuse	Short-sale exploitation

---

8. Equity Skimming

- Rent collected
- Mortgages unpaid
- Equity extracted
- Best with non-recourse loans

---

9. Reverse Mortgage Fraud

- Inflated values
- POA abuse
- Occupancy lies
- Senior exploitation

E. New Account Fraud (Banking EXAM FAVORITE)

Definition: Fraud within **first 90 days**.

Schemes

- False IDs
- Stolen checks
- Mobile deposits
- ATM deposits
- Pass-through accounts

Red Flags

- Immediate withdrawals
- Mail drop addresses
- No credit history (25+)

- Inconsistent behavior
- Large deposits → rapid withdrawals

F. Wire Transfer Fraud (VERY HIGH RISK)

Why Dangerous

Instant + irreversible = catastrophic losses

Common Schemes

- Dishonest insiders
- Identity misrepresentation
- Password compromise
- Forged authorizations
- Unauthorized wire room access
- Business Email Compromise (BEC)

Core Controls

- Order ≠ authorize
- Call-back to known numbers
- Segregated duties
- Mandatory vacations
- Logs, reconciliations, recordings

G. Payment Fraud (Largest Scope, Highest Volume)

Check Fraud

- Counterfeiting
- Washing
- Paperhangers
- Kiting
- Demand drafts

Card Fraud

- Lost/stolen cards

- CNP fraud
- Skimming vs shimming
- Account takeover
- Card number generation

Fraud Displacement Pattern

Chip & PIN ↓ → CNP ↑

H. Electronic & Emerging Payments

- EBPP
- P2P (PayPal, Venmo)
- Mobile wallets
- Virtual cards
- QR code scams

Exam insight:
Most fraud exploits **account setup**, not transaction tech.

I. Cryptocurrency & Virtual Economies

Why Fraud-Prone

- Pseudonymity
- Irreversibility
- Cross-border
- Weak regulation (historically)

Uses in Fraud

- Laundering
- Pump-and-dump
- Dark web commerce
- Virtual asset laundering

J. Insurance Fraud

Internal (Agent/Employee)

- Premium theft
- Settlement diversion
- Fictitious claims
- Tombstone policies
- Equity funding abuse

External

- Health care fraud
- Vehicle fraud (staged accidents, ditching)
- Claim padding

---

4. Important Terms and Definitions

- **Straw borrower** – lends identity
- **Made-as-instructed appraisal** – value engineered
- **Air loan** – no collateral exists
- **CNP fraud** – card-not-present
- **BEC** – business email compromise
- **Equity skimming** – rent over mortgage
- **Flopping** – deflated short sale
- **Pass-through account** – transient funds
- **Operational risk** – failed processes, people, systems

---

5. Comparisons and Distinctions

Skimming vs Shimming

Skimming	Shimming
Magnetic stripe	Chip cards
Older tech	Newer adaptation

Identity Fraud vs Identity Theft

Fraud	Theft
Data misrepresentation	Identity assumption
Credit abuse	Asset seizure

Flipping vs Flopping

| Inflate later | Deflate earlier |

---

6. Memory Hooks

- **VALUE DRIVES FRAUD** → Appraisals matter
- **FIRST 90 DAYS = DANGER**
- **FAST = FRAUD RISK**
- **ORDER ≠ AUTHORIZE**
- **DISCLOSE = LEGAL / HIDE = FRAUD**
- **CONTROLS SHIFT FRAUD, NOT ELIMINATE IT**

---

7. Likely Exam / High-Yield Points

If this appears in the exam, remember:

- Mortgage fraud = **collusion**
- New account fraud = **speed**
- Wire fraud = **segregation**
- Payment fraud = **displacement**
- Insurance fraud = **internal + external**
- Basel & FATF = **frameworks, not operations**

Common traps

- Ignoring disclosure
- Assuming fraud stops (it moves)
- Confusing fraud vs abuse
- Overreliance on automation

---

8. Quick Recall Sheet

- Appraisals drive losses
- Straw borrowers everywhere
- New accounts = highest risk
- Wires are lethal
- CNP > CP fraud
- Fraud displaces
- Disclosure determines legality
- Controls > detection

OPTIONAL ENHANCEMENTS

5 Recall Questions

1. Why are new accounts the highest fraud risk?
2. What makes wire fraud uniquely dangerous?
3. How does fraud displacement work?
4. Why are short sales fertile ground for fraud?
5. What turns property flipping into fraud?

5 Flashcards

- **Q:** First 90 days fraud?
  A: New account fraud
- **Q:** Inflate vs Deflate short sale?
  A: Flipping vs flopping
- **Q:** Best wire fraud control?
  A: Segregation + call-back
- **Q:** Who commits mortgage fraud?
  A: Collusive insiders
- **Q:** Why crypto attracts fraud?
  A: Irreversibility + anonymity

Insurance Fraud • Health Care Fraud • Consumer Fraud • Ponzi & Pyramid Schemes

---

1 Big Picture Summary (Anchor First)

This document covers **fraud committed through systems built on trust, volume, and complexity**:

- **Insurance fraud** exploits claims processes and underwriting assumptions
- **Health care fraud** exploits technical expertise, reimbursement systems, and third-party payers
- **Consumer fraud** exploits information asymmetry, urgency, and emotions
- **Ponzi & pyramid schemes** exploit greed, social proof, and opacity

Unifying principle:

Fraud increases when **verification lags transactions** and victims **cannot easily test truth**.

2️⃣ CFE Must-Know Frameworks (Very High Yield)

A. Who Commits Fraud?

Across all sections:

- **Customers / claimants**
- **Agents / brokers**
- **Employees**
- **Third parties**
- **Organized networks**

B. Where Fraud Occurs Most

Stage	Why High Risk
Origination	Data is unverified
Early claims	Limited scrutiny
High-volume processing	Exceptions overlooked
Third-party billing	Accountability diluted

3️⃣ INSURANCE FRAUD (Exam Core)

3.1 Major Categories

1. **Property schemes** (inflated inventory, fictitious losses)
2. **Life insurance fraud** (phony deaths, murder-for-profit)
3. **Liability schemes** (slip-and-fall)
4. **Workers' compensation fraud**
    - Premium fraud

- Agent fraud
- Claimant fraud
- Organized fraud

3.2 Workers' Compensation Fraud – HIGH YIELD

Premium Fraud (Employer-Driven)

- Employee misclassification
- Understatement of payroll
- Geographic manipulation
- Mod-factor evasion
- Corporate gerrymandering
- Forged certificates

Exam insight
👉 Payroll + classification = premium. Manipulate either → fraud.

Agent Fraud

- Premium theft (coverage issued, premiums pocketed)
- Altered applications to reduce premiums
- Illegal advice to misclassify employees

👉 **Employer liability still exists** if they signed the application.

Claimant Fraud

- Staged injuries
- Exaggerated injuries
- Secondary employment while disabled
- Doctor cooperation for false diagnoses

Organized Fraud (Exam Favorite)

The **4-player model**:

Role	Function
Lawyer	Organizer, volume settlements
Capper	Recruits claimants
Doctor	Validates false injuries
Claimant	Provides identity

3.3 Insurance Fraud Red Flags (Memorize)

- Claims soon after policy inception
- Too-perfect documentation
- No sentimental items in loss claims
- Receipt irregularities
- Pressure for speed
- Same providers / attorneys repeatedly
- Document alterations
- Poor-quality photocopies

🏥 HEALTH CARE FRAUD (Largest Volume on Exam)

4.1 Core Definition

Intentional deception to obtain unauthorized benefits from a health care program.

4.2 Health Care Systems (Conceptual Foundation)

System	Fraud Impact
Direct pay	Patient fraud ↓
Single payer	Provider fraud ↑
Third-party payer	Provider + patient fraud

4.3 Reimbursement Models & Fraud Incentives

Model	Fraud Tendency
Fee-for-service	Over-utilization
Capitation	Fictitious patients
Episode of care	Bundling abuse
Salary	Institutional fraud

4.4 Provider Fraud (TOP CFE CONTENT)

Core Schemes

- Fictitious providers
- Fictitious services
- Rolling labs
- Over-utilization
- Uncredentialed providers
- Disparate pricing
- Equipment fraud (DME)
- Pharmaceutical fraud
- Impostor providers

Coding Fraud (VERY HIGH YIELD)

- **Upcoding**
- **Unbundling**
- **Mutually exclusive procedures**
- **Global service period violations**
- **False diagnoses**

Key insight
👉 Coding complexity = fraud camouflage.

4.5 Institutional Fraud

- False cost reports

- DRG creep
- Experimental procedures
- Improper physician relationships
- Revenue recovery padding

4.6 Electronic Claims (EDI Fraud)

- No paper trail
- High speed
- Volume masking
- Authentication challenges

Control focus

- Encryption
- Digital signatures
- Exception reports
- Origin verification

4.7 Health Care Compliance Programs (Exam Essay Favorite)

Key components:

1. Written standards & code of conduct
2. Compliance officer reporting to CEO/Board
3. Training & certifications
4. Monitoring & analytics
5. Anonymous reporting
6. Investigation & discipline
7. Continuous improvement

👉 **Effective compliance = mitigation + sentencing leniency**

5️⃣ **CONSUMER FRAUD (Emotion-Driven)**

Common Psychology

- Urgency

- Authority
- Reciprocity
- Scarcity
- Fear / Hope

Major Scheme Families

- Advance-fee fraud
- Debt consolidation
- Diploma mills
- Health cure scams
- Travel & vacation fraud
- Sweepstakes & prizes
- Credit repair
- Work-at-home scams
- Affinity fraud
- Charity fronts

Electronic Consumer Fraud

- Phishing
- Smishing
- Vishing
- Pharming
- Identity leverage

Elder Fraud (Explicitly Tested)

- Home improvement scams
- Grandparent scams
- Romance schemes
- Tech support fraud

Exam warning

👉 Elder fraud often involves **trusted insiders**, not strangers.

6️⃣ PONZI & PYRAMID SCHEMES (Guaranteed Exam Questions)

Ponzi Scheme

- Old investors paid with new investors' money
- No real investment activity
- Collapses when inflows stop

Exam Red Flags

- Consistent returns
- Secrecy
- No segregation of duties
- Unregistered investments
- Pressure to reinvest
- "Too complex to explain"

Bernie Madoff – CAE-Level Insight

Why it lasted:

- Reputation & authority
- Stable (but fake) returns
- No third-party custody
- Internalized control functions
- Discouraged questioning

Illegal Pyramid Schemes

- Recruitment > product
- Early winners, late losers
- 70% Rule (retail focus)

Types:

- Pure cash schemes

- Product fronts (MLM)
- Endless chains
- Fill-and-split games

7️⃣ Ultra-High Yield CFE Memory Hooks

- **Speed kills controls**
- **Volume hides fraud**
- **Coding = camouflage**
- **Disclosure determines legality**
- **New accounts & early claims = danger**
- **No segregation = fraud certainty**
- **If it's too perfect, it's fake**
- **If it's too consistent, it's a Ponzi**

8️⃣ 15-Second Recall Sheet

- Workers' comp = premium, agent, claimant, organized
- Health care fraud = provider-driven
- FFS → overbilling
- Capitation → fake patients
- Coding fraud = unbundling + upcoding
- Consumer fraud = urgency + emotion
- Ponzi = new money pays old
- Pyramid = recruitment, not product

Fraud Examiners Manual – Consumer Fraud, Cyberfraud, & Procurement Fraud

(High-Yield | Memory-Efficient | Exam-Focused)

I. CONSUMER FRAUD – PONZI & PYRAMID SCHEMES

1. Key Concepts

- **Ponzi Scheme** – Pays earlier investors using funds from later investors; minimal or no legitimate business

- **Pyramid Scheme** – Earnings depend primarily on recruitment rather than product value
- **Affinity Fraud** – Exploits trust within religious, social, ethnic, or professional groups

💡 **Exam Tip:** *All pyramids are Ponzi schemes, but not all Ponzis are pyramids.*

---

2. Common Ponzi "Product Fronts"

Category	Examples	Why Effective
Financial Instruments	Stocks, currency trading, crypto, futures	Complexity hides fraud
MLMs	Supplements, cosmetics, insurance	Mathematical illusion
Speculations	Real estate, franchises, work-from-home	Legitimate appearance

⚠ **Red Flags**

- Guaranteed or unusually high returns
- Consistent payouts regardless of market
- Expense emphasis on recruitment over product

---

3. MLM vs Illegal Pyramid (Exam Favorite)

Indicator	Illegal Pyramid	Legitimate Business
Main income source	Recruitment	Product sales
Emphasis	Levels / stages	Product value
Sustainability	Requires infinite growth	Market-based

II. CYBERFRAUD (MAJOR CFE EXAM WEIGHT)

1. Definition (Must Memorize)

Cyberfraud: Computer-aided activity involving intentional misrepresentation or data alteration to obtain value and cause loss

---

2. Cyberfraud Characteristics

- No paper trail
- Requires IT expertise

- Often uses specialists
- Computer = **target, tool, or both**

---

3. Indicators of Intrusion (IOCs)

Network Indicators

- Abnormal traffic volume
- Suspicious DNS requests
- Geographic anomalies

User/File Indicators

- Excessive access attempts
- Unauthorized data downloads
- Registry/system file changes

System Performance

- Unexpected slowdowns
- Pop-ups, fake antivirus alerts
- Programs crashing or restarting

💡 **CFE Angle:** *Fraud examiners are not expected to fix systems but must recognize red flags.*

III. SOCIAL ENGINEERING SCHEMES (HIGH-YIELD)

Types to Memorize

Scheme	Key Feature
Phishing	Fake emails & websites
Spear phishing	Targeted corporate email
BEC (Business Email Compromise)	CEO or supplier impersonation
Vishing	Voice + spoofed caller IDs
Smishing	SMS-based phishing
Pharming	DNS redirection
Catfishing	Fake online relationships

Reverse Social Engineering	Victim contacts attacker

📊 **BEC Fact:** Largest cybercrime losses globally

IV. HACKING & UNAUTHORIZED ACCESS METHODS

Common Techniques

- Password cracking
- Keylogging (hardware/software)
- RATs (Remote Access Trojans)
- Packet sniffing
- Spoofing (IP, DNS, email)
- Piggybacking
- Dumpster diving
- Discarded media recovery

💡 **Mnemonic: S.P.O.O.F P.I.G. D**
Spoofing, Packet sniffing, OS exploits, Keylogging, Piggybacking, Insider, Dumpster diving

---

V. MALWARE (EXAM ESSENTIAL)

Malware Types

- Virus
- Worm
- Trojan
- Spyware / Adware
- Ransomware
- Logic bomb
- Trapdoor
- Coin miner (cryptojacking)
- Botnets

Ransomware Key Points

- Locks or encrypts data
- Payment ≠ recovery guarantee

- Severe operational & reputational risk
- Often followed by phishing attacks

Malware Detection Signs

- Unexpected restarts
- Missing or enlarged files
- Disabled antivirus
- Browser hijacking
- Excessive pop-ups

VI. PROCUREMENT & CONTRACT FRAUD (CORE FOR CFE)

1. Procurement Fraud Defined

Fraud occurring at **any phase** of acquiring goods or services to obtain value improperly

---

2. Procurement Phases (Memorize Order)

1. **Presolicitation**
2. **Solicitation**
3. **Bid Evaluation & Award**
4. **Post-Award / Administration**

---

3. Major Procurement Fraud Schemes

A. Collusion Among Contractors

- Bid rotation
- Bid suppression
- Complementary bidding
- Market division

🚩 **Red Flags**

- Same bidders always win
- Identical bid patterns
- Winning bidder subcontracts to losers

B. Collusion with Employees

- Need recognition schemes
- Bid tailoring
    - Narrow specs
    - Broad specs
    - Vague specs
- Bid manipulation
- Leaking bid data
- Bid splitting
- Unjustified sole-source awards

C. Defective Pricing (Negotiated Contracts)

- Inflated labor/material costs
- Failure to disclose discounts
- Phantom vendors
- Outdated cost data

D. Performance-Stage Schemes

Scheme	Description
Nonconforming goods	Inferior substitution
Change order abuse	Low bid → inflated changes
Cost mischarging	Unallowable / misallocated costs

VII. INFORMATION SECURITY CONTROLS

CIAAN Model

- **Confidentiality**
- **Integrity**
- **Availability**

- **Authentication**
- **Non-repudiation**

Control Categories

Type	Examples
Physical	Guards, locks, biometrics
Technical	Firewalls, IDS/IPS, encryption
Administrative	Policies, training, SoD

IDS vs IPS (Exam Shortcut)

- **IDS** = Detects & alerts
- **IPS** = Detects & blocks

VIII. INCIDENT RESPONSE (VERY TESTABLE)

Five-Step Model

1. Preparation
2. Detection & Analysis
3. Containment & Eradication
4. Breach Notification
5. Recovery & Follow-Up

⚠ **Legal Reminder:** Evidence preservation is mandatory

✅ **FINAL EXAM FAST-REVIEW (ONE-PAGE MEMORY)**

- **Ponzi** = Fake investment
- **Pyramid** = Recruitment based
- **BEC** = CEO impersonation + urgency
- **Malware** = Broader than virus
- **Change orders** = Favorite fraud channel
- **Procurement fraud** can happen in *all phases*

- **Separation of duties** is critical
- **Detection ≠ Prevention**

CONTRACT & PROCUREMENT FRAUD + LEGAL FOUNDATIONS

(Fraud Examiners Manual – Financial Transactions & Law Sections)

I. CONTRACT & PROCUREMENT FRAUD

A. COST MISCHARGING SCHEMES

1. Core Concept

Whether a cost mischarge is fraud **depends on intent**, not just error.

✅ **Audit mantra:** Error = poor control | Fraud = intent to deceive

---

2. Common Cost Mischarging Methods

Memorize as **"D-N-U-W-D-S-C-P-F"**

Category	Description
Double charging	Same cost charged to multiple contracts
Nonexistent/infl	Fake or overstated expenses
Un	Entertainment, ads, etc. charged to contract
Wrong category	Costs charged to incorrect accounts
Discount concealment	Vendor discounts not disclosed
Standard abuse	Outdated or improper standard costs
Collusion	Rebates, inflated pricing with vendors
Phantom	Fake vendors used to inflate costs
False	Fabricated or altered support

---

3. RED FLAGS – Cost Mischarging

Think **"Docs – Pricing – Disclosure – Controls"**

Documentation

- Missing / poor-quality support

- Inconsistent documents for same item
- Evidence of alteration/falsification

Pricing

- Costs inconsistent with estimates
- Old standards supporting proposals
- Wide price variance for same item

Disclosure

- Failure to disclose vendor discounts
- Withholding cost/pricing data
- Repeated noncompliance with bidding rules

Controls

- Unqualified personnel preparing cost data
- Weak estimating governance

II. THREE TYPES OF COST MISCHARGES

A. ACCOUNTING MISCHARGES

Definition: Knowingly hiding unallowable costs in allowable accounts.

📌 **Classic tactic:** Charging capped costs (B&P, IR&D) into:

- Salaries
- Repairs & Maintenance
- Office Supplies

✅ **Audit focus:** Account reclassification patterns

B. MATERIAL MISCHARGES

Material = **physical inventory & deliverables**

Common Schemes

- Fixed-price → cost-type contract transfers
- Standard vs actual pricing abuse
- Excess buying on one contract, use on another
- Intercompany/subsidiary inflated pricing

MATERIAL MISCHARGE RED FLAGS

Group as **Transfers – Inventory – Pricing – Controls**

- Mass inventory transfers between jobs
- Transfers at non-actual costs
- Charges with no physical inventory
- Excess write-offs / scrap account usage
- No audit trail
- Weak warehouse & receiving controls

C. LABOR MISCHARGES

Highest fraud risk (no physical evidence)

Labor Cost Inflation Methods

- Inflated salaries/fees
- Charging juniors at senior rates
- Time card falsification
- Cost-plus contract dumping
- Billing services vs actual hours

LABOR RED FLAGS

Think **"Volume – Pattern – Alignment – Controls"**

- Sudden spikes in labor hours
- Charges misaligned with progress
- No corresponding material usage
- Always near budget (too perfect)
- High turnover
- Rare vacations
- Weak timekeeping controls

III. DETECTION TECHNIQUES (EXAM-FAVORITE)

Material Mischarge Detection

- Trace job-to-job transfers

- Compare standard vs actual costs
- Review inventory write-offs
- Scan GL & adjusting entries
- Investigate ownership & conflicts

Labor Mischarge Detection

- Reconcile timecards to payroll
- Trend labor % by contract
- Compare prior vs current year labor mix
- Site visits (who's doing what)
- Analyze shifting charge numbers

IV. PREVENTING PROCUREMENT FRAUD

A. FOUR PILLARS

1. **Employee Education**
2. **Internal Controls**
3. **Continuous Monitoring**
4. **Vendor Management**

B. Key Internal Controls

- Segregation of duties
- Authorization & approval controls
- Receiving controls
- Reconciliation & recording controls

✅ **Exam tip:** Control weakness ≠ fraud, but enables it

C. Vendor Management (HIGH-YIELD)

Area	Key Risk
Vendor onboarding	Shell / related parties
Master file maintenance	Duplicate / fake vendors

Payments	Same person creates + pays
Monitoring	No post-engagement review

✅ **Golden rule:** Vendor creators ≠ payment approvers

V. LEGAL FOUNDATIONS (CFE CORE – LAW)

A. TYPES OF LAW (Mnemonic: S-P-A-I-C)

- **S**tatutory
- **P**rocedural
- **A**dministrative
- **I**nternational
- **C**ommon law

✅ Fraud examiners must know **procedure + rights**, not just fraud schemes.

B. CRIMINAL vs CIVIL FRAUD

Feature	Criminal	Civil
Brought by	State	Victim
Burden	Beyond reasonable doubt	Preponderance
Intent needed	Yes (mens rea)	Sometimes
Penalty	Jail/Fines	Damages

C. ELEMENTS OF FRAUD (CORE)

F-M-K-R-D

1. False statement
2. Material fact
3. Knowledge of falsity
4. Reliance
5. Damages

VI. SPECIAL FRAUD CATEGORIES (EXAM TRAPS)

Negligent Misrepresentation

- No intent needed
- Requires **duty + no reasonable basis**

Concealment

- Only fraud if **duty to disclose exists**

Bribery

Type	Key Feature
Official	Public official
Commercial	Private sector
Illegal gratuity	Reward after decision

VII. GLOBAL ANTI-CORRUPTION (COMPARE THIS)

Law	Key Point
FCPA (US)	Foreign public officials only; allows facilitation
UK Bribery Act	Covers private bribery; NO facilitation
OECD Convention	Supply-side bribery
UNCAC	Prevention, criminalization, asset recovery

VIII. WHAT CFE EXAMS LOVE TO ASK

✅ **Intent vs negligence**
✅ **Red flag identification**
✅ **Proper detection procedure**
✅ **Civil vs criminal thresholds**
✅ **Control failures vs fraud**
✅ **Vendor master file risks**

CONTRACT & PROCUREMENT FRAUD + LEGAL FOUNDATIONS

(Fraud Examiners Manual – Financial Transactions & Law Sections)

I. CONTRACT & PROCUREMENT FRAUD

A. COST MISCHARGING SCHEMES

1. Core Concept

Whether a cost mischarge is fraud **depends on intent**, not just error.

✅ **Audit mantra:** Error = poor control | Fraud = intent to deceive

---

2. Common Cost Mischarging Methods

Memorize as **"D-N-U-W-D-S-C-P-F"**

Category	Description
Double charging	Same cost charged to multiple contracts
Nonexistent/infl	Fake or overstated expenses
Un	Entertainment, ads, etc. charged to contract
Wrong category	Costs charged to incorrect accounts
Discount concealment	Vendor discounts not disclosed
Standard abuse	Outdated or improper standard costs
Collusion	Rebates, inflated pricing with vendors
Phantom	Fake vendors used to inflate costs
False	Fabricated or altered support

---

3. RED FLAGS – Cost Mischarging

Think **"Docs – Pricing – Disclosure – Controls"**

Documentation

- Missing / poor-quality support
- Inconsistent documents for same item
- Evidence of alteration/falsification

Pricing

- Costs inconsistent with estimates
- Old standards supporting proposals

- Wide price variance for same item

Disclosure

- Failure to disclose vendor discounts
- Withholding cost/pricing data
- Repeated noncompliance with bidding rules

Controls

- Unqualified personnel preparing cost data
- Weak estimating governance

II. THREE TYPES OF COST MISCHARGES

A. ACCOUNTING MISCHARGES

Definition: Knowingly hiding unallowable costs in allowable accounts.

📌 **Classic tactic:** Charging capped costs (B&P, IR&D) into:

- Salaries
- Repairs & Maintenance
- Office Supplies

✅ **Audit focus:** Account reclassification patterns

B. MATERIAL MISCHARGES

Material = **physical inventory & deliverables**

Common Schemes

- Fixed-price → cost-type contract transfers
- Standard vs actual pricing abuse
- Excess buying on one contract, use on another
- Intercompany/subsidiary inflated pricing

MATERIAL MISCHARGE RED FLAGS

Group as **Transfers – Inventory – Pricing – Controls**

- Mass inventory transfers between jobs
- Transfers at non-actual costs
- Charges with no physical inventory

- Excess write-offs / scrap account usage
- No audit trail
- Weak warehouse & receiving controls

C. LABOR MISCHARGES

Highest fraud risk (no physical evidence)

Labor Cost Inflation Methods

- Inflated salaries/fees
- Charging juniors at senior rates
- Time card falsification
- Cost-plus contract dumping
- Billing services vs actual hours

LABOR RED FLAGS

Think **"Volume – Pattern – Alignment – Controls"**

- Sudden spikes in labor hours
- Charges misaligned with progress
- No corresponding material usage
- Always near budget (too perfect)
- High turnover
- Rare vacations
- Weak timekeeping controls

III. DETECTION TECHNIQUES (EXAM-FAVORITE)

Material Mischarge Detection

- Trace job-to-job transfers
- Compare standard vs actual costs
- Review inventory write-offs
- Scan GL & adjusting entries
- Investigate ownership & conflicts

Labor Mischarge Detection

- Reconcile timecards to payroll
- Trend labor % by contract
- Compare prior vs current year labor mix
- Site visits (who's doing what)
- Analyze shifting charge numbers

IV. PREVENTING PROCUREMENT FRAUD

A. FOUR PILLARS

1. **Employee Education**
2. **Internal Controls**
3. **Continuous Monitoring**
4. **Vendor Management**

B. Key Internal Controls

- Segregation of duties
- Authorization & approval controls
- Receiving controls
- Reconciliation & recording controls

✅ **Exam tip:** Control weakness ≠ fraud, but enables it

C. Vendor Management (HIGH-YIELD)

Area	Key Risk
Vendor onboarding	Shell / related parties
Master file maintenance	Duplicate / fake vendors
Payments	Same person creates + pays
Monitoring	No post-engagement review

✅ **Golden rule:** Vendor creators ≠ payment approvers

V. LEGAL FOUNDATIONS (CFE CORE – LAW)

A. TYPES OF LAW (Mnemonic: S-P-A-I-C)

- **S**tatutory
- **P**rocedural
- **A**dministrative
- **I**nternational
- **C**ommon law

✅ Fraud examiners must know **procedure + rights**, not just fraud schemes.

B. CRIMINAL vs CIVIL FRAUD

Feature	Criminal	Civil
Brought by	State	Victim
Burden	Beyond reasonable doubt	Preponderance
Intent needed	Yes (mens rea)	Sometimes
Penalty	Jail/Fines	Damages

C. ELEMENTS OF FRAUD (CORE)

F-M-K-R-D

1. False statement
2. Material fact
3. Knowledge of falsity
4. Reliance
5. Damages

VI. SPECIAL FRAUD CATEGORIES (EXAM TRAPS)

Negligent Misrepresentation

- No intent needed
- Requires **duty + no reasonable basis**

Concealment

- Only fraud if **duty to disclose exists**

Bribery

Type	Key Feature
Official	Public official
Commercial	Private sector
Illegal gratuity	Reward after decision

VII. GLOBAL ANTI-CORRUPTION (COMPARE THIS)

Law	Key Point
FCPA (US)	Foreign public officials only; allows facilitation
UK Bribery Act	Covers private bribery; NO facilitation
OECD Convention	Supply-side bribery
UNCAC	Prevention, criminalization, asset recovery

VIII. WHAT CFE EXAMS LOVE TO ASK

✅ **Intent vs negligence**
✅ **Red flag identification**
✅ **Proper detection procedure**
✅ **Civil vs criminal thresholds**
✅ **Control failures vs fraud**
✅ **Vendor master file risks**

🔐 **FRAUD EXAMINERS MANUAL – SECURITIES FRAUD & MONEY LAUNDERING**

High-Retention CFE Reviewer (Condensed)

I. SECURITIES – CORE CONCEPTS

A. What Is a Security?

A **security** generally includes:

- **Equity** (stocks, shares)
- **Debt** (bonds, debentures, notes)

- **Derivatives** (futures, options)
- **Investment contracts** (Howey test)

📌 Definition varies by jurisdiction, but substance > form.

B. Traditional Securities

Type	Key Point
Stocks	Ownership interest; profits via dividends & appreciation
Bonds	Debt obligation; fixed payments + maturity
CDs	Bank-issued debt; fixed return; early withdrawal penalty

II. DERIVATIVES (HIGH-RISK / HIGH-EXAM VALUE)

A. Futures

- **Obligation** on both buyer & seller
- Used for **hedging** or **speculation**
- Traded on exchanges
- Settled via:
    - Physical delivery, or
    - **Cash settlement**

Key mechanics

- Margin = **performance bond**, not down payment
- Marked-to-market daily
- Clearinghouse removes counterparty risk

B. Options

Aspect	Futures	Options
Obligation	Buyer & seller	Seller only
Buyer's status	Must perform	Right, not obligation
Result if unused	Delivery or cash	**Expires worthless**

Option Types

- Call = right to **buy**
- Put = right to **sell**
- American (exercise anytime)
- European (exercise at expiry)

Option value =

- Intrinsic value (in-the-money only)
- Time value (complex; Black-Scholes)

C. OTC Derivatives (Major Risk Area)

- Not standardized
- Not centrally cleared
- **High counterparty credit risk**
- Often customized → audit & valuation risk

III. INVESTMENT CONTRACTS (VERY EXAMINABLE)

A. The Howey Test (ALL FOUR REQUIRED)

1. Investment of money
2. Common enterprise
3. Expectation of profits
4. Profits from **efforts of others**

👉 If YES → **Security**, even if called something else

B. Common Investment Contracts

- Ponzi schemes
- Pyramid schemes
- Prime bank notes
- Precious metals schemes
- Viatical settlements (often unclear)
- Limited partnerships

- Joint ventures
- Hedge funds
- Promissory notes

IV. CLASSIC SECURITIES FRAUD SCHEMES

A. Ponzi Schemes

- New investor funds pay old investors
- No real profits
- Collapse is inevitable

🚩 Guaranteed high returns
🚩 Consistent profits regardless of market

B. Illegal Pyramid Schemes

- Rewards from recruiting, not product sales
- **Not all pyramids are securities**, but many qualify as investment contracts

---

C. Prime Bank Note Schemes

- Fake high-yield instruments
- Heavy secrecy + NDAs
- Reference to IMF / big banks for fake credibility

V. PARTNERSHIPS & BUSINESS STRUCTURES

Structure	Is it a Security?
General Partnership	❌ Usually no (active role)
Limited Partnership	✅ Usually yes
Joint Venture	Depends on investor control

📌 **Substance test**: Are investors passive?

VI. OIL / GAS / MINERAL SCAMS (RED-FLAG HEAVY)

Common Misrepresentations

- Inflated drilling costs
- Fake leases
- Overstated production forecasts
- Disproportionate royalties
- Oversold ownership interests

📌 Case study: **Bre-X scandal** → sampling fraud + jurisdictional limits

---

VII. HEDGE FUNDS – FRAUD RISK AREAS

Why vulnerable

- Complex strategies
- Fee incentives (2 & 20)
- Limited transparency

Common Fraud Types

- Asset theft
- Portfolio overvaluation
- Insider trading
- Late trading

Red Flags

- Resistance to due diligence
- No independent service providers
- Background misrepresentation

VIII. PROMISSORY NOTES – SECURITY OR NOT?

Presumption

✅ **Assumed to be a security** unless clearly otherwise

Resemblance Test

1. **Motive & expectation** (investment vs loan)
2. **Plan of distribution** (common trading?)
3. **Other regulation** (banking, mortgage laws?)

IX. SECURITIES REGULATION – PURPOSE

Primary objectives

- Investor protection
- Fair & transparent markets
- Reduction of systemic risk

Major Regulators (Illustrative)

- SEC (US)
- FCA (UK)
- ESMA (EU)
- IOSCO (Global standard-setter)

📌 IOSCO Principles = **global benchmark** (not binding)

X. SECURITIES FRAUD BY REGISTERED PERSONS

A. Professional Misconduct

- Unsuitable recommendations
- Failure to disclose risks
- Conflict of interest

B. Churning (EXAM FAVORITE)

- Excessive trading for commissions

Indicators

- Turnover > 300%
- High cost-to-equity ratio
- Broker has discretion

C. Selling Away

- Selling unapproved securities outside firm
- Often targets elderly / retail investors

D. Market Manipulation

- Artificial price inflation
- Common with penny & micro-cap stocks

E. Insider Trading

- Trading on **material, nonpublic information**
- Includes front-running and tipping

XI. MATERIAL MISREPRESENTATIONS & OMISSIONS

Material =

Would a reasonable investor care?

✓ False approval claims
✓ Hidden criminal history
✓ Concealed risks

XII. MONEY LAUNDERING – CORE FRAMEWORK

Definition

Disguising the **source, control, ownership**, or **nature** of illicit funds.

Three Stages

1. **Placement** – introduce cash
2. **Layering** – obscure trail
3. **Integration** – re-enter economy

XIII. COMMON LAUNDERING METHODS (HIGH-YIELD)

- Structuring (smurfing)
- Front businesses
- Trade-based laundering
- Shell companies
- Casinos

- Insurance products
- Digital currencies
- Alternative remittance systems (hawala)

XIV. FATF FRAMEWORK (VERY EXAMINABLE)

FATF Recommendations

Require:

- Risk-based AML programs
- Customer Due Diligence (CDD)
- Suspicious Activity Reporting (SAR/STR)
- Beneficial ownership transparency

Financial Institutions Must:

- Identify customers & beneficial owners
- Monitor transactions
- Report suspicious activity
- Maintain records

XV. KEY AML RED FLAGS (MEMORIZE LIST TYPE)

- Structuring deposits below thresholds
- Third-party payments
- Use of shell entities
- Cash-heavy businesses
- Rapid policy cancellations
- Over/under-invoicing in trade

XVI. INVESTIGATIVE TAKEAWAYS (CFE PRACTICAL)

- Substance over labels
- Follow the money
- Check licensing status

- Verify disclosures vs reality
- Map scheme to **definitions + tests**
- Always link to:
    - **Security?**
    - **Registration?**
    - **Fraud indicators?**

CFE REVIEWER – TAX FRAUD, LEGAL RIGHTS & EVIDENCE

(Fraud Examiners Manual – High-Yield Summary)

I. TAX FRAUD – CORE CONCEPTS

Definition

Tax Fraud
Intentional acts to defraud the government of owed taxes through **false claims or concealment**.

Tax Evasion vs. Tax Avoidance

Item	Tax Evasion	Tax Avoidance
Nature	Illegal	Legal
Method	Fraudulent actions	Legitimate deductions/credits
Key Test	**Intent**	Compliance with law

✅ **Exam Key:** *Intent* determines evasion vs. avoidance.

II. INTENT & WILLFULNESS (VERY HIGH-YIELD)

Willfulness

- Voluntary, intentional violation of a known legal duty
- Required for **criminal liability**
- **Good-faith misunderstanding negates willfulness**

Conduct Showing Willfulness

Memorize: **"DF-DCCAMM"**

- **D**ouble books
- **F**alse entries/documents

- **D**estroying records
- **C**oncealing assets
- **C**overing income sources
- **A**voiding normal records
- **M**oving assets offshore
- **M**isleading conduct

⚠️ Even without willfulness → **civil penalties may still apply**

III. COMMON INDICATORS OF TAX FRAUD

Memorize: **"MAD-SODF"**

- **M**isrepresentation
- **A**rtifice
- **D**ouble books
- **S**ecret bank accounts
- **O**verstated deductions
- **D**isguised transactions
- **F**ictitious transactions

IV. TYPES OF TAX EVASION SCHEMES

1. Income & Wealth Tax Evasion

Examples:

- Not filing required returns
- Understating income/wealth
- Fake asset transfers
- Failure to withhold employee taxes
- Undisclosed foreign accounts
- False source of income jurisdiction

2. Falsifying Tax Deductions

- Fake expenses / non-existent employees
- Inflated invoices

- False qualifications (e.g., dependents)
- Misclassifying non-deductible expenses

3. Tax Credit Schemes

- Fake eligibility
- Abuse of refundable credits

4. Consumption Tax Schemes (VERY TESTED)

Includes:

- **Sales Tax**
- **VAT**
- **Excise Tax**

Common schemes:

- Unrecorded sales
- Cash skimming
- False export transactions
- **Missing trader schemes**
- **Carousel VAT fraud**
- Smuggling to avoid excise tax

V. EVIDENCE OF TAX FRAUD

Direct Evidence

- Unexplained bank deposits
- False documents
- False explanations
- Illegal business participation
- False claims (e.g., exemptions)

Circumstantial Evidence

- Assets/expenditures > known income
- Income exceeding deposits

✅ **Exam Tip:**
Most tax fraud cases rely **primarily on circumstantial evidence**

VI. DEFENSES TO TAX EVASION

Common Valid Defenses

- **No Tax Deficiency** (best defense)
- **Lack of Willfulness**
- **Avoidance, Not Evasion**
- **Objectively Reasonable Position**
- **Reliance on Attorney/Accountant**
- **Mental Illness**
- **Innocent Spouse**
- **Statute of Limitations**

Ineffective Defenses

- Death of taxpayer
- Bankruptcy
- Amending returns after fraud

VII. FRAUD SCHEMES TARGETING TAXPAYERS

Examples:

- **Tax identity theft**
- Fake refund claims
- Fake dependents
- Government impersonation (phishing, calls, emails)

✅ Victims often discover fraud after **rejected returns**

VIII. INDIVIDUAL RIGHTS DURING EXAMINATIONS (VERY TESTED)

Employee Duties

- Duty to cooperate (reasonable requests only)
- Duty to preserve evidence (litigation hold)

Employee Rights

- Contractual rights

- Whistleblower protections
- Privacy rights (vary by jurisdiction)

⚠️ **Private employers can violate employee rights**

IX. RIGHT TO REMAIN SILENT

Applies When:

✅ Questioned by **government authorities**

Does NOT Apply:

❌ Internal investigations by private employers
→ Employee can be terminated for refusal

⚠️ Exception:
If employer acts **with or at direction of police**, rights may attach

---

X. SEARCH & SEIZURE

Key Principle

Protection applies **only against government actions**

Search Warrants

- Generally required for government searches
- Not required for private parties

Exceptions

- Consent searches
- Evidence in plain view

XI. DEFAMATION & PRIVACY (EXAM FAVORITES)

Defamation Elements

1. Untrue statement of fact
2. Published to a third party
3. Unprivileged occasion
4. Damage to reputation

✅ **Truth is an absolute defense**

Invasion of Privacy

Two common forms in fraud exams:

- **Intrusion into private matters**
- **Public disclosure of private facts**

XII. DATA PRIVACY – INTERNATIONAL FRAME

OECD Privacy Principles (memorize list)

- Lawfulness
- Purpose limitation
- Data minimization
- Accuracy
- Access
- Security
- Retention limits

GDPR (EU)

Key rights:

- Lawful basis
- Notice
- Consent
- Access
- Erasure
- Portability
- Breach notification (72 hours)

💡 **Applies even to non-EU companies handling EU data**

XIII. BASIC PRINCIPLES OF EVIDENCE

Types of Evidence

- **Testimonial**
- **Real**
- **Demonstrative**

Direct vs. Circumstantial

- Fraud intent usually proven **circumstantially**

Common Law vs. Civil Law

Topic	Common Law	Civil Law
Evidence Rules	Strict	Flexible
Juries	Common	Rare
Hearsay	Restricted	Generally allowed
Character Evidence	Limited	Allowed

XIV. HEARSAY – KEY EXCEPTIONS (MEMORIZE)

- Admissions by party opponent
- Business records
- Statements against interest
- Present sense impressions
- Excited utterances
- State of mind
- Medical diagnosis
- Recorded recollections

XV. EXAM POWER TIPS

✅ Tax fraud = **INTENT + ACT**
✅ Criminal vs. civil hinges on **willfulness**
✅ Private employer investigations ≠ constitutional rights
✅ Evidence errors = top defense strategy
✅ GDPR applies **extra-territorially**

Law: Evidence, Privileges, and Testifying

CFE Exam–Optimized Structured Review

I. BASIC PRINCIPLES OF EVIDENCE

A. Printed Materials & Learned Treatises

- Printed materials supporting **technical or professional assertions** are admissible if:
    - **Generally relied upon** by the public or professionals
- **Learned treatises**:
    - Admissible to **support or attack expert testimony**
    - Must be established as a **reliable authority**
    - Some jurisdictions allow use **only during cross-examination**

Exam focus: Treatises ≠ automatically admissible everywhere

B. Refreshing a Witness's Memory

- Witness may refer to **notes or writings** to refresh memory
- Conditions:
    - Witness must testify **independently afterward**
    - Writing becomes admissible **only if opposing counsel requests it**

C. Other Hearsay Exceptions

- Includes:
    - **Dying declarations**
    - **Ancient documents**
- Courts may admit hearsay if deemed **trustworthy**
- Trustworthiness is the **core principle**

D. Hearsay in Civil Law Systems

- No strict hearsay rule
- Judges assess **weight**, not admissibility
- Hearsay is **freely admitted**

Key contrast: Common law = exclusionary; civil law = discretionary

---

II. CHAIN OF CUSTODY

A. Purpose

Establishes:

1. **Who possessed evidence**
2. **What was done with it**

Goal: Prove **no material alteration**

B. What Must Be Documented

- Who had custody
- When/how received
- Storage and handling
- Any changes
- How custody transferred

C. Gaps or Mishandling

- Do NOT automatically bar admissibility
- Affect **weight**, not **admissibility**
- Courts allow evidence with **disclosure of deficiencies**

D. Digital Evidence

Minimum requirements:

- Identify each item
- Document source, authorization, location, date/time
- Maintain continuous custody record

Exam trap: Digital evidence = higher custody sensitivity

III. IMPEACHMENT OF WITNESSES

A. Definition

Impeachment = challenging **credibility or reliability**

Not applicable in inquisitorial systems (no cross-examination)

B. Common Methods

- Bias or self-interest

- Impaired perception
- Prior inconsistent statements
- Criminal convictions
- Reputation for untruthfulness

C. Criminal Convictions (U.S. FRE 609)

Admissible if:

- Crime involved **dishonesty or false statement**
- Or felony (generally within **10 years**)

D. Collateral Matters Rule

- If matter is **collateral**:
    - Examiner must accept witness's answer
    - No extrinsic evidence allowed

IV. PRIVILEGES AND PROTECTIONS

A. General Rule

- Privileged evidence is:
    - **Undiscoverable**
    - **Inadmissible**
- Judges/juries must **disregard** it

B. Legal Professional Privileges (Global)

Names vary:

- US – Attorney-Client
- UK – Legal Advice
- Canada – Solicitor-Client
- EU – Legal Professional

Requirements:

1. Attorney–client communication

2. Purpose = legal advice
3. Intended confidentiality

C. Waiver of Privilege

Occurs if:

- Client testifies
- Attorney testifies at client's request
- Disclosure to third parties
- Inadvertent disclosure

Sharing with **legal consultants** (e.g., CFEs) ≠ waiver if for legal advice

---

D. Crime–Fraud Exception

- Privilege does **NOT** apply to communications involving:
    - Ongoing or future crime/fraud

E. Work-Product Doctrine (U.S.)

Protects:

- Materials prepared **in anticipation of litigation**

Does NOT protect:

- Underlying **facts**
- Documents created for **ordinary business purposes**

May be overridden if:

- Opposing party shows **substantial need**
- But **mental impressions** are absolutely protected

F. Other Privileges

- Litigation privilege (UK/Canada)
- Self-evaluation privilege (limited, weak)
- Marital / spousal privilege (varies by country)
- Parent-child privilege (mostly civil law)

- Informant privilege (law enforcement only)
- Accountant-client privilege (limited)

CFE exam alert: Privileges are **jurisdiction-specific**

V. TESTIFYING

A. Types of Testimony

1. **Lay (Fact) Testimony**
    - Firsthand observations
    - Limited opinions (common sense only)
2. **Expert Testimony**
    - Based on specialized knowledge
    - Helps fact finder understand complex issues

B. Information vs Evidence

- **Information** = anything learned
- **Evidence** = what is admitted at trial

Non-admissible info can still lead to admissible evidence

C. Lay Opinions Allowed For:

- Appearance
- Identity
- Conduct
- Emotional state (limited)
- Sound, size, distance

Not allowed:

- Scientific or technical conclusions

VI. EXPERT WITNESSES

A. Expert Roles

- **Testifying expert**

- **Consulting expert**

B. Expert Functions (Matson)

1. Establish facts
2. Interpret facts
3. Critique opposing expert
4. Define professional standards

C. Qualifying an Expert (Common Law)

Judge assesses:

1. Qualifications
2. Relevance
3. Reliability

Education ≠ required
Experience alone may qualify

D. Expert Reports

Typically include:

- Opinions and basis
- Facts/data considered
- Exhibits
- Qualifications
- Prior testimony
- Compensation

E. ACFE Ethics – Critical Rule

CFEs must NOT opine on guilt or innocence

Allowed:

- Describe evidence
- Explain fraud indicators

- Recommend action

VII. EXAM STRATEGY SUMMARY

High-Yield Takeaways

- **Trustworthiness** governs hearsay exceptions
- **Chain of custody affects weight first, admissibility second**
- **Privileges ≠ universal**
- **Digital evidence heightens custody risk**
- **Experts explain facts — they do not decide guilt**
- **Jurisdiction matters everywhere**

PLANNING, EVIDENCE, & INTERVIEWS (Fraud Examination Core)

I. PLANNING A FRAUD EXAMINATION

1. Selecting the Investigation Team — *Know the DON'TS*

Do **NOT** select team members who:

- Are friends / repayment of favors
- Have negative attitudes
- Have conflicts of interest
- Are closely related to the suspect or complainant
- Lack discretion or restraint
  ✅ Independence and objectivity are critical

💡 **Exam tip:** Independence ≠ internal vs external — it's about **lack of vested interest**

---

2. Investigation Leader

The leader must:

- Have investigative + legal/compliance knowledge
- Be **independent** of the area affected
- Have authority, access, and resources
- Be chosen based on **severity of allegation**

---

3. Understanding the Organization

Investigators must understand:

- Industry, competition, culture
- Cash flows, procurement, vendors/customers
- Org chart, key roles, policies
- Recordkeeping systems
  ➡️ Purpose: **risk assessment & investigation focus**

---

4. Investigation Planning (VERY EXAM-HEAVY)

An investigation plan must:

1. Be **collaborative**
2. Start early and be **continuously updated**
3. Be **case-specific**, but guided by a standard framework

Core Planning Elements (MEMORIZE):

- What is known
- Goals
- Who to inform
- Scope
- Time frame
- Law enforcement involvement
- Roles & tasks
- Operational issues
- Case plan
- Resources
- Organizational readiness

---

5. Key "WHAT IS KNOWN" Questions

Before starting, answer:

- Nature & period of suspected fraud
- Who is involved / affected

- Prior investigations?
- Compliance history?
- Profitability/growth anomalies?
- Fraud policy exists?
- Expected report type & budget

📌 **Exam cue:** This section is tested as **"initial assessment"**

---

6. Goals of the Investigation

Beyond "did fraud occur?", goals may include:

- Prevent further loss
- Preserve evidence
- Recover losses
- Enable disciplinary/criminal action
- Improve controls
- Promote anti-fraud culture
- Protect legal privilege

✅ Goals must be **specific, realistic, measurable**

---

7. Scope of the Investigation

Scope depends on:

- Goals
- Key issues
- Required discretion
- Constraints (time, authority, legal)
- Compliance culture
- Management involvement
- Widespread vs isolated issues
- Government expectations

⚠️ **Expand scope** if compliance program failure is indicated

---

8. Time Frame

- Must have **start & due dates**
- Consider earnings releases & audit committee meetings
- Must be **realistic**

---

9. Law Enforcement Involvement

- Mandatory in some jurisdictions
- If referral is intended → notify **before starting**
- Law enforcement may participate

---

10. Roles & Reporting

- Must clearly define:
    - Authority
    - Responsibilities
    - Reporting lines
      Failure = wasted effort, gaps, faulty results

---

11. Operational Issues (Exam Favorite)

Consider:

- Cross-border data
- GDPR & privacy laws
- Record format differences
- Language & cultural issues
- Remote investigations

💡 GDPR limits processing & transfer of personal data

---

12. Case Plan (COURSE OF ACTION)

Includes:

- Scope

- Goals
- Timeline
- Resources
- Assignments
- Investigation approach

Typical structures:

- Chronological
- Functional
- By team member
- Hierarchical

---

13. Confidentiality (CRITICAL)

Why?

- Prevent evidence destruction
- Avoid retaliation
- Protect reputations
- Preserve investigation integrity

Key actions:

- Limit information
- Avoid alerting the suspect
- Guard case information
- Use privilege where applicable

II. EVIDENTIARY PRIVILEGE (HIGH-YIELD)

Attorney-Client Privilege

- Requires **legal direction/supervision**
- Protects communications, NOT underlying facts
- Cannot be applied retroactively

Work-Product Doctrine

- Materials prepared **in anticipation of litigation**

- Can extend to third-party experts
- Waived if expert testifies

📌 **Exam trap:** Evidence itself is NOT privileged

III. COLLECTING EVIDENCE

1. Types of Evidence (MEMORIZE)

- **Testimonial**
- **Digital**
- **Documentary**

---

2. General Rules for Documents

- Obtain originals when possible
- Minimize handling
- Maintain proper filing & indexing

---

3. Obtaining Documents

- By consent (preferably written)
- If company owns documents → usually accessible
- Otherwise → subpoena or court order

🚫 Never obtain through theft or trespass

---

4. Categories of Evidence

- **Direct** – proves facts directly
- **Circumstantial** – proves by inference
  ✅ Both are admissible

---

5. Organizing Evidence

- Segregate by transaction or witness
- Key document file
- Database with coding

- Maintain chronology

---

6. Chain of Custody (EXAM ESSENTIAL)

Must document:

- What
- When
- From whom
- Where stored

Purpose:

- Authenticity
- Evidence integrity

---

7. Handling Physical Documents

- Use sealed, dated, initialed containers
- Do not staple, fold, or mark originals
- Originals required for forensic testing

---

8. Forensic Document Examination

Common examinations:

- Forged signatures
- Alterations
- Indented writings
- Ink & paper comparison
- Counterfeits

Fraud examiners:

- Are NOT experts
- Must know **when to call one**

---

9. Handwriting & Forgeries

Types:

- Simulated/traced
- Freehand
- Autoforgery

Three outcomes:

- Identification
- Non-identification
- Inconclusive

---

10. Fingerprints

- **Latent** vs **Patent**
- Porous vs non-porous surfaces
- Never dust paper documents
- Preserve & submit to experts

---

11. Disposal of Evidence

Depends on:

- Privacy laws
- Litigation risk
- Retention policies
- Jurisdiction

IV. INTERVIEW THEORY & APPLICATION

1. Interview Types

- **Information-seeking**
- **Admission-seeking**

---

2. Interview Preparation

- Define objective
- Select interviewer
- Develop outline, not script

- Plan order of witnesses

✅ Least involved → most involved

---

3. Interview Environment

- Private
- Non-restrictive
- In-person preferred
- Remote OK with preparation

---

4. Characteristics of Good Interviewers

- Amiable
- Non-accusatory
- Impartial
- Professional
- Non-threatening

---

5. Legal Risks

- False imprisonment
- Recording consent laws
- Deception limits ➡️ Always consult legal counsel

---

6. PEACE Interview Model (MEMORIZE)

- **P**lanning
- **E**ngage & Explain
- **A**ccount / Clarify
- **C**losure
- **E**valuation

---

7. Cognitive Interview Technique

Two phases:

1. Narrative
2. Specific details

Key tools:

- Reconstruct environment
- Change order
- Change perspective

---

8. Question Types

- Introductory
- Informational
- Assessment
- Admission-seeking
- Closing

Avoid:

- Double negatives
- Complex questions
- Accusatory language

---

9. Indicators of Deception

⚠️ **Stress ≠ lying**

Look for:

- Speech changes
- Weak denials
- Avoidance of emotive words
- Over-friendliness
- Body language clusters

✅ **Never rely on one indicator alone**

✅ **FINAL CFE EXAM ADVICE**

This block of content is tested through:

- **Scenario judgment**
- **Best-next-step questions**
- **Legal/ethical boundaries**
- **Evidence admissibility**
- **Interview conduct**

FRAUD EXAMINERS MANUAL – SOURCES OF INFORMATION & DATA ANALYTICS

🧠 **CFE-Optimized Master Summary (High-Yield)**

I. INTERNET & OPEN-SOURCE SEARCHING (OSINT)

A. Search Engine Techniques

Key Principle: No single search engine is sufficient.

Advanced Operators (Bing & Google):

- site: limit to domain
- filetype: specific format (pdf, xls)
- "quoted phrase" exact match
- - exclude terms
- inbody: term must appear in content
- inanchor: term appears in backlinks
- ip: sites hosted at same IP

✅ **Exam Tip:** Questions often test **why multiple engines matter** → indexing differs.

B. Deep Web vs Dark Web

Aspect	Deep Web	Dark Web
Indexed by Google?	❌	❌
Access	Normal browser	Special browser (Tor)
Purpose	Databases, archives	Anonymity
Risk	Low	High

✅ **Key rule:** Dark web = **neutral tool**, but **high legal & cyber risk**

✅ Access requires **IT approval + security controls**

C. Internet Archives

Wayback Machine

- View deleted or changed websites
- Identify **what was removed** (high probative value)

II. PUBLIC RECORDS & DATABASES

A. Sources of Public Records

1. **Government repositories**
2. **Public record vendors**
3. **Investigative service companies**

Vendor Advantages

- Speed
- Cross-jurisdiction coverage

Key Limitation

Vendor data may be **incomplete, outdated, or inaccurate**

✅ **Always verify material records with original sources**

B. Public Record Search Limitations (Highly Tested)

- No actual document copies
- Jurisdictional gaps
- Abstracted data
- Legal restrictions (e.g., **FCRA**)

✅ **Always consult legal counsel** before accessing:

- Credit data
- Employment background info
- Sensitive personal records

III. SOCIAL MEDIA AS EVIDENCE

A. Uses in Investigations

- Lifestyle red flags
- Hidden assets
- Associations
- Travel patterns
- Employer/business intelligence

B. Legal & Privacy Rules (VERY EXAM-HEAVY)

✅ Allowed:

- Publicly visible information

❌ Prohibited:

- Pretexting
- Password cracking
- Social engineering
- Accessing private content without authority

✅ Courts may:

- Compel production via subpoena
- Order disclosure (rare, extreme)

C. Evidence Collection Best Practices

To preserve **authenticity & admissibility**:

- Screenshots
- Screen recordings
- PDF captures
- Specialized tools that **preserve metadata**

✅ **Chain of custody + contemporaneous documentation required**

IV. BACKGROUND & DUE DILIGENCE SEARCHES

A. Core Areas

- Business reputation
- Litigation history

- Criminal records
- Credit capacity
- Ownership & control (“family tree”)

B. Employment Background Checks

Common searches (where legal):

- Criminal court records
- Civil cases
- Licenses
- Education & employment verification
- Driving records

✅ **Mandatory background checks** apply to:

- Financial industry
- Securities
- Insurance
- Security roles

V. ASSET & PEOPLE LOCATIONS (HIGH-VALUE)

Locating People

- Credit header searches
- Past addresses
- Voter registration
- Bankruptcy, liens, judgments
- DBA filings

Locating Hidden Assets

- Property records
- Secured transactions
- Vehicle registrations
- Professional licenses
- Divorce records

- Business filings

✅ **Combine public records + social media + lifestyle analysis**

VI. DATA ANALYTICS IN FRAUD EXAMINATIONS

A. Structured vs Unstructured Data

Structured	Unstructured
Ledgers	Emails
Transactions	Chat logs
Payroll	Documents

✅ Modern fraud detection = **both**

B. Data Analysis Lifecycle (MEMORIZE)

1. **Planning**
2. **Preparation**
3. **Testing & interpretation**
4. **Post-analysis monitoring**

✅ **Predication required** before investigations
✅ Analytics can establish predication without accusations

C. Core Fraud Analytics Techniques

- Sorting
- Gap tests
- Duplicate detection
- Benford's Law
- Regression & correlation
- Stratification
- Pivot tables
- Join & matching
- Fuzzy matching

- Compliance checks

D. Benford's Law (VERY HIGH-YIELD)

- Applies to **natural numbers**
- Flags fabricated amounts
- Not valid for:
    - ID numbers
    - Assigned values
    - Artificial pricing

First digit "1" ≈ **30%**, "9" ≈ **<5%**

✅ Used for:

- Shell companies
- Bid splitting
- Journal entry fraud

E. Scheme-Specific Analytics

Asset Misappropriation

- Ghost employees
- Duplicate bank accounts
- Address overlaps

Corruption

- Round-dollar payments
- Just-below-approval thresholds
- Vendor-employee matches

Financial Statement Fraud

- Suspicious journal entries
- Odd posting times
- Reversals & estimates

VII. ADVANCED & EMERGING ANALYTICS

- Machine learning
- Predictive analytics
- AI-based transaction scoring
- Continuous monitoring
- Textual analytics (fraud keywords)
- Sentiment analysis
- Visual analytics (heat maps, link analysis)

✅ **Link analysis** is critical for:

- Money laundering
- Shell companies
- Collusion detection

VIII. DIGITAL FORENSICS (FOUNDATIONAL KNOWLEDGE)

A. Key Distinction

Digital Investigation	Digital Forensics
Leads examination	Evidence recovery
CAE/fraud examiner	Specialized expert

✅ Roles should **not be combined**

B. Digital Evidence Principles

- Extremely volatile
- Easy to alter
- Integrity must be preserved
- Improper handling → inadmissible

C. Common Digital Evidence Locations

- Computers & servers
- Smartphones
- Cloud storage

- Printers & copiers
- Removable media
- Networks

D. Forensic Process (MEMORIZE)

1. Planning
2. Seizing
3. Imaging
4. Processing
5. Analysis
6. Reporting/Testifying

✅ **Never analyze original media** ✅ Always use **forensic copies**

IX. CFE EXAM PRO TIPS 🎯

- Watch for **privacy vs access** distinctions
- Assume **legal counsel involvement** whenever rights may be affected
- Expect scenario-based questions combining:
    - Public records + analytics
    - Social media + admissibility
    - Data anomalies + predication

DIGITAL FORENSICS & TRACING ILLICIT TRANSACTIONS

(Fraud Examiners Manual – Structured Examiner Version)

PART I — DIGITAL FORENSICS (Big Picture)

Objective

Preserve, collect, analyze, and present **digital evidence** in a manner that:

- Maintains **integrity**
- Survives **legal challenge**
- Supports **expert testimony**

A. DIGITAL EVIDENCE SEIZURE — CORE RULES

1. Document First, Touch Last

Always record:

- Date/time of seizure
- System **state**: ON / OFF / STANDBY
- Open applications (if ON)
- Serial numbers, make/model
- Physical connections
- Surroundings + photos
- Start **chain of custody immediately**

✅ *Failure here = evidentiary vulnerability*

---

2. If Computer Is OFF → LEAVE IT OFF

Why:

- Booting alters timestamps
- OS writes to disk automatically
- Evidence becomes tainted

Rule:

❌ Never power on an OFF system during seizure

---

3. Inspect for Traps

- Intrusion detection software
- Self-destruct mechanisms
- Malware triggers

B. LIVE DATA COLLECTION (VOLATILE DATA)

What is Volatile Data?

Data lost when power/network is removed:

- RAM
- Encryption keys

- Running processes
- Network connections

When Live Collection Is Appropriate

✓ Memory-resident malware
✓ Encryption keys in RAM
✓ System is mission-critical
✓ Attack in progress
✓ Suspect actively using system

🚨 **Only trained forensic examiners may do this**

Order of Volatility (MOST → LEAST)

1. CPU registers/cache
2. RAM
3. Virtual memory (swap/page files)
4. Network connections
5. Running processes
6. Local disks
7. Backup media
8. Archived media (USB, CD, externals)

Basic Live Collection Steps (Exam Gold)

1. Log every action
2. Photograph screen
3. Identify OS
4. Note system vs actual time
5. Dump RAM
6. Check for disk/file encryption
7. Collect other OS volatile data
8. Decide seizure method
9. Complete forensic report

C. SHUTDOWN METHODS (Running Systems)

Hard Shutdown ✅ (Preferred if no live acquisition)

- Unplug power directly
- Preserves swap/temp files

Graceful Shutdown ❌ (Risky)

- Deletes temp files
- Erases swap file
- Removes malware traces

General Rule:

If running and no live collection → **Pull the plug**

D. SECURING DIGITAL EVIDENCE

Mandatory Controls

- Disconnect all devices
- Prohibit access
- Maintain chain of custody
- Use write-blockers
- Proper packaging
- Encrypt sensitive data

Chain of Custody Must Show

- What item
- From whom
- When/where received
- Who accessed it
- Continuous control

⚠ Gaps = case weakness

Write-Blocking Devices

- **Hardware**: Blocks all write commands
- **Software**: Filters prohibited requests

✅ Prevents alteration during imaging/analysis

E. IMAGING & ANALYSIS

Imaging Rules

- Never analyze original media
- Always image first
- Verify image integrity (hashes)

Imaging Steps

1. Acquire original media
2. Create forensic image
3. Verify image

Processing (Data Culling)

Reduce volume while preserving integrity via:

- Keyword searches
- Deduplication
- Date filtering
- File-type filtering

Analysis Focus

Look for:

- **Inculpatory evidence**
- **Exculpatory evidence**

Always preserve integrity and document methodology.

F. CLOUD & MOBILE FORENSICS — KEY RISKS

Cloud Forensics Challenges

- No physical access

- Jurisdiction issues
- Limited logs/metadata
- Data commingling
- Chain of custody gaps

✅ Contracts & SLAs matter for forensic readiness

Mobile Forensics Phases

1. Plan
2. Seize
3. Extract
4. Analyze
5. Document
6. Report/Testify

Golden Rules

- Preserve integrity
- Maintain audit trail
- Only competent personnel

PART II — TRACING ILLICIT TRANSACTIONS

A. TRACING: CORE DEFINITION (EXAM FAVORITE)

Tracing =

Identifying **what happened to property**,
where proceeds went, and
who handled or received them

B. GENERAL TRACING PROCESS

1. Collect information
2. Profile the subject
3. Review leads
4. Trace transactions

5. Evaluate recovery options

C. SUBJECT PROFILING

Financial Profile

- Income
- Assets
- Liabilities
- Expenses
- Net worth trends

Behavioral Profile

- Lifestyle indicators
- Spending habits
- Travel
- Associates
- Visible wealth vs income

🚩 Lifestyle > Income = red flag

D. DIRECT VS INDIRECT METHODS (CRITICAL)

---

1. DIRECT METHOD

Uses actual transaction records:

- Bank statements
- Checks
- Wires
- Loan documents
- Credit cards

✅ Strongest evidence
❌ Not always available

---

2. INDIRECT METHODS (Circumstantial Proof)

Used when:

- Records missing/incomplete
- Cash-based operations
- Lifestyle exceeds income

E. THREE INDIRECT METHODS (MEMORIZE)

---

1. Asset Method (Net Worth)

Formula

Assets – Liabilities = Net Worth

Net Worth Increase

+ Living Expenses

– Known Income

= Funds from Unknown Sources

✅ Best when suspect accumulated assets

---

2. Expenditures Method

Total Expenditures

– Known Sources

= Unknown Income

✅ Best when money spent on consumables
(travel, gambling, lifestyle)

---

3. Bank Deposit Analysis

Total Deposits

– Transfers

+ Cash Expenditures

– Known Income

= Unknown Sources

✅ Best when income mostly banked

F. COMMON RECORDS TO EXAMINE

- Bank statements
- Canceled checks
- Wire transfers
- Deposit tickets
- Credit card statements
- Loan & mortgage files
- Brokerage records
- Safe deposit boxes
- FIU reports (SARs/CTRs)
- Cryptocurrency exchange records

G. COMMON ASSET-HIDING METHODS (EXAM LIST)

- Cash hoarding
- Third-party names
- Shell companies
- Offshore accounts
- Cryptocurrency
- Trusts
- Overpaying taxes
- Paying down debt
- Prepaid cards
- Insurance products
- Real estate via nominees

H. CRYPTOCURRENCY — KEY POINTS

- Transactions are **pseudonymous**, not anonymous
- Public blockchains = traceable
- Exchanges & wallets subject to KYC/CDD

- Bank statements often reveal crypto activity

✅ Legal process usually required

I. RECOVERY & LEGAL AVENUES

- Civil discovery
- Subpoenas
- Court orders
- Mutual Legal Assistance (criminal)
- Letters rogatory
- Asset forfeiture actions

🧠 **EXAM MEMORY ANCHORS**

- **OFF stays OFF**
- **Integrity over speed**
- **Chain of custody = lifeline**
- **Lifestyle > income = investigate**
- **Direct if possible, indirect if not**
- **Asset, Expenditure, Deposit → know all three**

DIGITAL FORENSICS & TRACING ILLICIT TRANSACTIONS

(Fraud Examiners Manual – Structured Examiner Version)

PART I — DIGITAL FORENSICS (Big Picture)

Objective

Preserve, collect, analyze, and present **digital evidence** in a manner that:

- Maintains **integrity**
- Survives **legal challenge**
- Supports **expert testimony**

A. DIGITAL EVIDENCE SEIZURE — CORE RULES

1. Document First, Touch Last

Always record:

- Date/time of seizure
- System **state**: ON / OFF / STANDBY
- Open applications (if ON)
- Serial numbers, make/model
- Physical connections
- Surroundings + photos
- Start **chain of custody immediately**

✅ *Failure here = evidentiary vulnerability*

---

2. If Computer Is OFF → LEAVE IT OFF

Why:

- Booting alters timestamps
- OS writes to disk automatically
- Evidence becomes tainted

Rule:

❌ Never power on an OFF system during seizure

---

3. Inspect for Traps

- Intrusion detection software
- Self-destruct mechanisms
- Malware triggers

B. LIVE DATA COLLECTION (VOLATILE DATA)

What is Volatile Data?

Data lost when power/network is removed:

- RAM
- Encryption keys
- Running processes
- Network connections

When Live Collection Is Appropriate

✓ Memory-resident malware
✓ Encryption keys in RAM
✓ System is mission-critical
✓ Attack in progress
✓ Suspect actively using system

🚨 **Only trained forensic examiners may do this**

Order of Volatility (MOST → LEAST)

1. CPU registers/cache
2. RAM
3. Virtual memory (swap/page files)
4. Network connections
5. Running processes
6. Local disks
7. Backup media
8. Archived media (USB, CD, externals)

Basic Live Collection Steps (Exam Gold)

1. Log every action
2. Photograph screen
3. Identify OS
4. Note system vs actual time
5. Dump RAM
6. Check for disk/file encryption
7. Collect other OS volatile data
8. Decide seizure method
9. Complete forensic report

C. SHUTDOWN METHODS (Running Systems)

Hard Shutdown ✅ (Preferred if no live acquisition)

- Unplug power directly
- Preserves swap/temp files

Graceful Shutdown ❌ (Risky)

- Deletes temp files
- Erases swap file
- Removes malware traces

General Rule:

If running and no live collection → **Pull the plug**

D. SECURING DIGITAL EVIDENCE

Mandatory Controls

- Disconnect all devices
- Prohibit access
- Maintain chain of custody
- Use write-blockers
- Proper packaging
- Encrypt sensitive data

Chain of Custody Must Show

- What item
- From whom
- When/where received
- Who accessed it
- Continuous control

⚠ Gaps = case weakness

Write-Blocking Devices

- **Hardware**: Blocks all write commands
- **Software**: Filters prohibited requests

✅ Prevents alteration during imaging/analysis

E. IMAGING & ANALYSIS

Imaging Rules

- Never analyze original media
- Always image first
- Verify image integrity (hashes)

Imaging Steps

1. Acquire original media
2. Create forensic image
3. Verify image

Processing (Data Culling)

Reduce volume while preserving integrity via:

- Keyword searches
- Deduplication
- Date filtering
- File-type filtering

Analysis Focus

Look for:

- **Inculpatory evidence**
- **Exculpatory evidence**

Always preserve integrity and document methodology.

F. CLOUD & MOBILE FORENSICS — KEY RISKS

Cloud Forensics Challenges

- No physical access
- Jurisdiction issues
- Limited logs/metadata

- Data commingling
- Chain of custody gaps

✅ Contracts & SLAs matter for forensic readiness

Mobile Forensics Phases

1. Plan
2. Seize
3. Extract
4. Analyze
5. Document
6. Report/Testify

Golden Rules

- Preserve integrity
- Maintain audit trail
- Only competent personnel

PART II — TRACING ILLICIT TRANSACTIONS

A. TRACING: CORE DEFINITION (EXAM FAVORITE)

Tracing =

Identifying **what happened to property**,
where proceeds went, and
who handled or received them

B. GENERAL TRACING PROCESS

1. Collect information
2. Profile the subject
3. Review leads
4. Trace transactions
5. Evaluate recovery options

C. SUBJECT PROFILING

Financial Profile

- Income
- Assets
- Liabilities
- Expenses
- Net worth trends

Behavioral Profile

- Lifestyle indicators
- Spending habits
- Travel
- Associates
- Visible wealth vs income

🚩 Lifestyle > Income = red flag

D. DIRECT VS INDIRECT METHODS (CRITICAL)

---

1. DIRECT METHOD

Uses actual transaction records:

- Bank statements
- Checks
- Wires
- Loan documents
- Credit cards

✅ Strongest evidence
❌ Not always available

---

2. INDIRECT METHODS (Circumstantial Proof)

Used when:

- Records missing/incomplete

- Cash-based operations
- Lifestyle exceeds income

E. THREE INDIRECT METHODS (MEMORIZE)

---

1. Asset Method (Net Worth)

Formula

Assets – Liabilities = Net Worth

Net Worth Increase

+ Living Expenses

– Known Income

= Funds from Unknown Sources

✅ Best when suspect accumulated assets

---

2. Expenditures Method

Total Expenditures

– Known Sources

= Unknown Income

✅ Best when money spent on consumables
(travel, gambling, lifestyle)

---

3. Bank Deposit Analysis

Total Deposits

– Transfers

+ Cash Expenditures

– Known Income

= Unknown Sources

✅ Best when income mostly banked

F. COMMON RECORDS TO EXAMINE

- Bank statements
- Canceled checks
- Wire transfers
- Deposit tickets
- Credit card statements
- Loan & mortgage files
- Brokerage records
- Safe deposit boxes
- FIU reports (SARs/CTRs)
- Cryptocurrency exchange records

G. COMMON ASSET-HIDING METHODS (EXAM LIST)

- Cash hoarding
- Third-party names
- Shell companies
- Offshore accounts
- Cryptocurrency
- Trusts
- Overpaying taxes
- Paying down debt
- Prepaid cards
- Insurance products
- Real estate via nominees

H. CRYPTOCURRENCY — KEY POINTS

- Transactions are **pseudonymous**, not anonymous
- Public blockchains = traceable
- Exchanges & wallets subject to KYC/CDD
- Bank statements often reveal crypto activity

✅ Legal process usually required

I. RECOVERY & LEGAL AVENUES

- Civil discovery
- Subpoenas
- Court orders
- Mutual Legal Assistance (criminal)
- Letters rogatory
- Asset forfeiture actions

🧠 **EXAM MEMORY ANCHORS**

- **OFF stays OFF**
- **Integrity over speed**
- **Chain of custody = lifeline**
- **Lifestyle > income = investigate**
- **Direct if possible, indirect if not**
- **Asset, Expenditure, Deposit → know all three**

Tracing Illicit Transactions, Asset Recovery, and Report Writing

(Fraud Examiners Manual – Investigation Section)

I. TRACING ILLICIT TRANSACTIONS (INTERNATIONAL)

A. Mutual Legal Assistance (MLA)

What it is
A **government-to-government** mechanism to obtain assistance in criminal investigations involving foreign jurisdictions.

Common MLA Requests Include

- Bank account information
- Account documents
- Search warrants
- Subpoenas

- Production orders
- Account monitoring
- Forfeiture/confiscation assistance

Advantages of MLA

- Available **during investigation stage**
- May **not require dual criminality**
- Allows **wide range of assistance**

Grounds for Refusal

- De minimis value
- Prejudice to sovereignty/security
- No reasonable prospect of conviction
- Double jeopardy (already convicted/acquitted)
- Ongoing local proceedings
- Target has immunity

✅ **Exam Tip:**
If a question says *"foreign bank records + government cooperation"*, think **MLA first**.

B. Tools Requiring MLA

- **Account monitoring orders** (real-time surveillance)
- **Search warrants**
- **Production orders**
- **Forfeiture/confiscation orders**

✅ **Key Distinction**
These are **judicial tools**, not informal examiner requests.

C. Letters Rogatory

Used When

- No MLA treaty exists

Definition

- Formal **court-to-court** request for judicial assistance

Common Uses

- Service of process
- Taking evidence

Characteristics

- Slower than MLA
- Can be used in **civil and criminal** cases
- Civil → only after case filed
- Criminal → even before charges

✅ **Exam Contrast**

MLA	Letters Rogatory
Treaty-based	Used when no treaty
Faster	Slower
Central authority	Court-to-court

D. Tax Information Exchange Agreements (TIEAs)

- Government-to-government
- Prevent tax evasion
- Exchange tax information
- **Only for government investigators**

E. Approach to Finding Assets Abroad (EXAM FAVORITE)

4 Core Steps

1. Identify jurisdictions
2. Contact foreign counterparts
3. Research applicable laws
4. Investigate proceeds and ownership

✅ **Mnemonic: ICRI**
Identify → **C**ontact → **R**esearch → **I**nvestigate

II. ASSET RECOVERY

A. Purpose

Recover:

- Fraud losses
- Proceeds of crime
- Instrumentalities of fraud

B. Five-Step Recovery Process (VERY TESTED)

1. **Evaluate recovery potential**
2. Commence legal processes
3. Secure assets
4. Obtain judgment
5. Enforce judgment

✅ **Mnemonic: ECSOE**

C. Evaluate Potential for Recovery

Consider:

- Are assets already dissipated?
- Criminal prosecution?
- Ability to satisfy judgment?
- Availability of pretrial attachment?
- Risk of asset concealment?

D. Civil vs. Criminal Actions

Civil Action

- Victim-initiated
- Purpose: **compensation**
- Remedies vary by:
    - Common law
    - Statute
- May include:

    - Damages
    - Fees
    - Treble damages (statutory)

Criminal Action

- Prosecuted by government
- Penalties:
    - Fines
    - Imprisonment
- Victim recovery possible via:
    - Restitution
    - Asset forfeiture

✅ **Exam Key Rule**
Criminal cases **do not guarantee victim recovery**, but recovery *may* occur via restitution.

E. Securing, Judging, Enforcing

- **Freezing orders** → after litigation starts
- **Judgment** → formal court order
- **Enforcement** → may require MLA if cross-border

III. REPORT WRITING (VERY HIGH-YIELD)

A. Types of Reports

1. **Fraud Examination Reports**
2. **Expert Reports**

✅ **Key Difference**

Fraud Exam Report	Expert Report
Documents facts	Provides opinions
Internal use	Litigation use
No guilt opinions	Technical opinions allowed

B. Principles of Good Reports

Four Characteristics

1. Accuracy
2. Clarity
3. Impartiality & relevance
4. Timeliness

✅ **Mnemonic: ACIT**

C. Common Reporting Mistakes (EXAM GOLD)

❌ Expressing guilt/innocence
❌ Calling someone a liar
❌ Speculative conclusions
❌ Unsupported opinions

✅ **Allowed Opinions**

- Internal control adequacy
- GAAP compliance
- Preventive recommendations

❌ **Prohibited Opinions**

- Guilt or innocence
- Witness credibility

D. Proper vs Improper Language (TESTED)

Improper

"The suspect lied and is guilty of fraud."

Proper

"The suspect initially denied approval. After reviewing evidence, the suspect stated that he knowingly approved the transactions."

✅ **Rule:**
Report **facts + statements**, not interpretations.

E. Evidence Handling

- Maintain chain of custody
- Use copies, not originals
- Secure evidence (physical & digital)
- Mishandling evidence = **fatal to case**

F. Organization of Reports

- Chronological **OR**
- By transaction

✅ **During investigation:** Do NOT chronologically file evidence
✅ **During writing:** Chronology may help reader

G. Reader Analysis (EXAM FAVORITE)

Assume report may be read by:

- Management
- Lawyers
- Defendants
- Media
- Judges/juries

✅ **Golden Rule**

Write every report as if it will be disclosed in court.

IV. STANDARD FRAUD EXAMINATION REPORT STRUCTURE

ACFE-Recommended Sections

1. Background
2. Executive Summary
3. Scope
4. Approach
5. Findings
6. Summary

7. Impact
8. Follow-up / Recommendations

✅ **Mnemonic: BESAFSIR**

V. EXPERT REPORTS (ADVANCED TOPIC)

Must include:

- Qualifications
- Scope
- Facts/data considered
- Methodology
- Opinions & bases
- Alternative explanations
- Exhibits
- Compensation
- Prior testimony

✅ **Exam Rule**

Expert opinions must be **method-based, peer-supported, and defensible**.

VI. PROSECUTION CONSIDERATIONS

Prosecutors prefer cases that are:

- Well-documented
- Fully investigated
- Material in value
- Clearly organized

✅ **Fraud examiners should NOT**

- Refer weak or incomplete cases
- Speculate without evidence

VII. EXAM QUICK HITS (MEMORIZE)

- MLA ≠ Letters Rogatory

- Fraud examiners **do not opine on guilt**
- Restitution ≠ guaranteed recovery
- Opinions allowed only on technical matters
- Reports must withstand judicial scrutiny
- Evidence integrity is non-negotiable

Tracing Illicit Transactions, Asset Recovery, and Report Writing

(Fraud Examiners Manual – Investigation Section)

I. TRACING ILLICIT TRANSACTIONS (INTERNATIONAL)

A. Mutual Legal Assistance (MLA)

What it is
A **government-to-government** mechanism to obtain assistance in criminal investigations involving foreign jurisdictions.

Common MLA Requests Include

- Bank account information
- Account documents
- Search warrants
- Subpoenas
- Production orders
- Account monitoring
- Forfeiture/confiscation assistance

Advantages of MLA

- Available **during investigation stage**
- May **not require dual criminality**
- Allows **wide range of assistance**

Grounds for Refusal

- De minimis value
- Prejudice to sovereignty/security
- No reasonable prospect of conviction
- Double jeopardy (already convicted/acquitted)

- Ongoing local proceedings
- Target has immunity

✅ **Exam Tip:**
If a question says *"foreign bank records + government cooperation"*, think **MLA first**.

B. Tools Requiring MLA

- **Account monitoring orders** (real-time surveillance)
- **Search warrants**
- **Production orders**
- **Forfeiture/confiscation orders**

✅ **Key Distinction**
These are **judicial tools**, not informal examiner requests.

C. Letters Rogatory

Used When

- No MLA treaty exists

Definition

- Formal **court-to-court** request for judicial assistance

Common Uses

- Service of process
- Taking evidence

Characteristics

- Slower than MLA
- Can be used in **civil and criminal** cases
- Civil → only after case filed
- Criminal → even before charges

✅ **Exam Contrast**

MLA	Letters Rogatory
Treaty-based	Used when no treaty

Faster	Slower
Central authority	Court-to-court

D. Tax Information Exchange Agreements (TIEAs)

- Government-to-government
- Prevent tax evasion
- Exchange tax information
- **Only for government investigators**

E. Approach to Finding Assets Abroad (EXAM FAVORITE)

4 Core Steps

1. Identify jurisdictions
2. Contact foreign counterparts
3. Research applicable laws
4. Investigate proceeds and ownership

✅ **Mnemonic: ICRI**
Identify → **C**ontact → **R**esearch → **I**nvestigate

II. ASSET RECOVERY

A. Purpose

Recover:

- Fraud losses
- Proceeds of crime
- Instrumentalities of fraud

B. Five-Step Recovery Process (VERY TESTED)

1. **Evaluate recovery potential**
2. Commence legal processes
3. Secure assets
4. Obtain judgment
5. Enforce judgment

✅ **Mnemonic: ECSOE**

C. Evaluate Potential for Recovery

Consider:

- Are assets already dissipated?
- Criminal prosecution?
- Ability to satisfy judgment?
- Availability of pretrial attachment?
- Risk of asset concealment?

D. Civil vs. Criminal Actions

Civil Action

- Victim-initiated
- Purpose: **compensation**
- Remedies vary by:
    - Common law
    - Statute
- May include:
    - Damages
    - Fees
    - Treble damages (statutory)

Criminal Action

- Prosecuted by government
- Penalties:
    - Fines
    - Imprisonment
- Victim recovery possible via:
    - Restitution
    - Asset forfeiture

✅ **Exam Key Rule**
Criminal cases **do not guarantee victim recovery**, but recovery *may* occur via restitution.

E. Securing, Judging, Enforcing

- **Freezing orders** → after litigation starts
- **Judgment** → formal court order
- **Enforcement** → may require MLA if cross-border

III. REPORT WRITING (VERY HIGH-YIELD)

A. Types of Reports

1. **Fraud Examination Reports**
2. **Expert Reports**

✅ **Key Difference**

Fraud Exam Report	Expert Report
Documents facts	Provides opinions
Internal use	Litigation use
No guilt opinions	Technical opinions allowed

B. Principles of Good Reports

Four Characteristics

1. Accuracy
2. Clarity
3. Impartiality & relevance
4. Timeliness

✅ **Mnemonic: ACIT**

C. Common Reporting Mistakes (EXAM GOLD)

❌ Expressing guilt/innocence
❌ Calling someone a liar

❌ Speculative conclusions
❌ Unsupported opinions

✅ **Allowed Opinions**

- Internal control adequacy
- GAAP compliance
- Preventive recommendations

❌ **Prohibited Opinions**

- Guilt or innocence
- Witness credibility

D. Proper vs Improper Language (TESTED)

Improper

"The suspect lied and is guilty of fraud."

Proper

"The suspect initially denied approval. After reviewing evidence, the suspect stated that he knowingly approved the transactions."

✅ **Rule:**
Report **facts + statements**, not interpretations.

E. Evidence Handling

- Maintain chain of custody
- Use copies, not originals
- Secure evidence (physical & digital)
- Mishandling evidence = **fatal to case**

F. Organization of Reports

- Chronological **OR**
- By transaction

✅ **During investigation:** Do NOT chronologically file evidence
✅ **During writing:** Chronology may help reader

G. Reader Analysis (EXAM FAVORITE)

Assume report may be read by:

- Management
- Lawyers
- Defendants
- Media
- Judges/juries

✅ **Golden Rule**

Write every report as if it will be disclosed in court.

IV. STANDARD FRAUD EXAMINATION REPORT STRUCTURE

ACFE-Recommended Sections

1. Background
2. Executive Summary
3. Scope
4. Approach
5. Findings
6. Summary
7. Impact
8. Follow-up / Recommendations

✅ **Mnemonic: BESAFSIR**

V. EXPERT REPORTS (ADVANCED TOPIC)

Must include:

- Qualifications
- Scope
- Facts/data considered
- Methodology
- Opinions & bases
- Alternative explanations

- Exhibits
- Compensation
- Prior testimony

✅ **Exam Rule**

Expert opinions must be **method-based, peer-supported, and defensible**.

VI. PROSECUTION CONSIDERATIONS

Prosecutors prefer cases that are:

- Well-documented
- Fully investigated
- Material in value
- Clearly organized

✅ **Fraud examiners should NOT**

- Refer weak or incomplete cases
- Speculate without evidence

VII. EXAM QUICK HITS (MEMORIZE)

- MLA ≠ Letters Rogatory
- Fraud examiners **do not opine on guilt**
- Restitution ≠ guaranteed recovery
- Opinions allowed only on technical matters
- Reports must withstand judicial scrutiny
- Evidence integrity is non-negotiable

Fraud Examination Case

Bailey Books, Incorporated – Purchasing Fraud Scheme
Source: Fraud Examiners Manual17

---

1. Case Synopsis (Executive-Level)

The document evidences a **long-running kickback and fictitious invoicing scheme** involving the **Senior Purchasing Agent of Bailey Books** and a **sales representative of Orion Corporation**, resulting in **payment for undelivered goods, inflated pricing, policy circumvention, and personal enrichment**. The scheme was supported

by **collusion, falsified invoices, misdirected payments, and control override**, ultimately culminating in **confessions from both conspirators**.

---

2. Principal Parties

Role	Individual	Key Involvement
Senior Purchasing Agent	Linda Reed Collins	Approved inflated and fictitious purchases; accepted kickbacks
Vendor Sales Rep	James R. Nagel	Paid kickbacks; issued fake invoices
Vendor	Orion Corporation	Used as conduit (without corporate approval)
Company	Bailey Books, Inc.	Victim of fraud
Witnesses	Sara Dawson, Becky Robinson, Ernie Quincy	Provided corroborating evidence

---

3. Fraud Scheme Overview

A. Scheme Mechanics

The fraud involved **three escalating phases**:

1. **Kickbacks via Inflated Pricing (2019–2020)**
    - Prices intentionally inflated to cover “commissions”
    - Payments disguised as consulting fees to a shell entity
2. **Non-Competitive Procurement Override**
    - No-bid awards
    - Rejection of cheaper and better-performing vendors
    - Misrepresentation of urgency and operational need
3. **Fictitious Invoicing and Payment for Non-Delivery (2020)**
    - Two invoices paid totaling **$197,773**
    - No goods shipped or received
    - Proceeds split between conspirators via a controlled bank account

---

4. Key Fraud Indicators Identified

A. Procurement Red Flags

- Repeated **no-bid purchases** despite availability of lower-cost vendors
- **Prepayments** despite explicit company prohibition
- Override of Purchasing and Accounts Payable objections
- Artificial urgency unsupported by operational demand

B. Payment & Accounting Red Flags

- Payments approved prior to receipt of goods
- Vendor name mismatch: *"Orion Paper Company" vs. "Orion Corporation"*
- Deposits to a **non-corporate bank account**
- No corresponding accounts receivable entries at Orion

C. Behavioral Indicators

- Manager intimidation of subordinates
- Concealment and refusal to document follow-ups
- Attempts to discourage internal communication
- Sudden nervousness when shipment discrepancies arose

---

5. Control Failures (Condition)

Control Area	Failure
Vendor Management	No enforcement of competitive bidding
Payment Controls	Weak three-way match enforcement
Management Oversight	Excessive authority concentration
Exception Monitoring	No escalations for policy overrides
Conflict of Interest	Ineffective disclosure monitoring

---

6. Root Causes (Cause)

1. **Override of Controls by Senior Management**
2. **Inadequate Segregation of Duties in Procurement**
3. **Lack of Independent Review of Prepayments**
4. **Weak Vendor Validation and Bank Account Verification**
5. **Cultural Tolerance for "Relationship-Driven" Procurement**

---

7. Financial Impact (Effect)

Type	Amount
Confirmed Fictitious Payments	~$197,773
Kickbacks (Estimated)	>$150,000
Overpricing Losses	Not fully quantified
Reputational & Legal Exposure	High

---

8. Evidence Establishing Fraud (Criteria Met)

- ✅ **Transactional Evidence**
- ✅ **Witness Corroboration**
- ✅ **Banking & Check Tracing**
- ✅ **External Vendor Contradictions**
- ✅ **Confessions and Sworn Statements**

---

9. Fraud Classification

- **Occupational Fraud**
- **Corruption (Kickbacks)**
- **Asset Misappropriation**
- **Vendor Fraud**
- **Management Override**

---

10. Suggested Audit Observations (CAE-Ready)

Observation 1: Procurement Function Susceptible to Abuse of Authority

Senior purchasing personnel were able to override established policies without effective independent challenge, enabling sustained fraudulent activity.

Observation 2: Inadequate Controls Over Vendor Payments

Payments were released without confirmed receipt of goods due to ineffective enforcement of three-way matching and weak exception escalation.

Observation 3: Insufficient Vendor and Bank Account Validation

The organization lacked controls to validate vendor legal entities and authorized bank accounts prior to payment.

---

11. Recommended Enhancements (High-Level)

- Enforce **independent approval for no-bid and prepayment transactions**
- Mandate **vendor bank account verification** to legal entity level
- Implement **exception analytics** for prepayments and pricing outliers
- Strengthen **conflict-of-interest declarations with periodic attestations**
- Introduce **rotation and mandatory leave** in procurement roles

---

12. How You Can Reuse This Output

This can be directly repurposed into:

- ✔ Audit report observations (4Cs format)
- ✔ Fraud case file summaries
- ✔ Training case studies
- ✔ CFE exam scenario practice
- ✔ Board / Audit Committee discussion materials

1. WHY WHITE-COLLAR CRIME OCCURS (CORE THEMES)

A. Organizational & Cultural Drivers

- **Profit pressure** is a primary driver of corporate deviance.
- Highly competitive industries are more prone to:
    - Data falsification
    - Premature product release
    - Misrepresentation

B. Obedience & Authority (Milgram Effect)

- Ordinary people commit wrongdoing when ordered by authority.
- Organizations that reward obedience > ethics increase fraud risk.
- Employees may commit fraud:
    - To please management
    - To avoid punishment
    - Because resistance feels impossible

✅ **Key insight**: Ethical failure is often *situational*, not personality-based.

---

2. CORPORATE EXECUTIVES & LIABILITY

A. Why Executives Rarely Go to Jail

- Corporations often:
    - Pay executives' legal costs
    - Cover fines and settlements
    - Protect compensation & tenure

B. Barriers to Prosecution

- Corporate crimes are:
    - Complex
    - Difficult to prove intent
- Executives often rely on:
    - Legal loopholes
    - Past precedent of non-imprisonment

C. Sentencing Rationalizations

Executives argue against prison using:

- Age / health
- Community standing
- "No benefit to society"
- Offense "not immoral"

✅ **Audit implication**: Personal accountability is weaker at senior levels → higher inherent risk.

---

3. MANAGEMENT BEHAVIOR & RATIONALIZATION

Common justifications used by organizations:

- "Regulation is unnecessary"
- "Costs exceed benefits"
- "Damage is spread thin; no real victim"
- "We must protect shareholders / jobs"

Corporate Subculture (Braithwaite)

- White-collar crime thrives in secrecy
- Traits:
    - Conspiracies
    - Information silos
    - Restricted communication

✅ **Red flag**: Strong hierarchy + secrecy + performance pressure.

---

4. COSTS OF WHITE-COLLAR CRIME

A. Direct Costs

- Global fraud losses: **Trillions**
- Recovery is rare:
    - **~57%** recover nothing

B. Indirect Costs (Often Worse)

- Reputational damage
- Loss of market position
- Low employee morale
- Regulatory sanctions

✅ **Exam Tip**: Indirect costs are **unquantifiable but devastating**.

---

5. CONTROLLING ORGANIZATIONAL CRIME

Three Control Approaches

1. **Voluntary change**
    - Ethics programs
    - Cultural reform
2. **Government intervention**
    - Penalties, enforcement, publicity
3. **Consumer pressure**
    - Boycotts, advocacy (least effective)

Most Feared Sanction

➡️ **Publicity**, not fines.

---

6. COMPLIANCE vs DETERRENCE

Aspect	Compliance	Deterrence
Goal	Prevent violations	Punish & discourage
Focus	Voluntary adherence	Fear of consequences
Weakness	Low impact on large firms	Resource-intensive

✅ Best systems combine **both**.

---

7. OCCUPATIONAL FRAUD – FOUNDATIONAL THEORY

A. Cressey's Fraud Triangle ✅ ✅ ✅

Fraud occurs only when **ALL THREE** exist:

1. **Non-shareable pressure**
2. **Perceived opportunity**
3. **Rationalization**

Remove **any one** → no fraud.

B. Non-Shareable Financial Problems

- Status threats
- Personal failures
- Business reversals
- Employer-employee conflict

✅ Important: **Secrecy**, not fraud, creates isolation.

C. Perceived Opportunity

Two elements:

- **General knowledge** (position of trust)
- **Technical skill** (job-based ability)

Fraud follows job design:

- Accountants → journal entries

- Bankers → dormant accounts

D. Rationalization (Pre-Crime, Not After)

Common rationalizations:

- "Borrowing"
- "I'll pay it back"
- "They owe me"
- "Everyone does it"

✅ After first success → fraud becomes habitual.

---

8. TYPES OF OCCUPATIONAL OFFENDERS (CRESSEY)

1. Independent Businesspeople

- Convert deposits
- Use "borrowing" rationale

2. Long-Term Violators

- Small amounts over time
- Want to "clean slate"
- Fear social exposure > prison

3. Absconders

- Take money and flee
- Low social ties
- Fatalistic thinking

---

9. ALBRECHT FRAUD SCALE (EXAM FAVORITE)

Fraud likelihood ↑ when:

- **Pressure HIGH**
- **Opportunity HIGH**
- **Integrity LOW**

Top Individual Red Flags

- Living beyond means

- High personal debt
- Gambling
- Feeling underpaid

Top Organizational Red Flags

- Excessive trust
- No segregation of duties
- Weak authorization
- No internal audit

---

10. ACFE OCCUPATIONAL FRAUD – KEY FINDINGS

A. Most Common Schemes

1. Asset misappropriation (most frequent)
2. Corruption
3. Financial statement fraud (least frequent, most costly)

B. Detection Methods (Ranked)

1. Tips (~43%)
2. Internal audit
3. Management review

✅ Tip sources:

- Employees (most)
- Customers / vendors
- Anonymous reports matter

---

11. FRAUD DURATION INSIGHT

- Median duration: **12 months**
- Longer duration → exponentially higher losses
- Active detection (data analytics, audits) cuts loss & duration drastically

---

12. CORPORATE GOVERNANCE & FRAUD

Core Principles

- Accountability
- Transparency
- Fairness
- Responsibility

Strong Governance Includes:

- Independent board
- Active audit committee
- Separation of CEO & Chair
- Clear oversight of fraud risk

✅ Weak governance = fertile fraud ground.

---

13. MANAGEMENT'S FRAUD RESPONSIBILITIES

Management is **primarily responsible** for:

- Fraud prevention & detection
- Ethical tone
- Effective internal controls
- Response & remediation

Ignorance ≠ defense
"Conscious avoidance" still creates liability.

---

14. COSO INTERNAL CONTROL – FRAUD LENS

Five components:

1. Control environment
2. Risk assessment *(must consider fraud)*
3. Control activities
4. Information & communication
5. Monitoring

✅ Controls must **prevent, detect, and correct**.

---

15. COMPLIANCE & ETHICS PROGRAM (USSG / ISO)

Minimum expectations:

- Clear standards
- Board oversight
- Training
- Anonymous reporting
- Investigations
- Consistent discipline
- Continuous improvement

Failure to detect ≠ ineffective program — if **reasonably designed**.

---

16. AUDITORS' FRAUD RESPONSIBILITIES

External Auditors (ISA 240)

- Maintain professional skepticism
- Focus on material misstatement due to fraud
- Evaluate management override risk
- NOT fraud investigators

Two Fraud Types Auditors Care About:

1. Fraudulent financial reporting
2. Asset misappropriation

🧠 **FINAL MEMORY ANCHORS (FOR EXAMS)**

- **Fraud = Pressure + Opportunity + Rationalization**
- **Secrecy maintains fraud**
- **Culture beats controls**
- **Tips are king**
- **Tone at the top matters more than policies**
- **Governance failure = fraud enabler**

Fraud Prevention & Auditors' Fraud Responsibilities

(High-Retention | Exam-Focused | Framework-Driven)

I. CORE CONCEPTS YOU MUST REMEMBER (EXAM FAVORITES)

1. Fraud Definition (ISA / ACFE)

Fraud is:

An **intentional act** involving **deception** used to obtain an **unjust or illegal advantage**, committed by **management, employees, or third parties**.

✅ **Keyword triggers in exam questions**: *intentional*, *deception*, *illegal/unjust benefit*

---

2. Why Fraud Is Harder to Detect Than Error

Fraud is difficult to detect because it involves:

- **Management override of controls**
- **Collusion**
- **Falsified documentation**
- **Intentional concealment**

📌 **Exam trap**: Auditors are **not** guarantors of fraud detection — they provide *reasonable assurance only*.

II. FRAUD TRIANGLE (TESTED HEAVILY)

Fraud exists when **ALL THREE** are present:

Element	Meaning
Pressure / Incentive	Financial difficulty, performance targets, bonuses
Opportunity	Weak controls, override capability
Rationalization	"I deserve it", "temporary", "company owes me"

✅ If **any one** is missing → fraud unlikely
✅ Organizations reduce fraud by **breaking opportunity first**

III. AUDITOR'S RESPONSIBILITIES (ISA 240 – MUST MEMORIZE)

A. Primary Objectives

Auditor must:

1. **Identify & assess fraud risks**
2. **Design procedures responsive to fraud risks**
3. **Respond appropriately to identified or suspected fraud**

📌 **Management ≠ Auditor responsibility**

- **Prevention & detection → Management**
- **Reasonable assurance → Auditor**

B. Professional Skepticism (ISA 200)

Auditors must:

- Maintain a **questioning mind**
- Not rely solely on management integrity
- Investigate **inconsistencies**, altered documents, unusual responses

💡 **Exam trick**:

Prior positive audit experience **does NOT reduce** fraud risk.

IV. FRAUD RISK ASSESSMENT – HOW AUDITORS DO IT

1. Required Risk Assessment Activities

Auditor must:

- Inquire of **management**
- Inquire of **those charged with governance**
- Inquire of **internal audit (if present)**
- Perform **analytical procedures**
- Evaluate **unusual relationships**

📌 **Revenue recognition** is **presumed a fraud risk**
→ Must document if presumption is rebutted

---

2. Fraud Risk Factors – Categories

Fraud risk factors are **indicators**, not proof.

They map back to Fraud Triangle:

- Incentive / pressure
- Opportunity
- Rationalization (hardest to observe)

✅ Cannot be ranked mechanically
✅ Require **professional judgment**

V. RESPONSES TO FRAUD RISK (ISA 330)

A. Overall Audit Responses

Auditor may:

- Assign **more experienced staff**
- Add **forensic / IT specialists**
- Increase **unpredictability**
- Heighten supervision

B. Mandatory Procedures – Management Override

Auditor **must** perform:

1. **Journal entry testing**
2. **Review accounting estimates for bias**
3. **Examine significant unusual transactions**

📌 These apply **to ALL audits**, regardless of assessed risk

VI. WHEN FRAUD IS IDENTIFIED

Auditor must:

- Reassess risk
- Evaluate implications across audit
- Consider **collusion**
- Assess reliability of management representations

If continuing the audit is questionable:

Auditor must:

- Consider **withdrawal** (private sector)
- Follow **professional & legal reporting requirements**

📌 **Public sector note**: Often *cannot withdraw*

VII. COMMUNICATION & DOCUMENTATION

Communications required:

- Management
- Audit Committee / Board
- Regulators (if legally required)

Documentation must include:

- Fraud risk discussions
- Identified fraud risks
- Audit responses
- Journal entry testing results
- Rationale if revenue fraud presumption rebutted

VIII. INTERNAL AUDIT – FRAUD ROLE (IIA STANDARDS)

Internal Audit's Unique Role:

- **Prevent**
- **Detect**
- **Assess fraud risk**
- **Provide assurance on fraud governance**

📌 IA is **NOT responsible for managing fraud risk**, only **assessing & advising**

Internal Audit Key Fraud Responsibilities:

- Fraud risk assessment
- Continuous auditing & data analytics
- Evaluating fraud risk governance
- Reporting unacceptable fraud risk to the Board

IX. FRAUD PREVENTION PROGRAMS (VERY EXAMABLE)

Effective Programs Include:

- **Tone at the Top**
- **Code of Conduct**

- **Whistleblower mechanisms**
- **Mandatory vacations**
- **Job rotation**
- **Fraud awareness training**
- **Data monitoring**

✅ **Most effective deterrent**:

Increasing the *perception of detection*

X. WHISTLEBLOWING & HOTLINES (FREQUENT CFE QUESTION)

Why hotlines matter:

- Most fraud is detected by **tips**
- Third-party hotlines provide:
  - Anonymity
  - 24/7 access
  - Higher reporting rates

✅ Must include **anti-retaliation protection**

XI. FRAUD RISK ASSESSMENT (ORGANIZATION-WIDE)

Key Concepts:

Term	Meaning
Inherent risk	Risk before controls
Residual risk	Risk remaining after controls

Objective:

- Identify where fraud **could** occur
- Reduce residual risk to tolerable levels

📌 Fraud risk assessment is **continuous**, not one-off

XII. EXAM POWER MEMORY (QUICK FIRE)

- Fraud ≠ error → **intentionality matters**

- Management override = **always presumed risk**
- Auditors → reasonable assurance only
- Prevention responsibility → **Management**
- Detection → **Everyone**, tips most effective
- Internal Audit → assurance, not ownership

1. FRAUD RISK ASSESSMENT (FRA)

Purpose of a Fraud Risk Assessment

A fraud risk assessment enables organizations to:

- Identify **where fraud is most likely**
- Understand **who may commit fraud and how**
- Evaluate **effectiveness of anti-fraud controls**
- Design **targeted prevention, detection, and response**
- Comply with **professional standards (e.g., ISA 315)**

Exam cue: FRA is not optional—it is a **core governance and risk requirement**. [Fraud Exam...s Manual20 | PDF]

Key FRA Questions (Think Like a Fraudster)

- What **pressures and incentives** exist?
- What **control weaknesses** can be exploited?
- How can controls be **overridden or bypassed**?
- How would fraud be **concealed**?

✅ This mindset is explicitly required—**"it couldn't happen here" thinking is a red flag**.

What Makes a "Good" Fraud Risk Assessment

A good FRA is:

- **Embedded in organizational culture**
- **Sponsored by the right level** (ideally Board/Audit Committee)
- **Collaborative** (Management + Auditors)
- **Independent and objective**
- **Actively maintained**, not one-time

Exam trap: A technically sound FRA **fails** if it lacks trust, sponsorship, or participation. [Fraud Exam...s Manual20 | PDF]

Roles in FRA

Party	Key Responsibility
Management	Owns fraud risks and controls
Auditors	Risk identification, control evaluation
Sponsor	Ensures candor, neutrality, authority
Employees	Provide ground-truth insights

---

2. FRAUD RISK ASSESSMENT PROCESS (CORE STEPS)

Step 1: Identify Inherent Fraud Risks

Fraud risks typically fall into:

- **Financial Statement Fraud**
- **Asset Misappropriation**
- **Corruption**
- **External Fraud**
- **Regulatory / Legal Misconduct**
- **IT & Cyber Risk**
- **Reputational Risk**

✅ Recognize **internal vs external sources** of fraud risk.

Step 2: Assess Likelihood & Significance

Likelihood levels

- Remote
- Reasonably Possible
- Probable

Impact (Significance) levels

- Immaterial

- Significant
- Material

Factors considered:

- Past incidents
- Industry prevalence
- Control environment
- Ethical culture
- Volume & complexity
- Regulatory and reputational impact

📌 **Exam tip:** High reputational damage = **significant risk**, even if financial loss is small.

Step 3: Identify People/Departments Most Likely to Commit Fraud

- Consider **authority, access, pressure**
- Explicitly assess **management override risk**

Step 4: Map Existing Controls

Preventive Controls

- Segregation of duties
- Policies & procedures
- Background checks
- Access controls
- Training

Detective Controls

- Audits
- Reconciliations
- Whistleblower mechanisms
- Data analytics
- Surprise audits

Step 5: Evaluate Control Effectiveness

- Are controls **designed well**?
- Are they **operating consistently**?
- Are they **cost-effective**?
- Can management override them?

Step 6: Identify Residual Fraud Risk

Residual risk exists due to:

- Missing controls
- Noncompliance
- Override capability

Residual risks must be **re-rated and addressed**.

---

3. FRAUD RISK ASSESSMENT FRAMEWORKS

Framework 1 (COSO + ACFE Aligned)

Core flow:

1. Identify fraud schemes
2. Assess likelihood
3. Assess significance
4. Identify perpetrators
5. Map controls
6. Assess control effectiveness
7. Respond to residual risk

✅ This is the **classic exam favorite** framework. [Fraud Exam...s Manual20 | PDF]

Framework 2 (Holistic / Portfolio-Based)

Four pillars:

1. Environment & Culture
2. Anti-Fraud Controls
3. Leadership Behavior
4. Complaint & Response Protocols

Results are aggregated into a **fraud risk portfolio** for prioritization.

✅ This framework emphasizes **tone at the top** and **behavioral risk**.

---

4. RESPONDING TO FRAUD RISK

Management responses:

- **Avoid** the risk
- **Transfer** the risk (insurance)
- **Mitigate** via controls
- **Accept** residual risk

📌 **Exam formula:**
Risk = Likelihood × Impact

---

5. REPORTING FRAUD RISK ASSESSMENT RESULTS

Effective reports:

- Are **objective, not opinionated**
- Focus on **what matters**
- Use **visuals, dashboards, heat maps**
- Include **clear, measurable actions**
- Match the **language of the business**

❌ Avoid overly technical, verbose reports.

---

6. FRAUD RISK MANAGEMENT (FRM)

Core Objective

Manage fraud **before, during, and after occurrence** through:

- Prevention
- Detection
- Response

FRM Foundational Frameworks

- **COSO ERM (2017)**

- **COSO Internal Control (2013)**
- **Fraud Risk Management Guide – Second Ed (2023)**
- **ISO 31000**

[Fraud Exam...s Manual20 | PDF]

FRM 2023 – Five Principles

1. Fraud Risk Governance
2. Fraud Risk Assessment
3. Fraud Control Activities
4. Fraud Investigation & Corrective Action
5. Fraud Risk Monitoring

✅ **These map directly to COSO components**—critical for exams.

---

7. THIRD-PARTY FRAUD RISK

Customer Due Diligence (CDD)

- Simplified
- Standard
- Enhanced

Triggers for enhanced CDD:

- High value
- PEPs
- Foreign jurisdictions
- Complex ownership

Vendor Fraud Risk Controls

- Vendor questionnaires
- Background checks
- Ethics & compliance review
- Vendor master file controls
- Continuous monitoring

---

8. ETHICS FOR FRAUD EXAMINERS (VERY HIGH EXAM WEIGHT)

Core Ethics Principles

Fraud examiners must demonstrate:

- **Integrity**
- **Objectivity**
- **Independence**
- **Professional skepticism**
- **Confidentiality**

Absolute Prohibitions

- No illegal acts
- No unethical conduct
- No undisclosed conflicts
- **No opinion on guilt or innocence**
- No disclosure of confidential information without authorization

🔥 **This is a classic exam trap**.

Evidence & Opinions

- Opinions must be supported by **sufficient, relevant evidence**
- Fraud examiners **present facts and conclusions**, not verdicts

---

Confidentiality Rules

- Confidentiality survives **post-engagement**
- No promises of confidentiality to suspects
- Disclosures only with:
    - Client authorization
    - Legal compulsion

---

9. PROFESSIONAL SKEPTICISM

Fraud examiners must:

- Assume fraud **may exist**
- Relax skepticism **only when evidence disproves it**
- Never issue fraud-free assurances

✅ This principle is explicitly stated and frequently tested.

---

10. PRACTICAL MEMORY ANCHOR (FOR EXAM)

FRA → CONTROLS → RESIDUAL RISK → RESPONSE → MONITOR → ETHICS

ACFE Code of Professional Ethics & CFE Code of Professional Standards

(Condensed | Exam-Focused | Practitioner-Ready)

PART A — ACFE CODE OF PROFESSIONAL ETHICS

(Rules every CFE must follow – extremely high exam weight)

---

1. CONFIDENTIALITY & DISCLOSURE (CRITICAL)

General Rule

- Fraud examiners **are not automatically obligated** to report clients/employers.
- **Confidentiality is the default rule** — but **not absolute**.

When External Disclosure May Be Justified

Disclosure to regulators, law enforcement, or external authorities may be justified when:

- The **client/employer intentionally involves the CFE in illegal conduct**
- The client **issues misleading reports** based on the fraud examiner's work
- **Senior management** is involved and internal escalation is ineffective

✅ **Key exam phrase:**

"The confidentiality rule is not a license for inaction."

🔥 **Exam pitfall:** Confidentiality ≠ concealment of material wrongdoing.

---

2. COMPLETE REPORTING OF MATERIAL MATTERS

Core Rule

All material matters must be disclosed if omission would distort facts.

Two keywords:

- **Material**
- **Distortion**

Materiality (User-Oriented Concept)

Information is **material** if:

- Its omission would **change the user's decision**
- It would influence conclusions reached from the report

📌 Fraud examiners must assess materiality **from the user's perspective**, not their own.

Distortion of Facts

- Distortion usually arises from **omissions**
- Happens when:
    - Evidence is inconclusive but conclusions are overstated
    - Tentative findings are presented as definitive
    - Judgments are rushed without enough support

✅ If evidence is unclear:

- **Clearly state limitations**
- **Avoid conclusions**
- **Withhold judgment**

---

3. PROFESSIONAL IMPROVEMENT (CONTINUING OBLIGATION)

Rule

CFEs must **continually improve competence and effectiveness**.

CPE Requirements

- **20 hours per year**
    - **≥10 hours:** technical fraud subjects
    - **≥2 hours:** ethics

✅ Double-counting allowed with CPA, CIA, CA, etc., **if content qualifies**.

🔥 Exam cue: Ethics is not episodic — it **permeates all fraud work**.

PART B — CFE CODE OF PROFESSIONAL STANDARDS (ADOPTED 2020)

These are **enforceable professional standards**, not just ethical ideals.

I. PREAMBLE (TONE & RESPONSIBILITY)

CFEs must:

- Act with **integrity**
- Subordinate **self-interest** to:
    - Clients
    - Public interest
    - The profession

✅ Standards apply to **certified CFEs**
Associate members should strive to comply.

II. APPLICABILITY

- Applies to **all Certified Fraud Examiners**
- Covers any engagement where a **substantial purpose** is fraud:
    - Prevention
    - Detection
    - Investigation
    - Resolution

III. STANDARDS OF PROFESSIONAL CONDUCT

A. Integrity & Objectivity

CFEs must:

- Maintain integrity even if it disadvantages:
    - Client
    - Employer
    - Public interest
- Identify and disclose:

    - Actual conflicts
    - Potential conflicts
    - Perceived conflicts
- Remain objective throughout the engagement
- Avoid conduct that discredits the profession
- Comply with lawful court orders
- **Never lie under oath**
- **Never commit or induce criminal acts**

🔥 **Exam trap:** Serving a client ≠ sacrificing integrity.

B. Professional Competence

CFEs must:

- Accept only assignments they are competent to perform
- Use consultation/referral if needed
- Maintain required CPE
- Continually increase professional capability

✅ Competence is **situational**, not absolute.

C. Due Professional Care (EXAM FAVORITE)

Due professional care requires:

- **Diligence**
- **Critical analysis**
- **Professional skepticism**

Specific requirements:

- Conclusions must be supported by:
    - Relevant
    - Reliable
    - Sufficient evidence
- Fraud examinations must be:
    - Adequately planned

- Properly supervised

🔥 **Key exam phrase:**

Professional skepticism is mandatory.

D. Understanding with Client or Employer

Before starting:

- CFEs must agree on:
  - Scope
  - Limitations
  - Responsibilities of all parties

If scope/limitations change:

- A **new understanding must be reached**

✅ Protects both examiner and client.

E. Communication with Client or Employer

CFEs must:

- Communicate **significant findings** during the examination
- Not wait until final reporting if material issues arise

F. Confidentiality (Standards Layer)

CFEs:

- Must not disclose confidential or privileged information
- Unless:
  - Authorized by the client
  - Required by statute/regulation
  - Ordered by a court

✅ Does not prohibit:

- Peer review
- Investigative body reviews (with confidentiality safeguards)

IV. STANDARDS OF EXAMINATION

A. Fraud Examinations

Fraud examinations must be:

- Legal
- Professional
- Thorough

CFEs must:

- Establish **predication and scope priorities early**
- Re-evaluate scope continuously
- Seek efficiency (not over-investigate blindly)
- Consider **both inculpatory and exculpatory evidence**
- Avoid conjecture and bias

🔥 Exam cue: **Both sides of evidence must be considered.**

B. Evidence Handling

CFEs must:

- Maintain effective control over:
    - Documents
    - Data
    - Digital evidence
- Protect **chain of custody**:
    - Origin
    - Possession
    - Disposition
- Preserve evidence integrity

📌 Documentation depth depends on client needs, **not examiner convenience**.

V. STANDARDS OF REPORTING

A. General Reporting

- Reports may be:

    - Written
    - Oral
    - Testimony
- No prescribed format — **but must not be misleading**

B. Report Content (VERY HIGH EXAM WEIGHT)

Reports must:

- Be based on **sufficient, reliable, relevant evidence**
- Stay within the examiner's area of competence
- **Never express an opinion on legal guilt or innocence**

🔥 **Absolute rule:**
CFEs present **facts and conclusions**, not verdicts.

EXAM-READY MEMORY ANCHOR

ETHICS → CONDUCT → CARE → EVIDENCE → COMMUNICATION → REPORTING

Or in one line:

Integrity governs conduct; conduct governs evidence; evidence governs reporting.

PRACTICAL USE (Audit & Investigation)

This chapter directly supports:

- Fraud Investigation SOPs
- Internal Audit fraud protocols
- Whistleblower handling
- Regulator-defensible reports
- Expert-witness readiness
- Conflict-of-interest governance

I. FOUNDATIONS OF FRAUD EXAMINATION

What Fraud Examination Is

Fraud examination is a **systematic, legally aware, evidence-based process** to:

- **Prevent**
- **Detect**
- **Investigate**
- **Resolve** fraud and related misconduct.

It is **not**:

- A financial audit
- A legal determination of guilt
- A purely theoretical exercise

✅ **Core principle:** Fraud examination exists to establish facts and support decisions, not to prosecute or judge.

II. WHY FRAUD OCCURS – FRAUD THEORY (HIGH EXAM WEIGHT)

The Fraud Triangle

Fraud generally requires:

1. **Pressure** (financial, personal, organizational)
2. **Opportunity** (weak or overridden controls)
3. **Rationalization** (moral justification)

Modern frameworks expand this with:

- **Capability**
- **Culture**
- **Leadership behavior**

✅ **Exam cue:** Opportunity is the only element management can fully control.

III. FRAUD RISK MANAGEMENT & ASSESSMENT

Fraud Risk Management (FRM)

Fraud is a **business risk**, not just a crime issue.
Effective FRM integrates with:

- COSO ERM
- COSO Internal Control
- ISO 31000
- Organizational governance

Core objectives:

- Reduce likelihood
- Reduce impact
- Detect earlier
- Respond consistently

Fraud Risk Assessment (FRA)

A fraud risk assessment:

- Identifies **where and how fraud could occur**
- Assesses **likelihood and impact**
- Evaluates **preventive and detective controls**
- Determines **residual fraud risk**
- Drives **prioritized action plans**

FRA must:

- Think like a fraudster
- Explicitly consider **management override**
- Be **ongoing**, not one-time

IV. TYPES OF FRAUD (CLASSIC + MODERN)

Internal Fraud

- Financial statement fraud
- Asset misappropriation
- Corruption / bribery
- Payroll and expense fraud

External Fraud

- Customer fraud
- Vendor fraud
- Cybercrime and hacking
- Business email compromise

Regulatory & Ethical Misconduct

- Conflicts of interest
- Insider trading
- AML/CFT violations
- Data privacy violations

✅ **Exam tip:** Reputational and regulatory harm can make small financial frauds materially significant.

V. PREVENTION, DETECTION & RESPONSE CONTROLS

Preventive Controls

- Tone at the top
- Segregation of duties
- Access controls
- Policies and procedures
- Training and ethics programs

Detective Controls

- Audits
- Reconciliations
- Whistleblower mechanisms
- Data analytics
- Continuous monitoring

Response Controls

- Investigation protocols
- Escalation rules
- Discipline and remediation
- Root-cause correction

VI. FRAUD INVESTIGATION PROCESS

Investigation Phases

1. **Predication**
2. **Planning**
3. **Evidence collection**

4. **Analysis**
5. **Reporting**
6. **Remediation**

✅ Investigations must be:

- Legal
- Objective
- Evidence-driven
- Properly documented

Evidence Standards

Evidence must be:

- **Sufficient**
- **Reliable**
- **Relevant**

Fraud examiners must:

- Preserve **chain of custody**
- Consider **exculpatory and inculpatory evidence**
- Avoid conjecture and bias

VII. INTERVIEWING & BEHAVIORAL ANALYSIS

Key principles:

- Build rapport
- Ask non-accusatory questions
- Observe verbal and non-verbal cues
- Document statements accurately

⚠️ **Exam trap:** Interviews are evidence-gathering tools, not confessions-seeking exercises.

VIII. DATA ANALYTICS IN FRAUD

Modern fraud examination relies heavily on analytics:

- Stratification

- Trend analysis
- Benford's Law
- Continuous auditing
- Exception reporting

Analytics should support:

- Fraud risk assessment
- Detection
- Investigation
- Monitoring

✅ Analytics supplement judgment — they do not replace professional skepticism.

IX. ETHICS – THE BACKBONE OF FRAUD EXAMINATION

ACFE Code of Professional Ethics

Fraud examiners must demonstrate:

- Integrity
- Objectivity
- Independence
- Professional skepticism
- Confidentiality
- Due professional care

Absolute prohibitions:

- No illegal acts
- No unethical conduct
- No undisclosed conflicts
- **No opinion on guilt or innocence**
- No improper disclosure of confidential information

Confidentiality (Critical Exam Area)

Confidentiality is the rule — but:

- It is **not a license for inaction**

- Disclosure may be justified when:
    - Client involves examiner in illegality
    - Reports are knowingly misleading
    - Senior management is implicated

Materiality & Complete Reporting

Fraud examiners must:

- Disclose **all material matters**
- Avoid **distortion through omission**
- Clearly state limitations when evidence is inconclusive

X. CFE CODE OF PROFESSIONAL STANDARDS (PRACTICE RULES)

Key standards govern:

- Integrity and objectivity
- Professional competence
- Due professional care
- Client/employer understanding
- Communication
- Confidentiality
- Evidence handling
- Reporting

🔥 **High-yield rule:**

CFEs present facts and professional conclusions — never verdicts.

XI. REPORTING FRAUD FINDINGS

Fraud reports:

- May be written, oral, or testimony
- Must not be misleading
- Must be supported by evidence
- Must stay within examiner's competence

Reports should:

- Focus on facts
- Avoid speculation
- Clearly link evidence to conclusions
- Support governance and decision-making

XII. ROLES & RESPONSIBILITIES

Board & Audit Committee

- Tone at the top
- Oversight of fraud risk
- Ensure independence of investigations

Senior Management

- Own fraud risk
- Implement controls
- Support ethical culture

Internal Audit / Fraud Function

- Assess controls
- Investigate allegations (if mandated)
- Use analytics
- Report independently

XIII. MASTER MEMORY FRAMEWORK (EXAM & PRACTICE)

FRAUD EXAMINATION LIFECYCLE

Risk → Controls → Indicators → Investigation → Evidence → Reporting → Remediation → Monitoring

Or ethically framed:

Integrity → Skepticism → Evidence → Objectivity → Reporting → Accountability