Part 1A — Accounting Concepts First

1. Big Picture Summary

Before studying fraud schemes, the manual first builds the **accounting foundation** needed to understand how fraud affects records and financial statements. The visible opening pages explain that fraud examiners must understand the **source and flow of financial transactions**, accounting terminology, journal entries, the accounting cycle, the main financial statements, and the reporting frameworks used to prepare them.

This is extremely important for certification exams because many questions test:

- how a fraudulent act flows through the accounting records,
- which financial statement is affected,
- whether the fraud impacts assets, liabilities, equity, revenue, expense, or cash flow,
- and whether the issue is one of recognition, valuation, classification, timing, or disclosure.

---

2. Must-Know Exam Points

HIGH YIELD

- The core accounting equation is **Assets = Liabilities + Owners' Equity**.
- Fraud examiners must understand **debits and credits**, journal entries, and how transactions move through the accounting cycle.
- The two main accounting methods are **cash basis** and **accrual basis**.
- Under **accrual accounting**, revenue is recognized when earned and expenses when incurred or matched, not necessarily when cash moves.
- The major financial statements include:
    - balance sheet / statement of financial position
    - income statement / statement of profit or loss
    - statement of changes in owners' equity
    - statement of cash flows
- Financial statements are commonly prepared under **GAAP** or **IFRS**.
- Key qualitative characteristics of useful financial information include:
    - relevance
    - materiality
    - faithful representation
    - comparability
    - consistency

    - verifiability
    - timeliness
    - understandability
- Recognition of an element generally requires:
    - probable future economic benefit flowing to/from the entity
    - cost or value that can be measured reliably.

---

3. Key Concepts and Explanations

A. Accounting Equation

Definition

The basic accounting model is:

Assets = Liabilities + Owners' Equity

Why it matters

This is the backbone of double-entry accounting. Fraud questions often test whether a transaction causes:

- asset increase/decrease,
- liability increase/decrease,
- or distortion of equity through income manipulation.

Exam use

If you can map a fraud scheme into this equation, many questions become easier.

B. Accounting Cycle and Journal Entries

The visible pages explain that the accounting cycle is the route by which transactions are identified, analyzed, recorded, and eventually summarized into financial statements. Journal entries record transactions and create the audit trail. Adjusting journal entries may also be made at period-end, such as for depreciation or write-offs.

Why it matters for fraud exams

Fraud often enters through:

- false journal entries
- unsupported adjustments
- omitted entries
- timing shifts
- misclassification

A fraud examiner must know where in the cycle a fraud could be inserted or concealed.

C. Cash Basis vs Accrual Basis

Cash basis

Revenue and expenses are recorded when cash is received or paid.

Accrual basis

Revenue is recorded when earned; expenses are recorded in the same period as the related revenue or when incurred, regardless of cash timing. The visible pages note that GAAP-based reporting generally uses accrual accounting because it better matches economic activity.

Exam trap

A scheme may manipulate timing by exploiting the difference between:

- cash received vs revenue earned
- cash paid vs expense incurred

This becomes critical in revenue recognition, liability omission, and expense manipulation questions.

D. Financial Statements

The visible pages describe the major statements:

1. Balance Sheet / Statement of Financial Position

Shows assets, liabilities, and equity at a point in time.

2. Income Statement / Statement of Profit or Loss

Shows revenues and expenses over a period, resulting in net income or loss.

3. Statement of Changes in Owners' Equity / Retained Earnings

Shows changes in owner investment, earnings, and distributions.

4. Statement of Cash Flows

Shows sources and uses of cash classified into:

- operating activities
- investing activities
- financing activities.

Why this matters

Fraud questions often ask:

- which statement is distorted,

- whether profit is inflated but cash is weak,
- whether liabilities are hidden on the balance sheet,
- or whether operating cash flow is inconsistent with reported income.

E. GAAP, IFRS, and Useful Financial Information

The visible pages discuss generally accepted accounting principles and IFRS as reporting frameworks. They also discuss qualitative characteristics that make financial information useful.

High-yield characteristics

- **Relevance** — capable of influencing decisions
- **Materiality** — large/important enough to matter
- **Faithful representation** — complete, neutral, free from error
- **Comparability**
- **Consistency**
- **Verifiability**
- **Timeliness**
- **Understandability**

Exam angle

Fraudulent financial reporting usually undermines these qualities, especially:

- faithful representation,
- comparability,
- and sometimes timeliness and understandability.

F. Recognition of Elements

The visible pages state that recognition in financial statements generally requires:

1. probable future economic benefit associated with the item, and
2. the item's cost or value can be measured reliably.

Why it matters

This is central to questions on:

- recognizing receivables
- provisions

- liabilities
- asset impairment
- reserves
- expense accruals

Part 1B — Financial Statement Fraud

Now that the accounting foundation is in place, the next topic in sequence is **Financial Statement Fraud**, followed by the scheme areas already summarized earlier. The table of contents in the first file shows this topic includes:

- what financial statement fraud is
- cost of financial statement fraud
- why it is committed
- trends
- financial statement fraud schemes
- fictitious revenues
- timing differences
- improper asset valuation
- concealed liabilities and expenses
- improper disclosures
- red flags
- detection
- financial statement analysis
- interviews
- prevention.

This confirms that the earlier summary should be expanded to include not only concealed liabilities and improper disclosures, but also the broader structure of financial statement fraud as a major exam area.

---

4. Important Terms, Definitions, and Classifications

Opening accounting terms

- **Asset** — resource owned/controlled expected to provide benefit
- **Liability** — obligation or claim against assets

- **Owners' equity** — residual interest of owners
- **Journal entry** — record of a transaction in accounting books
- **Adjusting entry** — end-of-period entry to properly reflect balances
- **Cash basis** — record when cash changes hands
- **Accrual basis** — record when earned/incurred
- **Balance sheet** — point-in-time financial position
- **Income statement** — period performance
- **Cash flow statement** — sources and uses of cash
- **GAAP / IFRS** — reporting frameworks
- **Recognition** — inclusion of an item in financial statements when criteria are met
- **Materiality** — significance to user decisions

Financial statement fraud terms

- fictitious revenues
- timing differences
- improper asset valuation
- concealed liabilities and expenses
- improper disclosures

Other topic sequence in this first section

The table of contents also confirms the exam-relevant order of later topics:

- cash receipts
- fraudulent disbursements
- inventory/other assets
- corruption
- theft of data and intellectual property.

---

5. Comparisons and Distinctions

Cash basis vs accrual basis

- **Cash basis**: focuses on cash movement
- **Accrual basis**: focuses on economic activity and matching

Balance sheet vs income statement

- **Balance sheet**: financial position at a point in time
- **Income statement**: performance over a period

Operating vs investing vs financing cash flows

- **Operating**: day-to-day business cash
- **Investing**: long-term asset acquisition/disposal
- **Financing**: debt and equity-related cash

Recognition vs disclosure

- **Recognition**: item appears in statement totals
- **Disclosure**: additional explanatory information in notes or supporting presentation

This last distinction is especially important because many fraud questions hinge on whether something should have been:

- recorded,
- measured differently,
- or disclosed.

---

6. Memory Aids

Accounting foundation

A-L-OE

- **A**ssets
- **L**iabilities
- **OE** Owners' Equity

Financial statement set

B-I-E-C

- **B**alance sheet
- **I**ncome statement
- **E**quity statement
- **C**ash flow statement

Qualitative characteristics

RM-FC-VTU

- **R**elevance

- **M**ateriality
- **F**aithful representation
- **C**omparability/Consistency
- **V**erifiability
- **T**imeliness
- **U**nderstandability

Recognition rule

PM

- **P**robable benefit
- **M**easurable reliably

---

7. Updated Study Order for Your Reviewer

For best learning and retention, your first batch should now be studied in this order:

Batch 1A — Foundations

1. Accounting Concepts
2. Financial Statements
3. GAAP / IFRS
4. Qualitative Characteristics
5. Recognition Concepts

Batch 1B — Financial Statement Fraud

6. What financial statement fraud is
7. Main schemes
8. Red flags
9. Detection methods
10. Financial statement analysis
11. Prevention

Batch 1C — Asset Misappropriation and Corruption

12. Cash receipts
13. Fraudulent disbursements
14. Inventory and other assets

15. Corruption
16. Theft of data and intellectual property

---

8. Quick Recall Sheet

What comes first?

The reviewer starts with **Accounting Concepts**, then **Financial Statement Fraud**, then the main fraud-scheme categories in Financial Transactions and Fraud Schemes.

Core accounting equation

Assets = Liabilities + Owners' Equity

Main accounting methods

Cash basis vs accrual basis

Main financial statements

Balance sheet, income statement, changes in equity, cash flow statement

Reporting frameworks

GAAP and IFRS

Useful information qualities

Relevance, materiality, faithful representation, comparability, consistency, verifiability, timeliness, understandability

Recognition rule

Probable + measurable reliably

Mortgage Fraud, Insurance Fraud, Consumer Fraud, Cyberfraud, Contract & Procurement Fraud, and Law Overview

1. Big Picture Summary

This batch expands from core occupational fraud topics into broader, highly testable certification areas involving:

- fraud in **real estate and mortgage lending**
- fraud against **insurance carriers**
- **consumer/investment scams**
- **technology-enabled fraud**
- **contract and procurement abuses**
- the overall **legal framework** surrounding fraud

For exam purposes, this batch is important because the schemes are often tested through:

- definitions

- scheme mechanics
- red flags
- investigative steps
- controls/prevention
- distinctions between similar frauds

The visible pages show that mortgage fraud is driven by pressure, commissions, weak controls, and collusion; insurance fraud depends heavily on misrepresentation and suspicious claims patterns; cyberfraud often begins with unauthorized access or social engineering; procurement fraud frequently involves collusion or cost mischarging; and the law section frames how fraud is categorized and pursued.

---

2. Must-Know Exam Points

HIGH YIELD

- **Mortgage fraud** often thrives in commission-driven, high-volume, competitive environments.
- Key mortgage schemes visible include:
    - builder bailout
    - air loans
    - identity fraud
    - identity theft schemes in loans
    - foreclosure rescue scams
    - loan modification scams
    - short sale abuse
    - property flipping / flopping
    - equity skimming
    - mortgage pooling
    - reverse mortgage abuse
    - new account fraud schemes.
- **Insurance fraud** red flags often appear in the claim narrative, timing, documentation quality, claimant behavior, provider behavior, and mismatch between evidence and alleged loss.
- **Ponzi vs pyramid** is a classic exam distinction:
    - pyramid = money tied to recruitment structure
    - Ponzi = false investment return story with little or no real business activity.
- **Cyberfraud** often lacks a traditional paper trail and may require specialist support.

- Common cyberfraud methods visible include:
    - hacking
    - phishing
    - spear phishing
    - business email compromise
    - vishing
    - smishing
    - pharming
    - catfishing
    - reverse social engineering
    - password cracking
    - browsing
    - keystroke logging.
- **Cost mischarging** in procurement/contracts falls into three main visible types:
    - accounting mischarges
    - material mischarges
    - labor mischarges.
- Procurement fraud prevention themes include:
    - employee education
    - internal controls
    - monitoring procurement activities
    - vendor management
    - vendor background checks
    - controls over vendor master file management.
- The law section shown in the table of contents signals major exam areas such as:
    - overview of legal systems
    - law related to fraud
    - bankruptcy/insolvency fraud
    - securities fraud
    - money laundering

- tax fraud
- individual rights during examinations
- criminal prosecutions.

---

3. Key Concepts and Explanations

A. Mortgage Fraud

The visible mortgage-fraud pages discuss the structure of the mortgage industry, key participants, contributing factors, and common schemes. They note that the industry's features—competition, commissions, loan volume, technology, new products, and new players—can create fertile conditions for fraud.

Key industry participants visible

- mortgagor / borrower
- mortgagee / lender
- seller
- mortgage broker
- real estate agent
- developer
- loan officer
- loan underwriter
- appraiser
- mortgage investor.

Why it matters

Exam questions often ask:

- who benefits,
- who misrepresents what,
- who must disclose what,
- and where collusion enters the transaction.

B. Builder Bailout Scheme

A builder bailout scheme appears when a builder facing excess inventory or declining market conditions uses concealed incentives or inflated values to move property and support loan approvals. Visible pages mention indicators such as inflated appraisals, undisclosed concessions, use of straw borrowers, builder-made payments, and missing addenda disclosing incentives.

High-yield red flags visible

- new construction / renovated conversions in oversupplied market
- declining sales and volume, then spike in both sales price and volume
- prices paid to non-lien holders or listed parties
- missing required disclosure forms/addenda
- payments made by builder to keep loan current
- vacant property / deteriorating neighborhood.

C. Air Loans

An air loan is described as a loan against nonexistent property, or a transaction built on fabricated participants and documents. The visible page notes fabricated borrower, property, appraisal, and supporting documents.

Exam point

This is one of the cleanest examples of completely fictitious collateral.

D. Foreclosure Rescue / Loan Modification / Short Sale Abuse

The visible pages show multiple distress-based homeowner scams:

Foreclosure rescue scams

Promise relief from delinquency but often extract fees or title and leave the homeowner worse off. Visible variations include:

- phantom help scam
- lease-back scheme.

Loan modification scams

Abuse government or lender modification programs using false hardship, occupancy, income, or asset information.

Short sale fraud

Visible pages discuss abusive facilitators, hidden side deals, false hardship, use of straw buyers or related parties, and undervaluation followed by quick resale.

Property flipping / flopping

The visible pages distinguish legitimate renovation-based flipping from fraudulent rapid resale fueled by deceptive valuation or concealment. Short-sale flopping is highlighted as a specific abuse where undervaluation and quick resale create hidden profit.

E. Equity Skimming / Mortgage Pooling / Reverse Mortgage Abuse

Equity skimming

Uses tenants' rent or other proceeds while mortgage payments stop, often leaving lender losses.

Mortgage pooling

Structured to hide legal lending-limit problems or route benefits to participants through disguised or fraudulent loan arrangements.

Reverse mortgage abuse

Visible examples include inflated values, identity theft or powers of attorney abuse, occupancy misrepresentation, and persuading seniors to misuse proceeds.

F. New Account Fraud

Visible pages show that new account fraud is especially dangerous because fraud is often committed immediately after account opening. Examples shown include:

- false identification
- business accounts using stolen checks
- personal accounts using fraudulent checks
- mobile deposit fraud
- automated teller machine deposit abuse.

Exam point

New accounts are risky because normal account history does not yet exist to reveal anomalies.

G. Insurance Fraud

The visible pages in *Manual6* cover property schemes, life schemes, liability schemes, workers' compensation fraud, premium fraud, agent fraud, claimant fraud, red flags, investigation tips, and detection/prevention tools.

Property schemes visible

- inflated inventory
- phony or inflated thefts
- paper boats.

Life insurance schemes visible

- fraudulent death claims
- murder for profit
- vanishing premium scheme.

Liability / workers' compensation

- false injury events
- exaggerated injury
- staged incidents
- organized rings involving lawyers, cappers/runners, doctors, and claimants.

H. Premium Fraud vs Claimant Fraud

Premium fraud

Misrepresentation to lower premiums, such as:

- misclassifying employees
- understating payroll
- disguising geography or operations
- creating shell/new corporations to avoid experience-based pricing
- forged documents.

Claimant fraud

Misrepresenting or fabricating injury/loss to obtain benefits or settlement. Visible pages include issues such as staged accidents, false medical treatment, second employment, organized-fraud networks, and suspicious documentation.

Exam distinction

- **Premium fraud** reduces what should be paid to the insurer.
- **Claimant fraud** increases what the insurer pays out.

I. Insurance Fraud Red Flags

Visible red flags include:

- late policy inception / recent increase in coverage before loss
- multiple policies and losses
- overly perfect documentation
- irregular receipts, altered documents, duplicate handwriting
- values inconsistent with receipts or accounting records
- no forced entry where burglary alleged

- evidence inconsistent with claimed fire/loss cause
- claimant pressure for quick settlement
- vague or conflicting medical/personal histories
- provider records out of sequence or suspiciously similar across patients
- injuries inconsistent with claimant's job, timing, or accident facts.

This is a very exam-heavy area because many questions are simple "which is the strongest red flag?" style items.

J. Consumer Fraud — Ponzi and Pyramid Schemes

The visible pages from *Manual7* focus on product fronts, multilevel marketing, speculative fronts, spotting pyramid schemes, and the distinction between illegal pyramids and Ponzi schemes.

Pyramid scheme

Participants' returns depend mainly on recruiting others and expanding the base.

Ponzi scheme

Promoters claim investment opportunity returns, but money from newer investors funds payouts to earlier investors, with minimal or no real profit-generating activity.

Visible summary distinction

The file explicitly shows the idea that:

- if earnings depend on recruiting and emphasizing levels/stages, it is an illegal pyramid;
- if it is presented as an investment opportunity with little or no commercial activity, it is a Ponzi scheme.

K. Cyberfraud

The visible cyberfraud pages define cyberfraud broadly and explain why it is difficult to investigate:

- limited traditional paper trail
- technology either used to commit crime or affected by it
- often requires specialists.

Recognizing intrusion

Visible indicators of intrusion include:

- unusual inbound/outbound traffic
- anomalies in user access to network files
- unusual network/computer performance
- suspicious log-in patterns

- bundles of data transferred
- large numbers of requests from same file
- changed system profiles
- software or hardware behaving abnormally.

L. Social Engineering and Related Cyber Schemes

Visible methods include:

- **Phishing** — impersonation to obtain credentials/data
- **Spear phishing** — targeted phishing against a specific person/entity
- **Business email compromise** — fraudulent email leveraging trusted business relationships, often to redirect payments or sensitive data
- **Vishing** — voice-based phishing
- **Smishing** — SMS-based phishing
- **Pharming** — redirecting victims to fake websites
- **Catfishing** — fake persona used to exploit emotionally/financially
- **Reverse social engineering** — attacker induces victim to seek help from attacker
- **Password cracking**
- **Browsing**
- **Keystroke logging**.

BEC variants visible

- supplier-payment redirection
- executive impersonation / wire transfer fraud
- direct deposit diversion
- real estate payment redirection
- data theft
- gift card fraud.

M. Contract and Procurement Fraud

The visible pages from *Manual8* discuss **cost mischarging** and prevention of procurement fraud.

Cost mischarging

Common visible methods include:

- charging same cost to more than one contract
- charging nonexistent or inflated costs
- charging unallowable costs
- charging to wrong category or contract
- failing to disclose discounts/credits
- outdated standards
- collusion with contractors
- using phantom suppliers
- falsified supporting documentation.

Three visible types

- accounting mischarges
- material mischarges
- labor mischarges.

Material mischarges

Visible examples include charging materials not incurred, wrong rates, obsolete items, excess residual inventory, transfers across jobs, and poor audit trail.

Labor mischarges

Visible examples include false salary/consulting charges, charging lower-rate staff as higher-rate, fictitious time, altered time cards, and charging labor to the wrong contract.

N. Procurement Fraud Prevention

Visible prevention themes include:

- employee education
- internal controls
- separation of duties
- supervisory controls
- receiving controls
- authorization/approval controls
- reconciliation controls

- recording controls
- continuous monitoring and analytics
- vendor management
- vendor background checks
- controls over vendor master file
- monitoring compliance with AP policies.

O. Law Overview

The visible table-of-contents pages in *Manual8* show the next legal study areas:

- overview of law
- law related to fraud
- bankruptcy/insolvency fraud
- securities fraud
- money laundering
- tax fraud
- individual rights during examinations
- criminal prosecutions.

This means your next law-focused batch should likely be organized separately from the fraud-scheme batches.

---

4. Important Terms, Definitions, and Classifications

Mortgage fraud terms

- builder bailout
- air loan
- foreclosure rescue scam
- phantom help
- lease-back
- loan modification fraud
- short sale abuse
- short sale flopping
- property flipping

- equity skimming
- mortgage pooling
- reverse mortgage abuse
- new account fraud.

Insurance fraud terms

- premium fraud
- claimant fraud
- workers' compensation fraud
- vanishing premium
- paper boat
- inflated inventory
- organized fraud
- cappers / runners.

Consumer fraud terms

- product front
- MLM
- speculative front
- illegal pyramid
- Ponzi scheme.

Cyberfraud terms

- intrusion indicators / IOCs
- hacking
- phishing
- spear phishing
- BEC
- vishing
- smishing
- pharming
- catfishing

- reverse social engineering
- keystroke logging.

Procurement terms

- cost mischarging
- accounting mischarge
- material mischarge
- labor mischarge
- vendor master file controls
- vendor monitoring.

---

5. Red Flags, Indicators, and Warning Signs

Mortgage fraud

- inflated or unrealistic appraisals
- unsupported assumptions
- missing disclosures/addenda
- builder or third party making payments
- straw borrower involvement
- concealed concessions
- rapid resale / unexplained appreciation
- suspicious hardship or occupancy claims
- false identity / falsified account-opening info.

Insurance fraud

- too-perfect claim package
- altered receipts / mismatched dates
- inconsistent cause of loss
- no physical evidence supporting claim
- loss timing close to policy issue/change
- claimant behavior inconsistent with injury
- duplicate or suspicious medical/provider patterns
- pressure for quick settlement

- documentation irregularities.

Cyberfraud

- abnormal traffic
- odd login attempts
- changed system files
- user complaints about performance
- weird pop-ups / toolbars / software
- suspicious requests for credentials or urgent payment changes
- impersonated executives/vendors.

Procurement fraud

- poor/incomplete contractor support
- estimates inconsistent with pricing
- repeated refusal to disclose estimating practices
- vague material charges
- excessive labor charges
- personnel qualifications not aligned with billed rates
- no clear audit trail
- weak vendor master controls.

---

6. Detection Methods, Audit Approaches, and Analytical Tools

Mortgage fraud

- review appraisal assumptions against leases, comparables, legal description, capitalization rates, absorption rates, and market conditions
- scrutinize incentives, addenda, and down-payment assistance
- look for occupancy, identity, or hardship misrepresentation
- assess whether parties and funds flow make economic sense.

Insurance fraud

Visible pages mention:

- immediate evidence preservation
- signed statements

- scene and job-duty questioning
- independent medical examination
- address similarity reports
- file comparison tools
- electronic confirmations
- exception/manual override reports
- SIU involvement
- public awareness/reporting mechanisms.

Cyberfraud

- review intrusion indicators
- analyze logs and network behavior
- examine access anomalies
- assess user behavior and credential compromise
- verify suspected payment or data requests independently.

Procurement fraud

Visible detection steps include:

- examining cost records and ledgers
- reviewing transfers of materials/labor across jobs
- comparing contract costs to commercial benchmarks
- reviewing usage, scrap, residual inventory
- scanning GL, AR subledger, and sales journal for unusual entries
- testing labor distributions and rates
- reviewing terminated employees charged to contracts
- interviewing personnel and checking external records for misconduct.

---

7. Prevention and Internal Controls

Mortgage / lending

- stronger underwriting
- identity verification
- transaction recording/cameras/fingerprints where appropriate

- mandatory disclosure requirements
- controls over new accounts and deposits.

Insurance

- policy review and underwriting checks
- claim verification
- medical/document authenticity checks
- SIUs
- reporting hotlines/mechanisms
- fraud awareness.

Cyberfraud

- user awareness
- spam/phishing filters
- antivirus/endpoint controls
- password hygiene
- independent verification of payment-change requests
- credential protection.

Procurement

- education
- SoD
- approvals and receiving controls
- reconciliations
- monitoring/analytics
- vendor due diligence
- vendor master governance.

---

8. Comparisons and Distinctions

Ponzi vs pyramid

- **Ponzi**: marketed as investment; returns paid from later investors
- **Pyramid**: structure depends on recruitment tiers and fees.

Premium fraud vs claimant fraud

- **Premium fraud**: underpay insurer
- **Claimant fraud**: overcollect from insurer.

Phishing vs spear phishing vs BEC

- **Phishing**: broad impersonation attack
- **Spear phishing**: targeted version
- **BEC**: business-context impersonation, often around payments or sensitive data.

Flipping vs flopping

- **Flipping**: rapid resale at higher price, sometimes legitimate
- **Flopping**: manipulative undervaluation/short-sale abuse followed by hidden profit resale.

Material vs labor mischarge

- **Material**: wrong goods/costs/inventory transfers
- **Labor**: wrong hours/rates/personnel/job charging.

---

9. Memory Aids

Mortgage distress scams

FLSF

- **F**oreclosure rescue
- **L**oan modification
- **S**hort sale
- **F**lopping/flipping

Insurance fraud

P-C-R-D

- **P**olicy/premium issues
- **C**laim narrative issues
- **R**ecords irregularities
- **D**ocument mismatch

Cyberfraud social engineering

P-S-B-V-S-P

- **P**hishing
- **S**pear phishing

- **B**EC
- **V**ishing
- **S**mishing
- **P**harming

Cost mischarging

A-M-L

- **A**ccounting
- **M**aterial
- **L**abor

---

10. Likely Exam Questions / High-Yield Traps

- Which mortgage scheme relies on a **nonexistent property**?
- Which insurance fraud type involves **misstating payroll or employee class**?
- Which cyber scheme uses a **trusted business context** to redirect a payment?
- Which procurement fraud type involves **charging materials from one job to another**?
- What is the best distinction between **Ponzi** and **pyramid**?
- Why are **new accounts** especially risky in financial-institution fraud?
- What is the strongest red flag when a burglary claim shows **no forced entry**?
- Which fraud is more likely when there is **urgent wire instruction change from an executive/vendor email**?

---

11. Quick Recall Sheet

Mortgage fraud

Think: **collusion + concealment + distressed borrower/property + false value/disclosure**

Insurance fraud

Think: **mismatch between story, records, timing, and physical/medical evidence**

Consumer fraud

Think: **Ponzi = fake investment returns; pyramid = recruitment-driven structure**

Cyberfraud

Think: **unauthorized access + social engineering + credential/payment/data theft**

Procurement fraud

Think: **wrong cost, wrong contract, wrong support, weak vendor controls**

Law

Think: **next separate module** — fraud types, proceedings, rights, money laundering, prosecutions

---

12. Practice Section

10 Recall Questions

1. What factors make the mortgage industry especially vulnerable to fraud?
2. What is an air loan?
3. What is the difference between premium fraud and claimant fraud?
4. What is a vanishing premium scheme?
5. What is the basic difference between a Ponzi scheme and an illegal pyramid?
6. What does BEC stand for?
7. What is vishing?
8. What are the three visible types of cost mischarging?
9. Why is new account fraud particularly risky?
10. Name three visible indicators of computer intrusion.

10 Flashcard-Style Q&A

Q: Loan against nonexistent collateral or fabricated property.
A: Air loan.

Q: Distress scam where homeowner pays for promised help that never comes.
A: Foreclosure rescue / phantom-help type scam.

Q: Misstating payroll/classification to lower workers' compensation premium.
A: Premium fraud.

Q: Fraudulent claim based on false or exaggerated injury/loss.
A: Claimant fraud.

Q: Investment scam paying older investors using newer investors' money.
A: Ponzi scheme.

Q: Recruitment-based unlawful scheme.
A: Illegal pyramid scheme.

Q: Targeted email/social engineering against a specific victim.
A: Spear phishing.

Q: Voice-based phishing.
A: Vishing.

Q: Charging material costs improperly across jobs/contracts.
A: Material mischarge.

Q: Charging wrong hours/rates/personnel to a contract.
A: Labor mischarge.

5 Situational / Application Questions

1. A lender approves a loan using inflated appraisal assumptions and undisclosed builder concessions. What mortgage scheme risk is most likely implicated?
2. An employer reports very low payroll and low-risk employee classifications, yet multiple claims arise from higher-risk work. What fraud type should be suspected?
3. An employee receives an urgent email from a "supplier" changing bank details for payment. What cyberfraud risk is most likely?
4. A contractor transfers materials from one job to another and bills both contracts. What procurement fraud category does this indicate?
5. A promoter emphasizes commissions from recruiting others into tiers, but claims it is an investment opportunity. What should you analyze to distinguish a pyramid from a Ponzi?

This batch is substantial enough that the best next step is to split it into:
2A Mortgage Fraud + New Account Fraud, **2B Insurance Fraud**, **2C Consumer Fraud + Cyberfraud**, and **2D Contract/Procurement Fraud + Law Overview**.

Batch 3 Certification Reviewer

Securities Fraud, Tax Fraud, Individual Rights, Evidence, Testifying, and Planning a Fraud Examination

1. Big Picture Summary

This batch is foundational for the **legal and investigative side** of the CFE-style reviewer. Unlike earlier batches that focused more on fraud schemes, this set focuses on:

- when an investment or transaction may qualify as a **security**
- how **tax fraud** is distinguished from tax avoidance
- what rights and duties exist during **internal investigations**
- how **evidence** is evaluated, preserved, and protected
- how a fraud examiner should **testify**
- how to **plan, scope, structure, and protect** a fraud examination

This is highly testable because certification exams often shift from "what is the scheme?" to:

- "what is the legal implication?"

- “what evidence is needed?”
- “what privilege or protection may apply?”
- “what should the examiner do first?”
- “what should be included in the investigation plan?”

---

2. Must-Know Exam Points

HIGH YIELD

- Not every investment-related arrangement is automatically a security; classification matters because it affects regulatory and legal treatment.
- Traditional securities include **stocks, bonds, and certificates of deposit**. The visible pages also discuss **futures**, **options**, **OTC options**, and **investment contracts**.
- Many fraud schemes may qualify as securities offerings, including:
    - Ponzi schemes
    - illegal pyramid schemes
    - prime bank note schemes
    - precious metals/stones schemes
    - viatical settlements
    - certain partnerships, joint ventures, oil/gas/mineral interests, hedge funds, and promissory notes.
- **Tax evasion** is different from **tax avoidance**. Tax evasion is illegal; tax avoidance generally involves lawful reduction of taxes. Intent and willfulness are central.
- Important tax-fraud indicators include:
    - misrepresentation of facts
    - hiding income/assets
    - double books
    - secret bank accounts
    - overstated deductions
    - fictitious transactions.
- During investigations, employees may have duties to cooperate, but they may also have legal, contractual, privacy, whistleblower, and other rights depending on jurisdiction.
- Three main evidence types shown in the visible pages are:
    - testimonial evidence

    - digital evidence
    - documentary evidence.
- **Chain of custody** is crucial for physical and documentary evidence authenticity and handling.
- Major protections/privileges discussed include:
    - attorney-client / legal professional privilege
    - litigation privilege / work-product
    - self-evaluation privilege
    - marital privilege
    - informant identity privilege
    - accountant-client privilege in some jurisdictions.
- A fraud examination must be **planned early**, **scoped clearly**, **documented continuously**, and structured to preserve confidentiality and avoid alerting suspects.

---

3. Key Concepts and Explanations

A. Securities Fraud

The visible pages in *Manual9* discuss securities definitions, traditional securities, derivatives such as futures and options, investment contracts, and common investment-related fraud schemes.

Traditional securities visible

- stocks
- bonds
- certificates of deposit.

Derivative / market instruments visible

- futures contracts
- options
- OTC options.

Why this matters

Exams often test whether a product is:

- a traditional security,
- a derivative,
- or an investment contract,
  because that determines how fraud or regulatory issues are analyzed.

B. Futures and Options

Futures

A futures contract is shown as an agreement to buy/sell a commodity or asset at a specified future time and price. Visible pages explain concepts like:

- standardized exchange trading
- cash settlement vs physical delivery
- clearing
- margin
- maintenance margin
- mark-to-market / trading basis.

Options

An option gives the holder a **right, not an obligation**. Visible pages distinguish:

- **call option** — right to buy
- **put option** — right to sell
- writers/sellers vs holders/buyers
- intrinsic value and time value
- in the money / at the money / out of the money.

Exam trap

Students often confuse:

- futures = obligation
- options = right without obligation for the holder

C. Investment Contracts

The visible pages discuss an investment contract concept similar to a broad test for when an arrangement becomes a security. The visible factors include:

- investment of money or another asset
- common enterprise
- investor expects profit
- profit comes from efforts of others.

Why it matters

Many deceptive schemes disguise themselves as:

- partnerships
- investment pools
- offshore note programs
- metals or mineral ventures
- pooled life-settlement interests

The exam may ask whether substance is more important than label. It usually is.

D. Securities-Related Fraud Schemes

Visible examples include:

- Ponzi schemes
- illegal pyramid schemes
- prime bank note schemes
- schemes involving precious metals and stones
- viatical settlements
- partnership/joint venture abuses
- oil, gas, and mineral interests
- hedge fund-related misconduct.

High-yield note

The visible hedge-fund pages mention vulnerabilities such as:

- theft of investor assets
- late trading
- insider trading.

E. Tax Fraud

The visible pages in *Manual10* define tax fraud broadly, distinguish tax evasion from tax avoidance, discuss intent/willfulness, list common indicators, types of evasion schemes, defenses, and fraud schemes targeting taxpayers.

Tax evasion vs tax avoidance

- **Tax evasion**: illegal efforts to avoid reporting or paying taxes

- **Tax avoidance**: lawful minimization of tax through legitimate means.

Intent / willfulness

Visible pages stress that criminal tax liability usually depends on a **willful attempt** to evade or defeat taxes unlawfully. Honest mistakes generally do not equal evasion.

Common indicators visible

- misrepresentation of facts
- artifice
- hiding income or assets
- double books
- secret bank accounts under false names
- overstated deductions
- fictitious transactions.

F. Types of Tax Evasion Schemes

Visible categories include:

- income and wealth tax evasion
- falsifying tax deductions
- tax credit schemes
- consumption tax schemes.

Consumption tax visible examples

The visible pages mention schemes involving:

- omitted transactions
- understated transaction value
- disguising taxable transactions
- missing trader arrangements
- smuggling to avoid excise tax.

G. Common Defenses to Tax Evasion Allegations

Visible defenses discussed include:

- no tax deficiency

- lack of willfulness
- avoidance, not evasion
- objectively reasonable position
- claim of right doctrine
- mental illness
- reliance on advice/expert
- ignorance of the law in limited contexts
- innocent spouse
- statutes of limitation.

Exam nuance

Some defenses may reduce criminal culpability but not necessarily remove civil liability, penalties, or interest.

H. Individual Rights During Examinations

The visible pages discuss employee duties and rights in investigations, duty to preserve evidence, contractual rights, whistleblower protections, privacy rights, monitoring, and data protection themes.

Core themes visible

- employees may have a duty to cooperate within reasonable scope
- organizations may have duties to preserve relevant information for litigation
- destroying evidence can trigger sanctions
- employment contracts or collective bargaining agreements may limit investigative actions
- whistleblowers may be legally protected from retaliation
- privacy rights affect workplace searches and monitoring
- notice, proportionality, transparency, and legal basis are important, especially in privacy-heavy jurisdictions.

Exam point

The examiner should not assume that internal access equals unrestricted investigative freedom.

I. Basic Principles of Evidence

The visible pages in *Manual11* discuss hearsay exceptions, chain of custody, impeachment, privileges and protections, and testifying.

Chain of custody

The visible pages define chain of custody as documenting who had possession or access to an item and what was done with it from collection through production in court.

Why it matters

Chain of custody supports:

- authenticity
- integrity
- reliability
- admissibility arguments

Visible good practices

- identify what the item contains
- document each receipt/removal
- record location and dates
- maintain continuous record of handoffs
- preserve original packaging/receipts where possible.

J. Impeachment

Visible impeachment methods include challenging a witness based on:

- bias or self-interest
- impaired ability to observe
- prior inconsistent statements
- certain criminal convictions
- reputation for untruthfulness.

Why it matters

This is a classic evidence/testifying topic. Expect questions on credibility attacks.

K. Privileges and Protections

Visible pages discuss:

- legal professional privilege / attorney-client privilege
- legal advice privilege
- litigation privilege / work-product

- self-evaluation privilege
- marital privilege
- parent-child privilege in some places
- informant identity privilege
- accountant-client privilege in some jurisdictions
- complications in cross-border privilege rules.

High-yield distinction

- **Attorney-client / legal professional privilege** protects confidential communications for legal advice.
- **Work-product / litigation privilege** protects materials prepared in anticipation of litigation.
- These protections can be **waived**.

L. Testifying

Visible pages discuss the nature of testimony, differences between common-law/adversarial and inquisitorial systems, factual vs expert testimony, and considerations for a law witness.

Key ideas visible

- testimonial evidence is statements made in proceedings
- factual testimony is based on firsthand knowledge/observation
- expert testimony may include specialized opinion
- the witness must distinguish information from evidence
- summaries/charts may be used when originals are too voluminous, subject to rules.

Exam point

A fraud examiner may serve as:

- fact witness,
- expert witness,
- or both, depending on role and qualifications.

M. Planning and Conducting a Fraud Examination

The visible pages in *Manual12* are very practical and exam-relevant. They cover team selection, leadership, learning about the organization, building the investigation plan, goals, scope, time frame, law-enforcement notification, task assignments, operational issues, case plan design, resources, confidentiality, suspect-alert avoidance, and evidentiary protections.

Core planning steps visible

Before planning is complete, visible pages say the team should:

- review what is known
- define goals
- identify whom to keep informed
- determine scope
- set time frame
- assess need for law enforcement assistance/notification
- define member roles
- address operational issues
- outline the course of action
- adapt resources
- prepare the organization.

Investigation goals visible

Examples include:

- prevent further loss/exposure
- determine ongoing misconduct
- secure evidence
- minimize/recover losses
- assess causes and prevention
- support appropriate legal/disciplinary action
- protect legal privileges.

N. Scope, Time, Roles, and Confidentiality

Scope

Visible pages say scope may be limited by:

- subject matter
- department
- geographic area
- resources

- legal/procedural limits
- organizational culture and policy issues.

Time frame

Must account for:

- task deadlines
- deliverables
- earnings releases
- audit committee timing
- realism based on allegation complexity.

Roles

Responsibilities and reporting lines must be clearly defined or the case may become chaotic.

Confidentiality / avoid alerting suspect

Visible pages recommend:

- limit discussions
- inform only need-to-know persons
- work discreetly
- investigate during nonbusiness hours where appropriate
- secure case information
- avoid emails/places where others can overhear
- consider privilege structures.

O. Collecting Evidence

At the start of the next chapter, visible pages note three main evidence types:

- testimonial
- digital
- documentary.

This connects directly back to the evidence chapter in *Manual11*.

---

4. Important Terms, Definitions, and Classifications

Securities terms

- stock
- bond
- certificate of deposit
- futures contract
- margin
- maintenance margin
- option
- call
- put
- intrinsic value
- time value
- OTC option
- investment contract
- hedge fund.

Tax terms

- tax fraud
- tax evasion
- tax avoidance
- willfulness
- tax deficiency
- innocent spouse
- claim of right doctrine
- consumption tax
- excise tax
- VAT
- missing trader scheme.

Rights/investigation terms

- duty to cooperate
- duty to preserve

- whistleblower protections
- workplace privacy
- monitoring notice
- GDPR-style principles of necessity, proportionality, transparency, purpose limitation.

Evidence terms

- hearsay
- chain of custody
- impeachment
- attorney-client privilege
- litigation privilege
- work-product
- self-evaluation privilege
- marital privilege
- informant privilege.

Investigation planning terms

- scope
- time frame
- case plan
- roles and assignments
- operational issues
- confidentiality
- need-to-know
- evidentiary privilege/protection
- documentary, digital, testimonial evidence.

---

5. Red Flags, Indicators, and Warning Signs

Securities / investment

- product label does not match economic substance
- promised profits depend mainly on promoters or recruitment
- nondisclosure agreements and exclusivity pressure

- unusually high returns / obscure instruments
- insiders benefiting disproportionately
- complex offshore or difficult-to-verify opportunities.

Tax fraud

- double books
- false-name accounts
- unexplained deposits
- false or inflated deductions
- fictitious transactions
- hidden income/assets
- invoices or records altered/destroyed.

Investigation/rights issues

- deletion or destruction of relevant records
- failure to suspend routine destruction
- retaliatory behavior toward whistleblowers
- overbroad or unlawful monitoring/searches
- privacy-law noncompliance.

Evidence handling

- unclear chain of custody
- missing dates/locations/handlers
- evidence accessed by unauthorized persons
- witness bias/self-interest
- inconsistent prior statements.

Investigation planning

- vague scope
- undefined roles
- no confidentiality controls
- overly rigid plan not updated
- suspect alerted too early

- insufficient resources or legal consultation.

---

6. Detection Methods, Audit Approaches, and Analytical Tools

Securities fraud

- look beyond labels to substance
- examine whether investor profits depend on others' managerial efforts
- assess whether instrument is being marketed deceptively
- review promoter control, investor role, and payout structure.

Tax fraud

Visible evidence examples include:

- direct evidence: unexplained deposits, false documents, false explanations, withholding claims without support
- circumstantial evidence: illicit income, income in excess of deposits, expenditures beyond admitted income.

Evidence and testimony

- establish chain of custody
- identify impeachment issues
- distinguish firsthand observation from derived summaries/opinions
- understand when summaries may be used in court.

Fraud examination planning

- gather known facts early
- ask scoping questions
- identify locations, actors, deadlines, objectives, budget, cultural/policy constraints
- build case plan
- document plan and updates continuously.

---

7. Prevention and Internal Controls

Securities / investment

- due diligence on product structure
- scrutinize promoter claims

- verify operational substance
- avoid blind reliance on labels or prestige.

Tax

- accurate recordkeeping
- document retention
- separation from informal/off-book activity
- control over deductions/credits and transaction classification.

Investigation governance

- preserve relevant information
- implement lawful privacy/monitoring policies
- anti-retaliation practices
- written monitoring/notice policies
- legal review before sensitive actions.

Evidence/investigation

- secure evidence
- restrict access
- document handoffs
- use privileged structures where appropriate
- maintain need-to-know discipline
- plan before acting.

---

8. Comparisons and Distinctions

Tax evasion vs tax avoidance

- **Evasion**: unlawful
- **Avoidance**: lawful tax minimization.

Fact witness vs expert witness

- **Fact witness**: firsthand observations
- **Expert witness**: specialized opinion/explanation.

Attorney-client privilege vs work-product

- **Attorney-client**: confidential legal communications

- **Work-product**: materials prepared in anticipation of litigation.

Testimonial vs documentary vs digital evidence

- **Testimonial**: statements by people
- **Documentary**: records/documents
- **Digital**: electronically stored information/devices/logs.

Futures vs options

- **Futures**: obligations
- **Options**: rights for holder, obligations for writer.

Ponzi / pyramid as securities issue

Some schemes may also be analyzed as securities offerings if they qualify as investment contracts.

---

9. Memory Aids

Investigation planning

G-S-T-R-C

- **G**oals
- **S**cope
- **T**ime frame
- **R**oles/resources
- **C**onfidentiality/case plan

Evidence

T-D-D

- **T**estimonial
- **D**igital
- **D**ocumentary

Tax

E-A-W

- **E**vasion = illegal
- **A**voidance = legal
- **W**illfulness matters

Privileges

A-W-M

- **A**ttorney-client
- **W**ork-product
- **M**arital

Securities

S-B-C / F-O-I

- **S**tocks
- **B**onds
- **C**Ds
- **F**utures
- **O**ptions
- **I**nvestment contracts

---

10. Likely Exam Questions / High-Yield Traps

- Which element most clearly distinguishes **tax evasion** from an honest mistake?
- Which evidence type requires especially careful **chain of custody** documentation?
- When does a communication qualify for **attorney-client privilege**?
- What is the difference between a **fact witness** and an **expert witness**?
- Which is more likely to be protected by **work-product** doctrine: raw business records or materials prepared for anticipated litigation?
- What is the first planning mistake in a fraud examination: no case plan, or no final report? Usually no proper case planning comes first.
- Which is the best description of an **investment contract**?
- Why might destroying records after anticipated litigation create sanctions?

---

11. Quick Recall Sheet

Securities fraud

Think: **what is the instrument really, who controls profits, and is substance different from label?**

Tax fraud

Think: **illegal evasion vs legal avoidance; willfulness is critical**

Employee rights / internal investigations

Think: **cooperation duty exists, but privacy, contracts, whistleblower laws, and preservation duties matter**

Evidence

Think: **admissibility, authenticity, credibility, custody, privilege**

Testifying

Think: **fact vs expert, firsthand vs summary/opinion**

Fraud examination planning

Think: **set goals, define scope, assign roles, protect confidentiality, document everything**

---

12. Practice Section

10 Recall Questions

1. What makes an arrangement an investment contract?
2. What is the difference between a futures contract and an option?
3. Why is willfulness important in tax evasion cases?
4. Name four common indicators of tax fraud.
5. What are the three main evidence types noted in the visible investigation chapter?
6. What is chain of custody?
7. What is impeachment of a witness?
8. What is the difference between attorney-client privilege and work-product protection?
9. What are key elements of an investigation plan?
10. Why should an examiner avoid alerting the suspect too early?

10 Flashcard-Style Q&A

Q: Illegal effort to evade or defeat taxes.
A: Tax evasion.

Q: Lawful minimization of taxes.
A: Tax avoidance.

Q: Evidence consisting of witness statements.
A: Testimonial evidence.

Q: Continuous documented record of evidence handling.
A: Chain of custody.

Q: Attack on a witness's credibility.
A: Impeachment.

Q: Protection for confidential legal communications.
A: Attorney-client / legal professional privilege.

Q: Protection for materials prepared in anticipation of litigation.
A: Work-product / litigation privilege.

Q: A witness who testifies from firsthand observation.
A: Fact witness.

Q: A witness offering specialized opinion.
A: Expert witness.

Q: Main early planning document for a fraud examination.
A: Investigation plan / case plan.

5 Situational / Application Questions

1. A promoter says an "investment club" is not a security because it is structured as a partnership. What should the examiner evaluate first?
2. A taxpayer claims huge deductions but cannot support them and keeps two sets of books. What tax-fraud themes are implicated?
3. During an internal investigation, a manager wants IT to secretly access all employee private communications without notice. What legal/right issues should be considered?
4. A key document changed hands multiple times with no written record. What evidentiary weakness does this create?
5. A fraud team begins interviewing witnesses before setting scope, goals, or reporting lines. What investigation-control failure is this?

Sources of Information, Digital Forensics, Asset Recovery, Report Writing, and Sample Fraud Examination Reports

1. Big Picture Summary

This batch focuses on how fraud examiners **find information, preserve digital evidence, trace and recover assets, and communicate results**. It moves from "how to investigate" into "how to gather intelligence and document the case properly."

This is highly testable because it connects core investigation workflow:

1. **Find the information**
2. **Preserve and analyze the evidence**
3. **Trace assets or illicit proceeds**
4. **Recover what can be recovered**
5. **Write a clear, defensible report**

The sample-report file also shows how fraud examination work product is presented in practice through memoranda, interview summaries, surveillance logs, invoice exhibits, canceled checks, and records reviews.

---

2. Must-Know Exam Points

HIGH YIELD

- Internet and database searching requires **specific keywords, operators, filters, phrase searching, and cross-checking results**.
- Public-record information can come from:
    - government sources
    - public-record vendors
    - investigative service companies.
- Online databases are useful but have limits:
    - incomplete coverage
    - outdated data
    - abstracts instead of originals
    - jurisdiction gaps
    - privacy-law restrictions.
- Social media can provide useful evidence, but fraud examiners must respect:
    - privacy settings
    - lawful access boundaries
    - authenticity/admissibility concerns
    - anti-pretexting / anti-hacking limits.
- In digital forensics, the main goal is to preserve the **integrity** of the evidence.
- If a computer is **running**, turning it off can destroy volatile evidence; but leaving it on can also alter data. This is why trained digital forensic involvement matters.
- Important digital-forensic concepts include:
    - volatile data
    - hard shutdown vs graceful shutdown
    - chain of custody
    - write-blocking
    - forensic imaging
    - processing/filtering data
    - cloud-forensics challenges
    - mobile forensics.

- Asset recovery often involves:
    - evaluating recoverability
    - commencing legal process
    - securing assets
    - obtaining judgment
    - enforcing judgment.
- Fraud examination reports should be:
    - accurate
    - clear
    - impartial and relevant
    - timely.
- A fraud examiner should be cautious about **conclusions and opinions**. Reports should not improperly state guilt or innocence.

---

3. Key Concepts and Explanations

A. Sources of Information

The visible pages in *Manual14* discuss internet searching, public records, online databases, archived web content, social media, background checks, due diligence, and employment background information.

Internet searching

Visible search guidance includes:

- use more than one search engine
- use exact phrases in quotation marks
- use specific keywords
- use exclusions/minus operators
- search by file type
- search by title/body/URL or operator-based constraints
- try variant spellings and synonyms
- review multiple pages of results
- use browser find tools to navigate results.

Why it matters

Exam questions may ask the best first step when searching online. The answer is usually not “search broadly and hope.” It is to search **precisely and iteratively**.

B. Public Records and Online Databases

Visible sources include:

- government websites and repositories
- public-record vendors
- investigative service companies.

Key point

A public-record database search is often a **lead**, not the final proof. The visible pages emphasize that database results may be incomplete, outdated, or abstracted; original-source validation may still be necessary.

Visible limitations

- online availability varies by jurisdiction
- only summaries/abstracts may appear
- data may be inaccurate or stale
- sources may not be reliable
- privacy laws can restrict access or use.

C. Deep Web, Dark Web, Archives, and Social Media

Deep web

Visible pages describe the deep web as content not indexed by standard search engines.

Dark web

Described as a portion of the deep web accessed through special tools, capable of legitimate and illegitimate uses, and requiring caution.

Internet archives

Visible pages mention archived web content as a useful source of historical information, such as removed posts, prior content, or old company statements.

Social media

Visible pages note that social media can help:

- investigate complaints
- identify witnesses

- research the accused
- learn about accusers
- find photos, places, travel, affiliations, or business information.

Key caution

Access must be lawful. Fraud examiners should not use pretexting, password-cracking, or unethical means to access restricted information.

D. Collecting Social Media Evidence

Visible pages discuss best practices for social media evidence, including:

- printing content
- screen recording / screenshots
- converting pages to preserved formats
- capturing links and embedded content
- preserving context and metadata where possible
- documenting each step of collection.

Why it matters

Social media changes quickly, so **timely capture** and **authenticity documentation** matter.

E. Background Checks and Due Diligence

Visible pages discuss using online sources for:

- people searches
- hidden assets
- litigation history
- criminal background
- business relationships
- financial condition
- professional licenses and credentials
- adverse media.

Exam point

Background checks and due diligence are often based on public-record searches, but legal counsel may be needed, especially for employment-related reviews or privacy-sensitive jurisdictions.

F. Digital Forensics

The visible pages in *Manual15* discuss seizure decisions, live collection, volatile data, securing evidence, hard shutdown, chain of custody, write-blockers, imaging, documentation, data filtering, cloud forensics, and mobile forensics.

Core principle

Maintain the **integrity of digital evidence**.

If the computer is on: leave it or turn it off?

The visible pages explain that this is not a simple question. Turning off a running system may destroy volatile evidence, but interacting with it can also alter data. This is why trained forensic personnel are important.

G. Volatile Data and Live Collection

Visible examples of volatile data include:

- RAM contents
- passwords or encryption keys in memory
- running programs/processes
- open sessions
- network connections
- operating-system state
- network-device logs.

Why it matters

Some evidence disappears when the machine powers down. That makes live collection appropriate in some cases, especially where:

- the machine is running
- encryption is present
- active attack/malware may be occurring
- critical systems cannot be shut down.

H. Securing Digital Evidence

Visible best practices include:

- disconnecting records/devices

- prohibiting access
- maintaining chain of custody
- using write-blocking devices where needed
- using proper packaging
- using encryption where needed
- documenting device condition, identifiers, status, tools used, and actions taken.

Hard shutdown vs graceful shutdown

The visible pages note that graceful shutdown can delete or alter some data, while hard shutdown may better preserve state in certain running-system contexts.

I. Forensic Imaging and Data Processing

Imaging

A forensic image is a bit-for-bit copy used for analysis instead of working directly on originals.

Processing / filtering methods visible

- keyword searching
- deduplication
- date-range filtering
- file-type filtering
- analytic review.

Exam point

Analysis should usually happen on the image, not on the live original evidence.

J. Cloud Forensics

Visible cloud challenges include:

- lack of frameworks/specialist tools
- lack of direct accessibility
- lack of data control
- lack of knowledge about storage location
- jurisdiction issues
- discovery complications

- preserving chain of custody
- resource sharing / multitenancy.

Why it matters

Cloud evidence may involve provider controls, contracts, logs, metadata, location uncertainty, and commingled data from multiple users.

K. Mobile Forensics

The visible pages introduce mobile forensics as increasingly important and note that logical extraction can recover items such as:

- messages
- multimedia
- contacts
- tasks
- images
- audio
- videos
- calendar entries.

L. Tracing Illicit Transactions and Asset Recovery

The visible pages in *Manual16* discuss cross-border tracing tools, mutual legal assistance, letters rogatory, tax-information exchange, finding assets abroad, legal recovery theories, civil/criminal proceedings, and the core recovery steps.

Cross-border tools visible

- mutual legal assistance (MLA) requests
- letters rogatory
- tax-information exchange agreements.

Approach to finding assets stored abroad

Visible steps include:

- identify likely jurisdictions
- contact foreign counterparts early
- research local laws

- locate proceeds and evidence of ownership.

Recovery steps visible

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

Exam point

Recovery is not just “find the money.” It is also a legal-process problem.

M. Civil vs Criminal Recovery

Visible pages explain:

- **civil actions** are brought to recover compensation or remedies
- **criminal actions** punish wrongdoing, though they may sometimes produce restitution or victim compensation routes.

Key distinction

Criminal prosecution does not automatically mean full victim recovery.

N. Report Writing

The visible report-writing pages in *Manual16* are very exam-relevant. They describe two common report types:

- fraud examination reports
- expert reports.

Characteristics of a good report

Visible pages list:

- accuracy
- clarity
- impartiality and relevance
- timeliness.

Good preparation

Visible guidance includes:

- active listening
- thoughtful planning
- understanding audience and scope
- documenting facts carefully
- retaining support for statements
- not releasing conclusions before procedures are complete.

O. Conclusions and Opinions in Reports

This is one of the most important visible sections.

Visible guidance indicates:

- conclusions should be based on the examination and supported by facts
- the examiner should avoid improper statements of guilt or innocence
- opinions are acceptable only in proper contexts and within expertise
- opinions should not be substituted for factual reporting where facts can speak for themselves.

The visible pages even contrast **improper** vs **proper** wording, showing that the examiner should point to inconsistencies and facts, not leap to personal accusations.

P. Organizing Information in the Report

Visible organization methods include:

- **chronological**
- **by transaction**.

Reader focus

The report should be understandable to the intended reader and often should be drafted with the expectation that third parties may read it.

Q. Sample Fraud Examination Reports

The visible pages in *Manual17* provide examples of actual-style fraud examination work products such as:

- interview memoranda
- telephone conversation memoranda
- meeting summaries
- invoice exhibits

- canceled-check reviews
- surveillance logs
- courthouse-record reviews
- anonymous tip documentation.

Why this matters

These examples show the **format, tone, and factual style** expected in practice:

- identify who, when, where
- state how the person was identified/advised
- separate facts from conclusions
- use attached exhibits and logs
- document records reviewed.

---

4. Important Terms, Definitions, and Classifications

Information-source terms

- public records
- public-record vendors
- investigative service companies
- deep web
- dark web
- internet archive
- social media evidence
- security social media sites
- due diligence
- background check.

Digital-forensics terms

- volatile data
- live collection
- hard shutdown
- graceful shutdown
- chain of custody

- write-blocker
- forensic image / mirror image / bitstream copy
- deduplication
- file-type filtering
- cloud forensics
- mobile forensics.

Asset-recovery terms

- MLA request
- letters rogatory
- tax-information exchange agreement
- civil action
- criminal action
- freezing order
- judgment
- enforcement.

Report-writing terms

- fraud examination report
- expert report
- conclusion
- opinion
- relevance
- impartiality
- chronological organization
- transaction-based organization.

Practical case-document terms

- memorandum
- surveillance log
- invoice exhibit
- canceled check review

- records review.

---

5. Red Flags, Indicators, and Warning Signs

Information gathering

- overreliance on one database
- failure to validate original sources
- outdated or abstract-only records
- privacy-restricted information being treated as freely usable.

Social media evidence

- content rapidly changing/disappearing
- lack of metadata/context
- privacy-restricted content accessed improperly
- no documentation of collection steps.

Digital evidence

- unauthorized user access to seized device
- turning systems on/off incorrectly
- missing chain of custody
- analysis done on original rather than image
- poor documentation of device status and actions taken.

Asset recovery

- delays that allow dissipation of assets
- failure to identify foreign jurisdictions early
- not assessing collectability before legal spend
- lack of local law/jurisdiction review.

Report writing

- overstated conclusions
- accusations without factual foundation
- unclear chronology
- biased language
- jargon without explanation

- opinions outside the examiner’s expertise.

---

6. Detection Methods, Audit Approaches, and Analytical Tools

Information-source methods

- multi-engine searching
- advanced operators
- archived-site review
- social media review
- public-record searching
- due diligence checks
- adverse media review
- litigation/criminal background review.

Digital-forensic methods

- live collection when justified
- forensic imaging
- keyword search
- deduplication
- date filtering
- file-type filtering
- analytic review
- cloud/mobile-specific collection planning.

Asset tracing/recovery methods

- locate jurisdictions
- identify ownership/proceeds
- engage foreign counterparts
- use MLA / letters rogatory where needed
- pursue civil/criminal routes strategically
- secure and enforce against assets.

Reporting methods

- chronological or transaction-based organization

- attach copies of key documents
- preserve support for each statement
- document interviews promptly.

---

7. Prevention and Internal Controls

Information gathering / due diligence

- validate from original sources
- consult legal counsel before sensitive background checks
- understand privacy-law limits
- preserve capture methodology.

Digital evidence

- use trained forensic personnel
- restrict access
- preserve chain of custody
- use write-blocking
- image before analysis
- document every action
- package/preserve properly.

Asset recovery

- move quickly where assets may dissipate
- assess recoverability early
- engage counsel and foreign counterparts
- use freezing/judgment tools strategically.

Report writing

- standardize memoranda/report forms
- require fact support
- separate fact from opinion
- review for clarity, neutrality, and timeliness.

---

8. Comparisons and Distinctions

Public-record vendor vs government source

- **Government source**: often original source
- **Vendor**: faster, aggregated, but may be incomplete or abstracted.

Deep web vs dark web

- **Deep web**: not indexed by search engines
- **Dark web**: specially accessed segment with anonymity features.

Live collection vs traditional shutdown-first seizure

- **Live collection**: useful for volatile data
- **Shutdown-first**: may protect some integrity but can lose volatile evidence.

Graceful shutdown vs hard shutdown

- **Graceful**: may alter/delete evidence during system processes
- **Hard**: may better preserve some states but also carries risks.

Civil action vs criminal action

- **Civil**: victim-focused compensation/remedy
- **Criminal**: punishment/public-law process, though may aid recovery indirectly.

Fraud examination report vs expert report

- **Fraud examination report**: documents results of the exam
- **Expert report**: presents specialized opinions where appropriate.

Conclusion vs opinion

- **Conclusion**: fact-based inference from evidence
- **Opinion**: interpretive statement, acceptable only in proper scope/context.

---

9. Memory Aids

Online information gathering

S-F-V-A

- **S**earch smart
- **F**ilter precisely
- **V**alidate originals
- **A**rchive quickly

Digital forensics

P-I-C-C

- **P**reserve
- **I**mage
- **C**hain of custody
- **C**ompare/analyze copy

Asset recovery

L-S-J-E

- **L**ocate assets
- **S**ecure assets
- **J**udgment
- **E**nforce

Good report

A-C-I-T

- **A**ccuracy
- **C**larity
- **I**mpartiality/relevance
- **T**imeliness

---

10. Likely Exam Questions / High-Yield Traps

- Why should a fraud examiner validate public-record database information against original sources?
- What is the main risk of interacting with a live running computer before forensic planning?
- Which data is most at risk of being lost when a system is powered down?
- Why is forensic imaging preferred before analysis?
- What is the difference between a civil action and a criminal action in fraud recovery?
- What are the five basic recovery steps noted in the visible asset-recovery section?
- Which is improper in a report: pointing out inconsistencies, or stating that the suspect is guilty?
- What makes a social media exhibit more defensible in court?

---

11. Quick Recall Sheet

Sources of information

Think: **search smart, validate, respect privacy, preserve what you find**

Digital forensics

Think: **integrity first**

- secure device
- preserve chain
- capture volatile data if justified
- image before analysis
- document everything

Asset recovery

Think: **find, freeze, sue, win, enforce**

Report writing

Think: **accurate, clear, neutral, timely**
Facts first. Avoid unsupported guilt statements.

Sample reports

Think: **memorandum style, exhibit-backed, fact-specific, date/time/person anchored**

---

12. Practice Section

10 Recall Questions

1. What are the major limitations of online public-record database searches?
2. What is the difference between the deep web and the dark web?
3. Why is social media evidence challenging from an admissibility standpoint?
4. What is volatile data?
5. Why use a write-blocking device?
6. What is a forensic image?
7. What are the five visible steps in asset recovery?
8. What is the difference between a fraud examination report and an expert report?
9. What four characteristics define a good report in the visible pages?
10. Why should an examiner avoid directly analyzing original digital evidence when possible?

10 Flashcard-Style Q&A

Q: Aggregated search source that may be fast but incomplete.
A: Public-record vendor database.

Q: Web content not indexed by ordinary search engines.
A: Deep web.

Q: An anonymity-oriented portion of the deep web requiring special access tools.
A: Dark web.

Q: Data likely lost when the machine powers down.
A: Volatile data.

Q: Device or software used to prevent writes to digital media during acquisition.
A: Write-blocker.

Q: Bit-for-bit duplicate of digital media for analysis.
A: Forensic image.

Q: Legal process often used for cross-border assistance.
A: MLA request or letters rogatory.

Q: Report quality feature meaning unbiased and only relevant information included.
A: Impartiality and relevance.

Q: Organizing report facts by event sequence.
A: Chronological organization.

Q: Organizing report facts by scheme/transaction set.
A: By transaction.

5 Situational / Application Questions

1. A fraud examiner finds a useful hit in a paid public-record database. What should be done before relying on it heavily?
2. A suspect laptop is powered on, encrypted, and connected to the network. What key forensic issue should be evaluated first?
3. A victim wants to recover stolen funds held abroad. What cross-border steps should be considered early?
4. A manager asks the examiner to state in the report that the suspect "is guilty." How should the examiner respond?
5. A social media post central to the case disappears the next day. What collection/control lesson does this illustrate?

White-Collar Crime, Occupational Fraud Theory, Fraud Risk Assessment, Ethics, and Auditors' Fraud Responsibilities

1. Big Picture Summary

This revised batch now starts with the **theoretical and empirical foundation** for fraud prevention:

- why white-collar and occupational fraud happen,
- how pressure, opportunity, and rationalization interact,
- what occupational fraud looks like in practice based on ACFE data,

- what controls reduce loss and duration,
- and how organizations, CFEs, auditors, and internal auditors should respond.

This is a very important batch for certification exams because it combines:

- **fraud theory**
- **fraud statistics**
- **fraud risk management**
- **professional ethics**
- **external audit responsibilities**
- **internal audit responsibilities**.

---

2. Must-Know Exam Points

HIGH YIELD

- **White-collar crime** includes illegal acts committed through occupational roles, and organizational culture, obedience to authority, pressure, and rationalization can contribute to it.
- **Cressey's Fraud Triangle** consists of:
    - non-shareable financial pressure
    - perceived opportunity
    - rationalization.
- Cressey's point was that **all three elements** are needed for trust violation to occur.
- **Albrecht's Fraud Scale** reframes the model around:
    - situational pressures
    - opportunities to commit fraud
    - personal integrity.
- The ACFE occupational fraud data shown in the visible pages indicates:
    - **asset misappropriation** is the most common category
    - **financial statement fraud** is the least common but costliest
    - **corruption** sits in between.
- The visible pages show that **tips** are the most common initial detection method.
- Anti-fraud controls associated with lower losses or shorter duration include visible items such as:
    - code of conduct

    - external audit of financial statements
    - internal audit department
    - management certification of statements
    - fraud training
    - anti-fraud policy
    - hotline
    - proactive data monitoring/analysis
    - surprise audits.
- Fraud risk assessment converts theory into structured prevention by identifying risks, rating them, mapping controls, and evaluating residual risk.
- CFEs must report **material matters completely**, maintain integrity and confidentiality, and avoid opinions on legal guilt or innocence.
- Auditors must maintain **professional skepticism** and respond to fraud risk, especially **management override**.

---

3. Key Concepts and Explanations

A. White-Collar Crime

The visible pages in *Manual18* discuss the social and organizational context of white-collar crime. They note that pressure, competition, obedience, corporate culture, and rationalizations can all push people toward misconduct.

Important visible themes

- competitive and performance pressure can encourage deception
- obedience to authority can lead people to act against their own moral standards
- corporations may normalize misconduct when goals dominate ethics
- management and corporate culture strongly influence employee behavior.

Why this matters

Exam questions often ask not just *what control failed*, but *what conditions encouraged the fraud*. This section provides that lens.

B. Corporate Executives and Organizational Crime

Visible pages note that organizations sometimes shield executives from accountability and that fines or penalties alone may be weak deterrents if they are small relative to the benefit of misconduct. The pages also discuss compliance vs deterrence and the role of publicity, enforcement, and governance.

High-yield distinctions

- **Compliance approach** focuses on encouraging conformity to rules.
- **Deterrence approach** focuses on increasing certainty and cost of punishment.

C. Occupational Fraud

The visible pages explain that occupational fraud is illegal activity committed through one's occupation. They also reference different forms of occupational crime, including crimes benefiting the organization, crimes by professionals, and crimes by individuals abusing their work role.

Why it matters

This provides the conceptual bridge between white-collar crime generally and the more specific ACFE occupational-fraud framework.

D. Cressey's Fraud Triangle

This is one of the most important visible sections.

The visible pages explain that Cressey studied "trust violators" and concluded that occupational fraud often arises when three factors come together:

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

1. Non-shareable financial pressure

Visible pages explain that the problem is "non-shareable" from the perpetrator's point of view. It may be:

- personal debt
- gambling
- business reversals
- social-status pressure
- fear of loss of reputation or status
- other problems the person feels cannot be openly shared.

2. Perceived opportunity

Visible pages note that opportunity exists when the person believes they can exploit a control weakness, position of trust, access, or system gap to solve the problem.

3. Rationalization

Visible pages explain that perpetrators do not usually view themselves as criminals. They justify the conduct to preserve self-image. Common rationalizations include "borrowing," deserving the money, unusual situation, or expecting to repay it later.

High-yield conclusion

The visible pages explicitly state that all three elements are needed for the trust violation to occur.

E. Cressey's Offender Types

Visible pages discuss:

- **independent businesspeople**
- **long-term violators**
- **absconders**.

These help show that rationalization and social ties can differ across perpetrator types.

F. Albrecht's Fraud Scale

The visible pages explain that Albrecht reframed the model into the **Fraud Scale**, which includes:

- situational pressures
- opportunities to commit fraud
- personal integrity.

Key idea

When situational pressure and opportunity are high, and personal integrity is low, occupational fraud is more likely.

Exam distinction

- **Fraud Triangle** uses rationalization.
- **Fraud Scale** substitutes personal integrity as the balancing factor.

G. ACFE Report to the Nations / Occupational Fraud Statistics

The visible pages contain several highly testable findings based on the 2024 ACFE data.

Projected loss

The visible pages note ACFE's estimate that a typical organization loses about **5% of revenue** to fraud each year, while also explaining that this is an estimate and global totals cannot be perfectly measured.

Category patterns

Visible pages show:

- **Asset misappropriation** is most common
- **Corruption** is less common than asset misappropriation

- **Financial statement fraud** is least common but has the highest median loss.

Why this matters

This is one of the most common exam-tested data points.

H. Duration of Fraud Schemes

Visible pages indicate:

- median duration for all cases was **12 months**
- frauds detected in the first 6 months tend to cause much smaller losses
- longer-running schemes cause much larger losses.

Visible pages also show some scheme types, such as billing, check/payment tampering, expense reimbursements, payroll, and financial statement fraud, often lasting longer than others.

Exam lesson

Earlier detection materially reduces damage.

I. Detection of Occupational Fraud

The visible pages show that **tips** are the most common initial detection method, followed by internal audit and management review.

Visible pages also show tip sources, with **employees** being the largest source, followed by customers, anonymous sources, vendors, and others.

High-yield lesson

Hotlines and speak-up culture matter because tips dominate detection.

J. Anti-Fraud Controls and Their Effectiveness

Visible pages list common anti-fraud controls and show that many are associated with lower median losses and/or shorter fraud duration. Visible controls include:

- code of conduct
- external audit of financial statements
- internal audit department
- management certification of financial statements
- management review
- anti-fraud policy

- employee support programs
- fraud training
- hotline
- dedicated fraud function/team
- surprise audits
- proactive data monitoring/analysis
- job rotation / mandatory vacation
- rewards for whistleblowers.

Visible commentary notes that external audits, internal audit functions, management certification, data monitoring, and surprise audits were among the more useful tools in reducing loss.

K. Perpetrator Characteristics and Behavioral Red Flags

Visible pages show patterns about:

- position/authority
- department
- gender
- age
- prior convictions
- disciplinary history
- common behavioral red flags.

Highly testable visible red flags

The visible chart includes common behavioral signs such as:

- living beyond means
- financial difficulties
- unusually close association with vendor/customer
- unwillingness to share duties
- control issues / unwillingness to delegate
- irritability or suspiciousness
- “wheeler-dealer” attitude
- recent divorce or family problems

- addiction problems.

Important nuance

Visible pages indicate that most perpetrators had **no prior criminal conviction** and many had **no prior employment-related discipline**, so absence of a record does not equal low fraud risk.

L. Corporate Governance

Later visible pages in *Manual18* move into **corporate governance**, discussing:

- board of directors
- board committees
- audit committee
- compensation committee
- nominating committee
- management
- shareholders
- governance principles such as accountability, transparency, fairness, and responsibility.

Visible pages also discuss OECD principles and the role of governance in fighting fraud.

High-yield point

Fraud prevention is not only a control issue; it is also a **governance and oversight issue**.

M. Fraud Risk Assessment

Now that *Manual18* provides the theory and data, *Manual20* shows how organizations operationalize this into a fraud risk assessment.

Visible FRA themes

- identify vulnerable activities
- know who puts the organization at greatest risk
- develop mitigation plans
- identify high-risk areas
- assess anti-fraud controls
- comply with regulations and standards
- keep assessment active and relevant.

Visible fraud-risk categories

- fraudulent financial reporting
- asset misappropriation
- corruption
- external fraud
- regulatory/legal misconduct
- reputational risk
- technology risk.

Visible framework components

- environment and culture
- adequacy and quality of anti-fraud controls
- leadership behaviors and communication
- quality and consistency of complaint and response protocols.

Why this matters

Manual18 explains *why* fraud happens; Manual20 explains how to systematically assess and reduce that risk.

N. ACFE Ethics and Professional Standards

Manual21 adds the professional conduct layer.

Visible themes include:

- complete reporting of material matters
- avoiding distortion of facts
- professional improvement
- integrity and objectivity
- competence
- due professional care
- confidentiality
- evidence-based reporting
- no opinion on legal guilt or innocence.

High-yield point

The examiner’s duty is to present material facts and supported conclusions, not to act as judge or prosecutor.

O. Auditors' and Internal Auditors' Fraud-Related Responsibilities

Manual19 adds external and internal audit responsibilities.

Visible external-audit themes include:

- professional skepticism
- fraud-risk discussion among the engagement team
- inquiries of management, governance, and internal audit
- evaluation of fraud-risk factors
- response to management override
- communication and documentation.

Visible internal-audit themes include:

- fraud-related competency
- due professional care
- strategic planning
- engagement risk assessment
- communication of risk acceptance
- assurance over fraud governance, risk management, and controls.

---

4. Important Terms, Definitions, and Classifications

White-collar / occupational fraud terms

- white-collar crime
- occupational fraud
- compliance
- deterrence
- corporate governance
- audit committee
- accountability
- transparency
- fairness
- responsibility.

Fraud-theory terms

- non-shareable financial pressure
- perceived opportunity
- rationalization
- fraud triangle
- fraud scale
- personal integrity
- situational pressure.

Occupational-fraud statistics terms

- median loss
- duration
- detection method
- tip source
- anti-fraud control
- behavioral red flag.

Fraud risk assessment terms

- inherent fraud risk
- likelihood
- significance
- preventive control
- detective control
- residual risk
- fraud risk portfolio.

Ethics / audit terms

- material matters
- distortion
- professional skepticism
- management override
- those charged with governance
- due professional care

- confidentiality.

---

5. Red Flags, Indicators, and Warning Signs

Perpetrator behavioral red flags

Visible examples include:

- living beyond means
- financial difficulties
- close association with vendors/customers
- unwillingness to share duties
- control issues
- suspiciousness or irritability
- wheeler-dealer attitude
- family problems
- addiction issues.

Organizational / environmental red flags

Visible concepts across Manual18 and Manual20 include:

- unrealistic performance pressure
- weak tone at the top
- low trust culture
- poor segregation of duties
- ineffective whistleblower and complaint handling
- excessive pressure without ethics support
- management override
- weak control environment.

Audit / ethics red flags

- omission of material matters
- biased or overstated conclusions
- unsupported opinions
- unusual journal entries
- significant unusual transactions

- estimate bias
- inconsistent management explanations.

---

6. Detection Methods, Audit Approaches, and Analytical Tools

Occupational fraud detection

Visible data show:

- tips are the leading initial detection method
- internal audit and management review are next major methods
- active detection tends to reduce loss and duration.

Fraud risk assessment methods

Visible methods include:

- interviews
- focus groups
- surveys
- anonymous feedback
- control evaluation
- risk scoring by likelihood and significance
- aggregation into fraud risk portfolio.

Auditor responses

Visible auditor responses include:

- team discussion
- inquiries
- journal-entry testing
- review of estimates for bias
- review of unusual transactions
- evaluating audit evidence and implications of misstatements
- communication and documentation.

---

7. Prevention and Internal Controls

Anti-fraud controls

Visible controls from Manual18 and Manual20 include:

- code of conduct
- anti-fraud policy
- hotline
- employee support programs
- fraud training
- management review
- internal audit
- external audit
- certification of statements
- proactive data monitoring
- surprise audits
- segregation of duties
- security controls
- review of related-party transactions.

Governance controls

Visible governance measures include:

- independent board oversight
- audit committee activity
- clear accountability
- timely transparent disclosure
- fair treatment of shareholders
- ethical leadership.

Ethics/professional controls

- scope understanding
- competence and supervision
- confidentiality
- evidence-based reporting
- complete disclosure of material matters.

---

8. Comparisons and Distinctions

Fraud Triangle vs Fraud Scale

- **Fraud Triangle**: pressure, opportunity, rationalization
- **Fraud Scale**: situational pressure, opportunity, personal integrity.

Compliance vs deterrence

- **Compliance**: encourage voluntary conformity to rules
- **Deterrence**: increase certainty/cost of punishment.

Common vs costly

- **Asset misappropriation**: most common
- **Financial statement fraud**: least common but costliest
- **Corruption**: middle ground.

Inherent risk vs residual risk

- **Inherent**: before controls
- **Residual**: after considering controls and mitigation.

CFE vs auditor role

- **CFE**: investigation, evidence, reporting, ethics
- **External auditor**: reasonable assurance on financial statements
- **Internal auditor**: assurance/advisory role on fraud governance, risk, and controls.

---

9. Memory Aids

Fraud Triangle

P-O-R

- **P**ressure
- **O**pportunity
- **R**ationalization

Fraud Scale

S-O-I

- **S**ituational pressure
- **O**pportunity
- **I**ntegrity

Anti-fraud effectiveness

T-H-A-D

- **T**ips
- **H**otline
- **A**udit
- **D**ata monitoring

Risk assessment

L-S-C-R

- **L**ikelihood
- **S**ignificance
- **C**ontrols
- **R**esidual risk

---

10. Likely Exam Questions / High-Yield Traps

- Which fraud category is most common, and which is costliest?
- What are the three elements of the Fraud Triangle?
- How does the Fraud Scale differ from the Fraud Triangle?
- Why are tips so important in occupational fraud detection?
- What types of anti-fraud controls are associated with lower losses?
- Can the absence of a criminal record be treated as evidence of low fraud risk?
- Why is leadership behavior included in fraud risk assessment?
- Can a CFE state that a suspect is legally guilty?
- What is the auditor expected to test when management override risk exists?

---

11. Quick Recall Sheet

White-collar / occupational fraud

Think: **pressure + culture + opportunity + justification**

Fraud theory

- Fraud Triangle = pressure, opportunity, rationalization
- Fraud Scale = pressure, opportunity, integrity

ACFE data

- Asset misappropriation = most common
- Financial statement fraud = least common, highest loss
- Tips = most common detection source

Fraud prevention

Think: **governance + culture + controls + reporting channels + analytics**

Ethics and audit

Think: **material facts, no distortion, skepticism, no guilt opinion**

---

12. Practice Section

10 Recall Questions

1. What are the three elements of the Fraud Triangle?
2. What is meant by a non-shareable financial problem?
3. How does the Fraud Scale differ from the Fraud Triangle?
4. Which occupational fraud category is most common?
5. Which occupational fraud category has the highest median loss?
6. What is the most common initial detection method for occupational fraud?
7. Name four anti-fraud controls visible in the charts/pages.
8. Why is leadership behavior relevant to fraud risk assessment?
9. What does the ACFE ethics rule on complete reporting of material matters require?
10. What is one classic external-audit response to management override?

10 Flashcard-Style Q&A

Q: Pressure, opportunity, and rationalization model.
A: Fraud Triangle.

Q: Situational pressure, opportunity, and personal integrity model.
A: Fraud Scale.

Q: Most common occupational fraud category.
A: Asset misappropriation.

Q: Least common but costliest occupational fraud category.
A: Financial statement fraud.

Q: Most common initial detection method.
A: Tip.

Q: Leading employee-reporting mechanism often tied to tips.
A: Hotline / whistleblower mechanism.

Q: Fraud risk before controls.
A: Inherent risk.

Q: Fraud risk after controls.
A: Residual risk.

Q: Ethical requirement to disclose material matters if omission would distort facts.
A: Complete reporting of material matters.

Q: Major audit response area where management can bypass controls.
A: Management override.

5 Situational / Application Questions

1. A company has an anti-fraud policy on paper, but leaders pressure staff to hit impossible targets and ignore abuse. Which risk area is most relevant?
2. An employee has no criminal record, no prior discipline, and is widely trusted. Does that eliminate occupational fraud risk?
3. A fraud examiner believes a suspect stole funds but only has partial evidence. What should the examiner avoid stating in the report?
4. A fraud scheme lasted 24 months before discovery. What does the visible ACFE data suggest about likely loss impact relative to shorter-duration schemes?
5. An organization wants to prevent fraud more effectively. Based on the visible materials, where should it focus first: only punishing offenders after the fact, or strengthening detection and preventive controls such as hotlines, audit, and analytics?

Fraud Examiners Manual — Coherent Study Version

Recommended Study Order

Part 1 — Foundations: Accounting, Financial Statements, and Financial Statement Fraud

Part 2 — Core Occupational Fraud Schemes

Part 3 — Specialized Fraud Schemes

Part 4 — Law, Rights, Evidence, and Testifying

Part 5 — Investigation Execution and Reporting

Part 6 — Fraud Prevention, White-Collar Crime, Governance, and Fraud Risk Assessment

Part 7 — Ethics, Professional Standards, and Auditors' / Internal Auditors' Fraud Responsibilities

This sequence is the most retention-friendly because it moves from **how fraud affects records**, to **what the schemes are**, to **how they are investigated**, then to **how they are prevented and governed**.

Part 1 — Foundations: Accounting, Financial Statements, and Financial Statement Fraud

Big Picture Summary

Start here because fraud examiners must understand how transactions flow through accounting records and financial statements before they can understand how fraud distorts them. The opening material covers accounting concepts, financial statements, recognition, accrual vs cash basis, and then financial statement fraud schemes such as fictitious revenues, timing differences, improper asset valuation, concealed liabilities and expenses, and improper disclosures.

Must-Know Points

The accounting equation is **Assets = Liabilities + Owners' Equity**. The main statements are the balance sheet, income statement, changes in equity, and cash flow statement. Accrual accounting records events when earned or incurred, not when cash moves. Fraud questions often test whether an issue affects recognition, valuation, classification, timing, or disclosure.

Financial statement fraud is broader than fake revenue. It includes:

- fictitious revenues,
- timing differences,
- improper asset valuation,
- concealed liabilities and expenses,
- improper disclosures.

Key Concepts

Concealed liabilities and expenses overstate income by understating obligations or period costs. **Improper capitalization** shifts expenses to the balance sheet. **Improper disclosures** can make statements misleading even when reported numbers appear plausible. Vertical analysis, horizontal analysis, and ratio analysis are core detection tools.

Memory Hook

R-V-C-D-T

- **R**ecognition
- **V**aluation
- **C**lassification
- **D**isclosure
- **T**iming

If a question asks how the fraud affects the statements, test it against those five.

Likely Exam Traps

A company may have correctly recorded an amount but still mislead users through omitted disclosures. A cost booked as an asset instead of an expense is not an omission; it is a valuation/classification/timing distortion. Strong profits with weak cash flow can be a classic warning sign.

Part 2 — Core Occupational Fraud Schemes

Big Picture Summary

This part covers the core frauds most commonly tested under occupational fraud: cash receipts, billing schemes, shell companies, pay-and-return schemes, personal purchases, payroll fraud, and ghost employees. These are the practical fraud schemes that usually sit behind "asset misappropriation."

Must-Know Points

Billing schemes involve the victim paying false, inflated, or unauthorized invoices. A shell company is fake or controlled by the fraudster. A pay-and-return scheme uses a real vendor but diverts the refund from an intentional overpayment. Payroll fraud often centers on ghost employees. Personal purchases with company funds are a common sub-scheme.

Key Concepts

Shell company vs pay-and-return is a major distinction. In a shell-company scheme, the vendor itself is fake or controlled. In pay-and-return, the vendor is real but the refund is intercepted. Ghost employees may be fictitious, terminated employees, or real individuals who do not actually work there.

Red Flags

Shared employee/vendor addresses, duplicate invoices, odd invoice quality, unusual one-time charges, vendor favoritism, poor receiving evidence, or payroll names that no one knows are classic warning signs.

Memory Hook

V-I-P-P

- **V**endor setup
- **I**nvoice manipulation
- **P**ayment approval
- **P**ersonal benefit

Likely Exam Traps

Real vendor does not always mean no fraud. Legitimate vendor plus diverted refund still equals fraud. Ghost employee schemes often exploit weak onboarding, payroll change, timesheet, or termination controls rather than just weak payroll distribution.

Part 3 — Specialized Fraud Schemes

Big Picture Summary

This part groups the broader scheme families outside basic occupational fraud: corruption and conflicts of interest, theft of data and intellectual property, mortgage fraud, insurance fraud, consumer fraud, cyberfraud, and contract/procurement fraud. This is the most scheme-heavy part after Part 2.

3A. Corruption and Conflicts of Interest

Conflict of interest exists when an undisclosed personal interest compromises duty to the employer. Appearance also matters. Anti-corruption programs require more than policy—they need tone at the top, training, due diligence, reporting, enforcement, and monitoring.

3B. Theft of Data and Intellectual Property

Protect **confidentiality, integrity, and availability**. Competitive intelligence is legal and ethical information gathering; espionage is illegal or unethical acquisition. Common methods include human intelligence, surveillance, dumpster diving, insiders, and attacks.

3C. Mortgage Fraud and New Account Fraud

Mortgage fraud involves false identities, inflated values, concealed concessions, fake collateral, foreclosure rescue scams, short-sale abuse, flopping, equity skimming, and reverse mortgage abuse. New accounts are high-risk because there is no normal history yet.

3D. Insurance Fraud

Distinguish **premium fraud** from **claimant fraud**. Premium fraud underpays the insurer; claimant fraud overcollects from the insurer. Visible material covers inflated inventory, fake thefts, paper boats, fraudulent death claims, vanishing premium, workers' compensation fraud, organized rings, and red flags in claim packages and medical/provider patterns.

3E. Consumer Fraud

Know the distinction:

- **Pyramid** = recruitment-driven structure
- **Ponzi** = fake investment returns funded by later investors.

3F. Cyberfraud

Know:

- phishing,
- spear phishing,
- business email compromise,
- vishing,
- smishing,
- pharming,
- catfishing,
- reverse social engineering,
- password cracking,
- keylogging.

BEC is especially high-yield because it often redirects vendor or executive payments, steals payroll/direct deposit data, or triggers gift-card fraud.

3G. Contract and Procurement Fraud

Cost mischarging can be:

- accounting mischarges,
- material mischarges,
- labor mischarges. Vendor due diligence, vendor master controls, receiving controls, approval controls, and monitoring are central.

Memory Hook

C-D-M-I-C-C-P

- **C**orruption
- **D**ata/IP
- **M**ortgage
- **I**nsurance
- **C**onsumer
- **C**yber
- **P**rocurement

Likely Exam Traps

Ponzi and pyramid are not identical. Premium fraud and claimant fraud run in opposite directions. Competitive intelligence is not automatically espionage. A mortgage scheme can combine identity fraud, appraisal fraud, occupancy misrepresentation, and distress abuse at once.

Part 4 — Law, Rights, Evidence, and Testifying

Big Picture Summary

This part explains the legal environment around fraud: securities fraud concepts, tax fraud, rights during examinations, evidence, privileges, and testimony. This is the part that turns fraud knowledge into litigation- and investigation-ready knowledge.

4A. Securities Fraud

Know traditional securities like stocks, bonds, and CDs, but also futures, options, OTC options, and investment contracts. Many fraud schemes can be securities-related if they meet the investment-contract characteristics. Ponzi schemes, some pyramids, prime bank note schemes, viaticals, partnerships, hedge funds, and oil/gas/mineral interests may fall into this area.

4B. Tax Fraud

Tax evasion is illegal; **tax avoidance** is lawful minimization. Willfulness matters. Common indicators include double books, hidden assets, false-name accounts, overstated deductions, and fictitious transactions. Know the difference between civil, criminal, and administrative consequences.

4C. Individual Rights During Examinations

Employees may have duties to cooperate, but they may also have privacy, contractual, whistleblower, and labor-law protections depending on jurisdiction. Preservation duties are especially important once litigation is anticipated.

4D. Evidence

Main evidence types are testimonial, documentary, and digital. Chain of custody supports authenticity and integrity. Impeachment attacks credibility through bias, inconsistent statements, inability to observe, reputation for untruthfulness, or certain convictions.

4E. Privileges

Know the distinction between:

- attorney-client / legal professional privilege,
- legal advice privilege,
- litigation privilege / work-product,
- self-evaluation privilege,
- marital privilege,
- informant identity privilege,
- accountant-client privilege in some places.

4F. Testifying

A fraud examiner may be a fact witness, expert witness, or both. Factual testimony comes from firsthand knowledge; expert testimony comes from specialized knowledge and opinion. Do not confuse information gathered in investigation with admissible evidence.

Memory Hook

S-T-R-E-T

- **S**ecurities
- **T**ax
- **R**ights
- **E**vidence
- **T**estifying

Likely Exam Traps

Reasonable suspicion of fraud does not erase privacy or privilege rules. A good investigation fact may still be inadmissible unless properly preserved and presented. A futures contract creates obligation; an option gives the holder a right, not an obligation.

Part 5 — Investigation Execution and Reporting

Big Picture Summary

This part is the “how to actually do it” section: planning and conducting a fraud examination, collecting evidence, sources of information, social media and public records, digital forensics, tracing illicit transactions, asset recovery, report writing, and sample reports.

5A. Planning and Conducting a Fraud Examination

Start with known facts, goals, scope, time frame, roles, operational issues, resources, need-to-know communication, and whether law enforcement or counsel should be involved. Keep the plan flexible and documented. Avoid alerting suspects unnecessarily.

5B. Collecting Evidence

Think:

- testimonial,
- documentary,
- digital.
  Document everything. Chain of custody and confidentiality begin at the first touchpoint.

5C. Sources of Information

Use smart searching, public records, investigative vendors, archived sites, social media, due diligence, and background checks. But validate important information back to original sources and respect privacy and legal limitations.

5D. Digital Forensics

Main rule: protect evidence integrity. Decide carefully whether to preserve a live system, collect volatile data, or power it down. Use chain of custody, write-blockers, forensic imaging, and documented processing methods such as keyword searching, deduplication, date filtering, and file-type filtering. Cloud and mobile forensics introduce additional complications.

5E. Tracing Illicit Transactions and Asset Recovery

Cross-border tracing may require MLA requests, letters rogatory, and foreign counterpart coordination. Recovery generally follows:

1. evaluate recovery potential,
2. commence legal process,
3. secure assets,
4. obtain judgment,
5. enforce judgment.

5F. Report Writing

Good reports are:

- accurate,

- clear,
- impartial and relevant,
- timely.
  Fraud examination reports and expert reports differ. Supported conclusions are allowed; opinions must stay within proper limits. Do not state legal guilt or innocence.

5G. Sample Fraud Examination Reports

The sample memoranda show what defensible work product looks like: date/time anchored, person identified, facts separated from conclusions, exhibits attached, interviews summarized cleanly, surveillance logs structured, and records reviews explicitly described.

Memory Hook

P-S-D-T-R

- **P**lan
- **S**ource
- **D**ocument / digital evidence
- **T**race
- **R**eport

Likely Exam Traps

The best investigation is not the one with the most activity; it is the one with the best preservation, documentation, scope discipline, and report defensibility. Social media evidence is useful but can disappear quickly and raise authenticity issues.

Part 6 — Fraud Prevention, White-Collar Crime, Governance, and Fraud Risk Assessment

Big Picture Summary

This part explains *why* fraud occurs and *how organizations reduce it*. It combines white-collar crime concepts, occupational fraud theory, corporate governance, ACFE statistics, anti-fraud controls, and fraud risk assessment frameworks. This is the conceptual heart of prevention and deterrence.

6A. White-Collar Crime and Organizational Crime

Pressure, competition, obedience, rationalization, culture, and leadership matter. Compliance and deterrence are different theories of control. Fines alone may be weak deterrents if the perceived benefit of misconduct remains high.

6B. Occupational Fraud Theory

Know **Cressey's Fraud Triangle**:

- non-shareable financial pressure,
- perceived opportunity,

- rationalization.
  Know **Albrecht's Fraud Scale**:
- situational pressures,
- opportunities,
- personal integrity.

6C. ACFE Report to the Nations Themes

High-yield points:

- organizations lose an estimated 5% of revenue to fraud yearly,
- asset misappropriation is most common,
- corruption is intermediate,
- financial statement fraud is least common but most expensive,
- longer-running schemes cause larger losses,
- tips are the leading detection method,
- active controls reduce loss and duration.

6D. Perpetrator Traits and Red Flags

Most perpetrators had no prior conviction and many had no prior discipline. Common behavioral red flags include living beyond means, financial difficulty, unusually close vendor/customer relationships, unwillingness to share duties, irritability, wheeler-dealer attitude, addiction, and family problems.

6E. Corporate Governance

Know the role of:

- board,
- audit committee,
- compensation committee,
- nominating committee,
- management,
- shareholders.
  Core governance principles include accountability, transparency, fairness, and responsibility. Audit committees are central to fraud oversight. OECD governance principles reinforce effective framework, shareholder rights, transparency, disclosure, and board responsibilities.

6F. Fraud Risk Assessment

Use fraud theory and data to identify inherent risks, rate likelihood and significance, map preventive and detective controls, evaluate control effectiveness, and determine residual risk. Also evaluate environment and culture, leadership behavior, and complaint/response protocols.

Memory Hooks

P-O-R = Fraud Triangle
S-O-I = Fraud Scale
L-S-C-R = Fraud risk assessment

- Likelihood
- Significance
- Controls
- Residual risk

Likely Exam Traps

A strong written policy does not equal a strong anti-fraud culture. A clean criminal record does not equal low fraud risk. Financial statement fraud is not the most common category; it is the costliest.

Part 7 — Ethics, Professional Standards, and Auditors' / Internal Auditors' Fraud Responsibilities

Big Picture Summary

This final part explains what professionals must do once fraud risk or fraud work exists: CFEs must meet ethical and professional standards; external auditors must address material misstatement due to fraud; internal auditors must provide assurance over fraud governance, risk management, and controls.

7A. ACFE Ethics and Professional Standards

Key duties:

- integrity and objectivity,
- competence,
- due professional care,
- confidentiality,
- communication with client/employer,
- evidence-based reporting,
- complete reporting of material matters,
- no opinion on legal guilt or innocence.

7B. External Auditors' Fraud Responsibilities

Auditors aim for reasonable assurance, not a guarantee. Core themes:

- professional skepticism,
- engagement-team fraud discussion,
- fraud-risk inquiries,

- evaluation of fraud-risk factors,
- responses to management override,
- communication and documentation.

Management override response is especially high-yield:

- test journal entries and adjustments,
- review accounting estimates for bias,
- examine unusual transactions outside normal business.

7C. Internal Auditors' Fraud Responsibilities

Internal audit is not sole owner of fraud prevention. But it plays an important role in assurance over fraud governance, fraud risk management, and anti-fraud controls. The visible pages connect this with the Three Lines Model and the IIA's Global Internal Audit Standards. Core expectations include competency, due care, planning strategically, engagement risk assessment, effective communication, and raising acceptance of unacceptable risks.

Memory Hook

I-C-D-C

- **I**ntegrity
- **C**ompetence
- **D**ue care
- **C**onfidentiality

For auditor override response: **J-E-U**

- **J**ournal entries
- **E**stimates
- **U**nusual transactions

Likely Exam Traps

A CFE may support a conclusion but must not state legal guilt. Reasonable assurance is not absolute assurance. Internal audit supports fraud governance and assurance but does not replace management's ownership of controls.

Final Compressed Recall Sheet

If you only remember one line per part:

Part 1: Fraud distorts records through recognition, valuation, classification, timing, and disclosure.

Part 2: Core occupational fraud is mostly asset misappropriation through billing, payroll, purchasing, and cash schemes.

Part 3: Specialized schemes include corruption, data/IP theft, mortgage, insurance, consumer, cyber, and procurement fraud.

Part 4: Law and evidence require correct classification, preservation, privilege awareness, and proper testimony.

Part 5: Good investigations are planned, documented, evidence-preserving, and report-defensible.

Part 6: Fraud prevention depends on theory, culture, governance, controls, risk assessment, and active detection.

Part 7: Professionals must be ethical, evidence-based, skeptical, and clear about their exact responsibilities.

Foundations: Accounting, Financial Statements, and Financial Statement Fraud

1. Big Picture Summary

This part is the foundation of the whole reviewer. Before studying fraud schemes, investigations, and controls, you need to understand **how transactions are recorded, how financial statements are built, and how fraud distorts them**. The opening part of the manual starts with **accounting concepts**, then moves into **financial statement fraud**, making this the correct first study block.

For certification exams, this part matters because many questions are really testing whether you can identify:

- what account is affected,
- which financial statement is distorted,
- whether the issue is one of **recognition, valuation, classification, timing, or disclosure**,
- and how the fraud changes profit, assets, liabilities, equity, or cash flow.

---

2. Must-Know Points

HIGH YIELD

- The basic accounting equation is **Assets = Liabilities + Owners' Equity**.
- Fraud examiners must understand the **accounting cycle**, **journal entries**, and **adjusting entries** because fraud often enters through false, omitted, backdated, or misclassified entries.
- The major financial statements are:
    - balance sheet / statement of financial position
    - income statement / statement of profit or loss
    - statement of changes in owners' equity
    - statement of cash flows.
- **Accrual accounting** is central. Revenue is recognized when earned and expenses when incurred or matched, not simply when cash moves.
- Financial statement fraud commonly includes:
    - fictitious revenues

    - timing differences
    - improper asset valuation
    - concealed liabilities and expenses
    - improper disclosures.
- Concealed liabilities and expenses overstate income by understating obligations or costs.
- Improper disclosures can make statements misleading even if some recorded numbers look plausible.
- Core detection tools include:
    - vertical analysis
    - horizontal analysis
    - ratio analysis.

---

3. Key Concepts and Explanations

A. Accounting Equation

Assets = Liabilities + Owners' Equity

This is the backbone of accounting. Nearly every exam question in this section can be simplified by asking: "What changed in assets, liabilities, or equity?"

Why it matters:

- If liabilities are hidden, equity and profit may appear too high.
- If expenses are omitted, net income is overstated.
- If assets are inflated, the balance sheet becomes misleading.

B. Accounting Cycle and Journal Entries

The manual's opening section explains that fraud examiners need to understand how transactions move from source events into recorded accounting information and finally into the financial statements. Journal entries and adjusting entries are especially important because fraud often happens through entries that are false, unsupported, mistimed, or omitted.

Exam takeaway:

- Fraud may be committed by recording something false.
- Fraud may also be committed by **not recording** something that should have been recorded.

C. Cash Basis vs Accrual Basis

Cash basis records events when cash is received or paid.
Accrual basis records events when revenue is earned and when expenses are incurred or matched. The visible pages indicate GAAP-based reporting generally relies on accrual accounting because it better reflects economic activity.

Why this matters:
Many fraud questions exploit timing differences between:

- cash received vs revenue earned
- cash paid vs expense incurred.

D. Major Financial Statements

1. Balance Sheet / Statement of Financial Position

Shows assets, liabilities, and equity at a point in time.

2. Income Statement / Statement of Profit or Loss

Shows revenues and expenses over a period, ending in net income or loss.

3. Statement of Changes in Owners' Equity

Shows changes in investment, earnings, and distributions.

4. Statement of Cash Flows

Shows operating, investing, and financing cash flows.

Why this matters:
Exam questions often ask which statement is distorted, or how one statement looks strong while another reveals stress. For example, overstated profits with weak operating cash flow can be suspicious.

E. Recognition of Elements

The visible opening material states that recognition generally requires:

1. probable future economic benefit, and
2. a cost or value that can be measured reliably.

This matters for questions involving:

- liabilities,
- reserves,
- provisions,
- receivables,
- impairments,
- expense accruals.

F. Financial Statement Fraud

The visible table-of-contents pages show that financial statement fraud includes:

- what financial statement fraud is,
- why it is committed,

- trends,
- schemes,
- red flags,
- detection methods,
- financial statement analysis,
- interviews,
- and prevention.

The major scheme categories visible are:

- fictitious revenues
- timing differences
- improper asset valuation
- concealed liabilities and expenses
- improper disclosures.

---

4. Important Terms and Definitions

Asset — resource owned or controlled that is expected to provide benefit.

Liability — obligation or claim against the entity's resources.

Owners' equity — residual interest after liabilities are deducted from assets.

Journal entry — formal accounting record of a transaction.

Adjusting entry — period-end entry to update balances appropriately.

Cash basis accounting — recognizes transactions when cash moves.

Accrual basis accounting — recognizes transactions when earned or incurred.

Recognition — recording an item in the financial statements when the recognition criteria are met.

Materiality — significance of information to user decisions.

Concealed liabilities and expenses — understating liabilities or expenses to overstate income.

Improper capitalization — recording a current expense as an asset.

Improper disclosures — failure to disclose required material information.

Contingent liability — possible obligation depending on uncertain future events.

Subsequent event — event after reporting date that may need adjustment or disclosure.

Related-party transaction — transaction with a connected person or entity that may not be arm's length.

---

5. Comparisons and Distinctions

Cash Basis vs Accrual Basis

- **Cash basis**: focuses on cash movement.
- **Accrual basis**: focuses on economic activity.

Balance Sheet vs Income Statement

- **Balance sheet**: position at a point in time.
- **Income statement**: performance over a period.

Recognition vs Disclosure

- **Recognition**: item appears in the statements themselves.
- **Disclosure**: explanatory information appears in notes or related presentation.

Expense Omission vs Improper Capitalization

- **Expense omission**: expense or liability is not recorded.
- **Improper capitalization**: expense is recorded, but as an asset instead of a period cost.

Quantitative Error vs Misleading Presentation

- A number can be wrong because it was measured or recorded incorrectly.
- A statement can also be misleading because required disclosures were omitted.

---

6. Memory Hooks

Accounting equation

A = L + OE

Main financial statements

B-I-E-C

- **B**alance sheet
- **I**ncome statement
- **E**quity statement
- **C**ash flow statement

Recognition rule

P-M

- **P**robable benefit

- **M**easurable reliably

Fraud distortion checklist

R-V-C-T-D

- **R**ecognition
- **V**aluation
- **C**lassification
- **T**iming
- **D**isclosure

This is the best memory tool for Part 1. If a question asks how the fraud worked, run through those five.

---

7. Likely Exam / High-Yield Points

- Concealed liabilities and expenses usually **overstate earnings**.
- Improper disclosures often involve:
    - contingent liabilities,
    - subsequent events,
    - management fraud,
    - related-party transactions,
    - accounting changes.
- Hidden liabilities may be easier to commit than fake recorded transactions because omissions can leave less obvious trail.
- Ratio analysis does not prove fraud, but it helps identify where to investigate further.
- Questions may present apparently strong profits but weak cash flow or unusual payable trends. That can point to omitted liabilities or manipulated results.

---

8. Quick Recall Sheet

What comes first in the reviewer?

Accounting Concepts, then **Financial Statement Fraud**.

Core equation

Assets = Liabilities + Owners' Equity

Main accounting methods

Cash basis vs accrual basis

Main financial statements

Balance sheet, income statement, changes in equity, cash flow statement

Main financial statement fraud types

- fictitious revenues
- timing differences
- improper asset valuation
- concealed liabilities and expenses
- improper disclosures.

Best detection lenses

- vertical analysis
- horizontal analysis
- ratio analysis.

Best Part 1 recall rule

Ask: **Is the problem recognition, valuation, classification, timing, or disclosure?**

---

9. Recall Questions

1. What is the basic accounting equation?
2. What is the main difference between cash basis and accrual basis accounting?
3. What are the four major financial statements identified in the opening material?
4. What two general conditions are needed for recognition of an item in the financial statements?
5. What is improper capitalization?
6. What is the effect of concealing liabilities and expenses on reported profit?
7. Name five categories commonly associated with improper disclosures.
8. What is the difference between recognition and disclosure?
9. What are the three financial statement analysis methods specifically noted in the visible pages?
10. Why can omitted liabilities be harder to detect than some fabricated recorded transactions?

---

10. Flashcard-Style Q&A

Q: Assets = ?
A: Liabilities + Owners' Equity.

Q: Accounting method that records revenue when earned and expenses when incurred.
A: Accrual basis accounting.

Q: Statement showing financial position at a point in time.
A: Balance sheet / statement of financial position.

Q: Statement showing revenues and expenses over a period.
A: Income statement / statement of profit or loss.

Q: Recording a current expense as an asset.
A: Improper capitalization.

Q: Understating obligations or costs to overstate income.
A: Concealed liabilities and expenses.

Q: Failure to disclose required material information.
A: Improper disclosure.

Q: Analysis of statement items as percentages within the same period.
A: Vertical analysis.

Q: Comparing financial statement items across periods.
A: Horizontal analysis.

Q: A possible obligation depending on uncertain future events.
A: Contingent liability.

---

11. Situational / Application Questions

1. A company records a repair expense as equipment. What kind of fraud/distortion is this, and what is the likely effect on current-period income?
2. A company reports strong profits, but operating cash flow weakens while accounts payable look unusually low. What financial statement fraud area should be considered first?
3. A lawsuit likely to result in payment is not disclosed or accrued. Is this mainly a recognition issue, a disclosure issue, or potentially both?
4. A transaction amount appears properly recorded, but the related-party nature of the deal is omitted from the notes. What kind of problem is this?
5. An examiner notices a major shift in ratios but no obvious single fake entry. What should that suggest about the next step?

---

12. 1-Minute Review Version

Part 1 is about understanding how accounting works so you can see how fraud distorts it. Learn the accounting equation, the four main statements, and accrual accounting. Then memorize the major financial statement fraud types: fictitious revenues, timing differences, improper asset valuation, concealed liabilities/expenses, and improper disclosures. For almost every exam question, ask whether the issue is recognition, valuation, classification, timing, or disclosure.

---

13. 5-Minute Review Version

Start with the basics: **Assets = Liabilities + Owners' Equity**. Know the balance sheet, income statement, equity statement, and cash flow statement. Understand accrual accounting because fraud often manipulates when something is recognized, not just whether cash moved. Recognition generally requires probable benefit and reliable measurement.

Financial statement fraud includes fictitious revenues, timing differences, improper asset valuation, concealed liabilities and expenses, and improper disclosures. Concealed liabilities and expenses overstate profit. Improper capitalization shifts expense into assets. Improper disclosures often involve contingencies, subsequent events, management fraud, related parties, and accounting changes.

Detection uses vertical, horizontal, and ratio analysis. A ratio change alone is not proof, but it tells you where to look deeper. Remember the master checklist: **recognition, valuation, classification, timing, disclosure**. That is the fastest way to solve most Part 1 exam questions

Core Occupational Fraud Schemes

1. Big Picture Summary

Part 2 moves from accounting foundations into the **most common fraud schemes committed inside organizations**. This is the core occupational-fraud section: fraud committed through one's job, role, access, or authority. In the manual structure, this sits within the early "Financial Transactions and Fraud Schemes" section and includes the major asset-misappropriation and related operational schemes.

For exam purposes, this part is extremely important because many questions are built around:

- what the scheme is,
- how it works,
- what documents are manipulated,
- who benefits,
- what the red flags are,
- and what controls would have prevented or detected it.

This part should be learned as a sequence:

1. **Fraudulent disbursements / billing**
2. **Shell companies and vendor-related schemes**
3. **Pay-and-return and personal purchase schemes**
4. **Payroll fraud and ghost employees**
5. **Conflicts of interest and corruption-related occupational misconduct**

---

2. Must-Know Points

HIGH YIELD

- **Billing schemes** are fraudulent disbursement schemes where an organization pays false, inflated, duplicate, or unauthorized invoices.
- A **shell company scheme** uses a fictitious or controlled entity to bill the victim organization.
- A **nonaccomplice vendor / pay-and-return scheme** involves a real vendor, but the employee manipulates overpayments or refunds for personal gain.
- **Personal purchases** with company funds involve using company money, purchasing channels, or cards to buy nonbusiness items.
- **Payroll fraud** causes the organization to issue unauthorized compensation payments.
- A **ghost employee** may be:
    - fictitious,
    - a terminated employee,
    - or a real person who does not actually work for the company.
- **Conflict of interest** exists when an employee or agent has an undisclosed personal interest that affects duty to the employer.
- The **appearance** of a conflict can also matter, even if direct loss is not yet proven.
- Repeating control themes in this part are:
    - segregation of duties,
    - vendor master controls,
    - invoice/receiving matching,
    - authorization controls,
    - payroll setup and termination controls,
    - reconciliations,
    - complaint/tip mechanisms.

---

3. Key Concepts and Explanations

A. Occupational Fraud in This Part

This part mainly focuses on **asset misappropriation** and closely related corruption/conflict misconduct. Asset misappropriation is generally more common than financial statement fraud, and many of the schemes here depend on access to routine processes such as purchasing, invoicing, payroll, and approvals.

Why it matters:
These schemes often hide inside ordinary business processes, which is why exam questions usually test operational details rather than theory alone.

B. Billing Schemes

A **billing scheme** occurs when the victim organization pays for:

- goods not received,
- services not performed,
- inflated prices,
- duplicate invoices,
- or purchases that were not authorized for legitimate business need.

This is one of the most important occupational fraud schemes because it combines:

- fake documentation,
- weak approvals,
- weak vendor oversight,
- and concealment within accounts payable.

Why it matters:
A billing scheme does not always require a fake vendor. It may use a real vendor, a controlled vendor, or a mixed arrangement. That is why the scheme family is broad.

C. Shell Company Schemes

A **shell company** is a fictitious entity or a company with no real operations, created or controlled for fraudulent billing. The fraudster causes the organization to pay invoices submitted by that entity.

Visible enabling conditions include:

- control over vendor setup,
- invoice routing or approval access,
- weak segregation between preparing and approving vouchers,
- poor documentation,
- weak scrutiny over vendor addresses or ownership.

Variants may include:

- billing for fictitious goods,
- billing for services instead of goods,
- pass-through arrangements,
- self-approval or circular approval.

Why examiners love this topic:
It combines vendor fraud, documentation fraud, purchasing abuse, conflicts of interest, and false approvals in one scheme.

D. Nonaccomplice Vendor and Pay-and-Return Schemes

A **nonaccomplice vendor scheme** uses a legitimate vendor that is unaware of the fraud. The employee manipulates the transaction, not the vendor.

A **pay-and-return scheme** is a classic example:

- the employee causes an intentional overpayment,
- the vendor issues a refund or credit,
- the employee intercepts or diverts the refund.

This is a high-yield distinction because:

- **shell company** = fake/controlled vendor
- **pay-and-return** = real vendor, stolen refund.

E. Personal Purchases with Company Funds

This scheme occurs when an employee uses company money, procurement channels, or company cards to acquire personal items. Forms include:

- false invoicing through AP,
- misuse of credit cards,
- personal items disguised as business purchases,
- returning goods for cash or store credit.

Why it matters:
The scheme can look like normal purchasing unless:

- vendor descriptions are reviewed,
- expense narratives are checked,
- receiving evidence is tested,
- or returns/credits are tracked.

F. Payroll Fraud

Payroll fraud causes the organization to pay compensation that should not be paid. The fraud may exploit:

- employee setup,

- time/attendance,
- pay rate changes,
- distribution of payroll,
- or failure to remove terminated staff.

Why it matters:
Payroll fraud is especially dangerous because payroll is repetitive, high-volume, and often trusted.

G. Ghost Employees

A **ghost employee** is a person on payroll who should not be there. The visible material notes the ghost may be:

- fictitious,
- a former employee,
- or a real person who is not actually working.

To make the scheme work, the fraudster must usually ensure:

1. the ghost is entered into the payroll system,
2. compensation is generated,
3. payment is issued,
4. the payment is collected or redirected.

Common weak points:

- poor onboarding validation,
- weak HR/payroll segregation,
- no independent review of payroll master file changes,
- weak termination controls,
- weak payment distribution controls.

H. Conflicts of Interest

A **conflict of interest** exists when an employee, manager, or agent has an undisclosed personal economic interest in a transaction or decision affecting the employer.

Visible examples include:

- sales-related conflict schemes,
- business diversions,
- resource diversions,

- financial interest in supervised entities,
- conflict in disclosures,
- appearance of conflict.

Why it matters:
Not all occupational fraud is simple theft of cash or goods. Sometimes the fraud lies in **who benefits from a business decision**.

I. Sales-Related and Resource Diversion Conflicts

Visible examples in the manual include:

- underselling,
- writing off sales,
- delaying billings,
- diverting company opportunities,
- using employer resources to support private business.

These are important because the fraud may not look like a fake payment. It may look like a "business decision" that quietly benefits the employee or related party.

J. Why These Schemes Succeed

Across this part, the same enabling conditions keep appearing:

- trust concentrated in one person,
- weak review of master-file changes,
- poor segregation of duties,
- weak receiving controls,
- weak monitoring of refunds/credits,
- poor vendor due diligence,
- insufficient scrutiny of unusual behavior,
- lack of speak-up mechanisms or ignored complaints.

This repetition is useful. It means you can often solve exam questions by asking:

- Who controlled too many steps?
- What approval or reconciliation was missing?
- What independent check failed?

---

4. Important Terms and Definitions

Billing scheme — fraudulent disbursement through fictitious, inflated, or unauthorized invoices.

Fraudulent disbursement — scheme causing the victim organization to make improper payments.

Shell company — fictitious or non-operating entity used to submit fraudulent invoices.

Pass-through scheme — fraudster uses an intermediary arrangement to sell goods/services through a controlled or manipulated path to the employer.

Nonaccomplice vendor — legitimate vendor not knowingly participating in the fraud.

Pay-and-return scheme — intentional overpayment to a real vendor followed by diversion of the refund.

Personal purchases scheme — employee uses company funds or procurement channels for personal items.

Payroll fraud — unauthorized compensation payments.

Ghost employee — fictitious, former, or nonworking person on payroll.

Conflict of interest — undisclosed personal interest compromising duty to employer.

Appearance of conflict — situation that reasonably suggests compromised objectivity, even if direct wrongdoing is not yet fully proven.

Resource diversion — use of employer assets/resources to benefit private interests.

---

5. Comparisons and Distinctions

Billing Scheme vs Shell Company Scheme

- **Billing scheme** is the broad category.
- **Shell company scheme** is one type of billing scheme.

Shell Company vs Nonaccomplice Vendor

- **Shell company**: vendor is fake or controlled by fraudster.
- **Nonaccomplice vendor**: vendor is real and unaware.

Shell Company vs Pay-and-Return

- **Shell company**: payment goes to a fake or controlled entity.
- **Pay-and-return**: payment goes to a real vendor, but refund is stolen.

Payroll Fraud vs Ghost Employee

- **Payroll fraud** is the broad category.
- **Ghost employee** is one of the most classic payroll-fraud methods.

Personal Purchase vs Conflict of Interest

- **Personal purchase**: direct misuse of company funds for personal items.
- **Conflict of interest**: hidden personal economic interest influencing business choices.

Actual Conflict vs Appearance of Conflict

- **Actual conflict**: hidden financial interest or benefit is influencing conduct.
- **Appearance**: facts create a credible perception of compromised objectivity.

---

6. Memory Hooks

Core billing / AP fraud

V-I-P-P

- **V**endor
- **I**nvoice
- **P**ayment
- **P**ersonal benefit

Ghost employee scheme steps

E-G-P-C

- **E**nter on payroll
- **G**enerate pay
- **P**rocess payment
- **C**ollect/divert funds

Conflict of interest red flags

F-A-M-E

- **F**avoritism
- **A**ffiliations undisclosed
- **M**eans exceeded / sudden wealth
- **E**mployee-vendor overlap

Exam shortcut for scheme identification

Ask:

1. Is the vendor fake, real, or controlled?
2. Was the payment false, inflated, duplicated, or refunded?
3. Did the employee benefit directly or through a related party?

---

7. Likely Exam / High-Yield Points

- Vendor and employee sharing address or phone details is a strong shell-company or conflict-of-interest red flag.
- A real vendor does not eliminate fraud risk. Pay-and-return and overbilling can still occur.
- High-level personnel approving their own expenses or purchases create a high-risk control environment.
- Ghost employees often exploit poor termination or payroll master-file controls, not just weak timekeeping.
- Conflict-of-interest schemes may involve otherwise legitimate vendors or transactions; the fraud is in the undisclosed relationship and resulting biased decision.
- Complaints about favored vendors, unexplained pricing differences, or poor-quality goods can be major warning signs.

---

8. Quick Recall Sheet

Main scheme families in Part 2

- billing schemes
- shell company schemes
- nonaccomplice vendor / pay-and-return
- personal purchases
- payroll fraud
- ghost employees
- conflicts of interest.

Highest-yield distinctions

- fake vendor = shell company
- real vendor + stolen refund = pay-and-return
- fake/nonworking employee = ghost employee
- hidden economic interest = conflict of interest

Core control themes

- segregation of duties
- vendor master controls
- invoice/receiving matching
- approval controls

- payroll setup/termination controls
- reconciliations
- speak-up mechanisms.

Best Part 2 recall rule

When you see an AP/payroll/purchasing question, ask:
Who controlled setup, approval, payment, and review?

---

9. Recall Questions

1. What is a billing scheme?
2. What is a shell company?
3. What is the difference between a shell-company scheme and a nonaccomplice-vendor scheme?
4. What is a pay-and-return scheme?
5. What is a ghost employee?
6. What are the four basic steps needed to make a ghost-employee scheme work?
7. What is a conflict of interest?
8. Why can the appearance of a conflict matter even without proven direct loss?
9. Name three red flags of a shell-company or vendor scheme.
10. Name three core controls that reduce AP, vendor, and payroll fraud risk.

---

10. Flashcard-Style Q&A

Q: Fraudulent payment through fictitious, inflated, or unauthorized invoices.
A: Billing scheme.

Q: Fake or controlled vendor used to bill the employer.
A: Shell company.

Q: Legitimate vendor not knowingly participating in the fraud.
A: Nonaccomplice vendor.

Q: Intentional overpayment followed by diversion of refund.
A: Pay-and-return scheme.

Q: Personal items bought with company money or procurement channels.
A: Personal purchases scheme.

Q: Unauthorized compensation payments.
A: Payroll fraud.

Q: Fictitious, former, or nonworking person on payroll.
A: Ghost employee.

Q: Undisclosed personal interest affecting duty to employer.
A: Conflict of interest.

Q: Use of employer assets to support private interests.
A: Resource diversion.

Q: Warning sign involving shared details between vendor and employee.
A: Vendor/employee address or phone overlap.

---

11. Situational / Application Questions

1. A vendor is legitimate, but an employee causes duplicate or excess payment and intercepts the refund. What scheme is this?
2. A purchasing employee creates a vendor with a PO box linked to a relative and approves low-quality invoices with weak support. What scheme family is most likely?
3. A terminated employee continues receiving salary deposits for two months after leaving, and the funds go to an account controlled by another staff member. What fraud type and sub-scheme are indicated?
4. A manager consistently routes business to a supplier in which a close family member has a financial stake, but the relationship was never disclosed. What issue is present?
5. An organization has strong invoice approvals but weak vendor setup controls and no independent review of vendor master-file changes. Which scheme risk does this most increase?

---

12. 1-Minute Review Version

Part 2 is about the most common internal fraud schemes. Learn billing schemes first, especially shell companies, real-vendor refund fraud, and personal purchases. Then learn payroll fraud, especially ghost employees. Finish with conflicts of interest, where the issue is not always fake paperwork but hidden personal benefit affecting business decisions. The fastest way to solve Part 2 questions is to identify who controlled vendor setup, invoice approval, payment processing, payroll entry, and independent review.

---

13. 5-Minute Review Version

Billing schemes are fraudulent disbursements where the organization pays false, inflated, duplicate, or unauthorized invoices. A shell-company scheme uses a fake or controlled vendor. A nonaccomplice-vendor scheme uses a real vendor who is unaware. A pay-and-return scheme is when a real vendor is overpaid and the employee steals the refund. Personal purchases with company funds are another common variation.

Payroll fraud causes unauthorized compensation payments, and ghost employees are one of its classic forms. A ghost may be fictitious, terminated, or real but not working. The fraud works by entering the person into payroll, generating pay, issuing the payment, and diverting or collecting it. Weak onboarding, payroll master-file, termination, or payment controls make this easier.

Conflicts of interest involve undisclosed personal benefit affecting business decisions. The vendor or transaction may appear legitimate, but the hidden relationship or benefit makes it improper. The appearance of conflict can matter too. Across all of Part 2, the key defenses are segregation of duties, vendor master controls, receiving/invoice matching, payroll change controls, reconciliations, and complaint mechanisms.

Specialized Fraud Schemes

1. Big Picture Summary

Part 3 covers the major fraud families that go beyond the core AP/payroll/internal schemes in Part 2. These are still highly testable, but they are broader, more specialized, and often involve external parties, regulated industries, complex products, or technology. Based on the uploaded manuals, the most coherent grouping for Part 3 is:

- corruption and conflicts beyond basic internal schemes,
- theft of data and intellectual property,
- financial institution and mortgage fraud,
- insurance fraud,
- consumer fraud and investment-style scams,
- cyberfraud,
- contract and procurement fraud.

This part is important for certification exams because questions here often test:

- distinctions between look-alike schemes,
- red flags and warning patterns,
- how the scheme is monetized,
- how detection differs by industry,
- and what controls are most responsive.

---

2. Must-Know Points

HIGH YIELD

- **Conflict of interest** is not limited to vendor favoritism; it also includes business diversion, resource diversion, sales-related conflict schemes, and hidden economic interests.
- **Competitive intelligence** is lawful and ethical information gathering; **corporate espionage** is illegal, covert, or unethical acquisition of protected information.
- Key information-security preservation goals are **confidentiality, integrity, and availability**.
- **Mortgage fraud** includes builder bailouts, air loans, identity fraud, foreclosure rescue scams, loan modification fraud, short-sale abuse, flopping, equity skimming, reverse mortgage abuse, and new account fraud.

- **Premium fraud** underpays the insurer; **claimant fraud** overcollects from the insurer.
- **Ponzi** and **pyramid** schemes are not the same:
    - pyramid = recruitment-driven structure
    - Ponzi = fake investment-return structure.
- Common cyberfraud methods include phishing, spear phishing, BEC, vishing, smishing, pharming, catfishing, reverse social engineering, password cracking, and keystroke logging.
- Procurement fraud often centers on **cost mischarging**, which can be:
    - accounting mischarges
    - material mischarges
    - labor mischarges.

---

3. Key Concepts and Explanations

A. Expanded Corruption and Conflict Schemes

In Part 2, conflict of interest was introduced as an internal occupational issue. In this part, it is better understood as a broader corruption concept involving hidden personal benefit in business decisions. Visible material includes:

- sales-related conflicts,
- business diversions,
- resource diversions,
- financial interests in supervised entities,
- conflict-related disclosure issues,
- and appearance-based conflicts.

Why it matters:
The transaction may look real and the vendor may be legitimate. The fraud lies in the **undisclosed relationship, improper influence, or diverted opportunity**.

B. Theft of Data and Intellectual Property

This section focuses on non-cash assets that can be as valuable as money. The visible material highlights the three basic security goals:

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

Visible methods of information theft include:

- open-source research,
- human intelligence,
- surveillance,
- dumpster diving,
- mole or sleeper activity,
- physical infiltration,
- malicious insiders,
- computer attacks,
- poor disposal controls.

Competitive intelligence vs espionage

This is a high-yield distinction:

- **Competitive intelligence** = legal, ethical collection and analysis of relevant information
- **Espionage** = illegal, covert, or unethical acquisition of protected information.

Why it matters:
Exam questions often test whether the conduct is merely aggressive research or has crossed into unlawful or unethical territory.

C. Mortgage Fraud and Financial Institution Fraud

The visible mortgage-fraud material covers the structure of the mortgage industry, its participants, and the features that make it vulnerable: competition, volume pressure, commissions, technology, and multiple intermediaries.

Key participants visible

- borrower / mortgagor
- lender / mortgagee
- seller
- mortgage broker
- real estate agent
- developer
- loan officer
- underwriter
- appraiser
- mortgage investor.

Major mortgage schemes

- **Builder bailout**
- **Air loan**
- **Foreclosure rescue**
- **Phantom help**
- **Lease-back**
- **Loan modification fraud**
- **Short sale abuse**
- **Short-sale flopping**
- **Property flipping**
- **Equity skimming**
- **Mortgage pooling**
- **Reverse mortgage abuse**
- **New account fraud**.

High-yield scheme distinctions

Air loan = loan against nonexistent property or fabricated transaction.
Builder bailout = moving property through concealed incentives and inflated values.
Flopping = abusive undervaluation/short-sale scheme followed by hidden-profit resale.
Equity skimming = rent or property proceeds taken while mortgage obligations fail.

New account fraud

Especially risky because fraud often happens right after the account is opened, before normal behavior patterns exist. Visible examples include false ID, fraudulent checks, mobile deposit abuse, and ATM deposit fraud.

D. Insurance Fraud

The visible insurance-fraud material covers property, life, liability, workers' compensation, premium fraud, claimant fraud, provider issues, and organized-fraud patterns.

Property schemes

- inflated inventory
- phony or inflated thefts
- paper boats.

Life schemes

- fraudulent death claims

- murder for profit
- vanishing premium.

Workers' compensation / liability themes

- staged incidents
- false injury events
- exaggerated injuries
- organized rings using lawyers, runners/cappers, doctors, and claimants.

Premium fraud vs claimant fraud

This is a must-know distinction:

- **Premium fraud** reduces what should be paid to the insurer.
- **Claimant fraud** increases what the insurer pays out.

E. Consumer Fraud, Ponzi Schemes, and Pyramid Schemes

The consumer-fraud material emphasizes product fronts, MLM-like structures, speculative fronts, and the distinction between unlawful pyramids and Ponzi schemes.

Pyramid scheme

Participants' returns depend mainly on recruiting others into the structure.

Ponzi scheme

Promoter claims investment returns, but earlier investors are paid from newer investors' funds, with little or no real profit-generating activity.

Why this matters:
This distinction is one of the most commonly tested in fraud exams.

F. Cyberfraud

The visible material describes cyberfraud as difficult to investigate because it may lack a traditional paper trail, affect technology directly, and require specialist support.

Common cyberfraud methods

- phishing
- spear phishing
- business email compromise
- vishing

- smishing
- pharming
- catfishing
- reverse social engineering
- password cracking
- browsing
- keystroke logging.

BEC variants visible

- supplier-payment redirection
- executive impersonation / wire fraud
- direct-deposit diversion
- real-estate payment redirection
- data theft
- gift-card fraud.

Intrusion indicators

Visible pages note:

- unusual inbound/outbound traffic
- strange access to files
- abnormal system behavior
- suspicious login patterns
- large data transfers
- profile changes
- odd software/hardware behavior.

G. Contract and Procurement Fraud

The visible procurement-fraud material centers on **cost mischarging** and vendor/procurement control failures.

Three visible cost-mischarging types

- **Accounting mischarges**
- **Material mischarges**
- **Labor mischarges**.

Material mischarges

Examples include:

- charging materials not actually incurred,
- wrong rates,
- obsolete items,
- excess residual inventory,
- transfers across jobs,
- weak audit trail.

Labor mischarges

Examples include:

- fake consulting or salary charges,
- billing lower-rate staff as higher-rate,
- fictitious time,
- altered timecards,
- wrong-contract charging.

Prevention themes

- employee education
- segregation of duties
- receiving controls
- approval controls
- reconciliations
- vendor due diligence
- vendor master governance
- monitoring procurement activity.

---

4. Important Terms and Definitions

Competitive intelligence — lawful and ethical gathering/analysis of information.

Corporate espionage — illegal, covert, or unethical acquisition of proprietary information.

Confidentiality / Integrity / Availability — core information-security objectives.

Builder bailout — builder-driven scheme using concealed incentives or inflated values to move distressed inventory.

Air loan — loan based on nonexistent property or fabricated collateral/transaction.

Foreclosure rescue scam — distress-based scheme offering fake or abusive "help" to homeowners in default.

Short-sale flopping — undervalued short-sale scheme followed by quick resale for hidden profit.

Equity skimming — taking rent or proceeds while mortgage obligations fail.

Premium fraud — misrepresentation to reduce insurance premium owed.

Claimant fraud — fabrication or exaggeration of loss or injury to collect insurance proceeds.

Ponzi scheme — fake investment-return scheme paid from new investors' money.

Pyramid scheme — recruitment-driven unlawful scheme.

Phishing — impersonation attack to obtain credentials or data.

Spear phishing — targeted phishing attack.

BEC — business email compromise involving trusted business-context impersonation.

Vishing / Smishing / Pharming — voice, SMS, and redirection-based fraud methods.

Cost mischarging — improper allocation or charging of costs in contracts/procurement.

---

5. Comparisons and Distinctions

Competitive Intelligence vs Espionage

- **Competitive intelligence**: legal and ethical.
- **Espionage**: illegal, covert, or unethical.

Ponzi vs Pyramid

- **Ponzi**: fake returns from later investors' money.
- **Pyramid**: recruitment structure drives payouts.

Premium Fraud vs Claimant Fraud

- **Premium fraud**: underpay insurer.
- **Claimant fraud**: overcollect from insurer.

Phishing vs Spear Phishing vs BEC

- **Phishing**: broad impersonation attempt.
- **Spear phishing**: targeted impersonation.
- **BEC**: business-context impersonation, usually for payments/data.

Flipping vs Flopping

- **Flipping**: rapid resale, sometimes legitimate.
- **Flopping**: manipulative undervaluation/short-sale abuse for hidden profit.

Material vs Labor Mischearge

- **Material**: wrong goods/costs/inventory.
- **Labor**: wrong hours/rates/personnel/job allocation.

---

6. Memory Hooks

Specialized scheme families

C-D-M-I-C-C-P

- **C**orruption/conflict
- **D**ata/IP
- **M**ortgage
- **I**nsurance
- **C**onsumer
- **C**yber
- **P**rocurement

Cyberfraud methods

P-S-B-V-S-P

- **P**hishing
- **S**pear phishing
- **B**EC
- **V**ishing
- **S**mishing
- **P**harming

Insurance distinction

P = Pay less, C = Claim more

- **P**remium fraud = pay less to insurer
- **C**laimant fraud = claim more from insurer

Procurement mischarging

A-M-L

- **A**ccounting
- **M**aterial
- **L**abor

---

7. Likely Exam / High-Yield Points

- A method can involve public information and still be legal competitive intelligence; hidden access, theft, deception, or covert acquisition can move it into espionage.
- Mortgage fraud often involves multiple parties and layered misrepresentations, not just a false appraisal.
- BEC is often about **payment redirection** more than malware.
- Insurance fraud questions often hinge on timing, records consistency, and whether the fraud occurs at premium-setting or claim-payment stage.
- Ponzi vs pyramid remains one of the most likely comparison questions.
- Procurement fraud may involve legitimate contracts but false allocation of costs, labor, or materials.

---

8. Quick Recall Sheet

Main families in Part 3

- corruption/conflict
- theft of data/IP
- mortgage/financial institution fraud
- insurance fraud
- consumer fraud
- cyberfraud
- procurement fraud.

Highest-yield comparisons

- competitive intelligence vs espionage
- Ponzi vs pyramid
- premium fraud vs claimant fraud
- phishing vs spear phishing vs BEC
- flipping vs flopping

- material vs labor mischarge

Best Part 3 recall rule

When the scheme is specialized, ask:

1. What industry or context is this in?
2. Where does the money or benefit come from?
3. What is the key distinction from similar schemes?

---

9. Recall Questions

1. What is the difference between competitive intelligence and corporate espionage?
2. What does CIA stand for in information security?
3. What is an air loan?
4. What is short-sale flopping?
5. What is the difference between premium fraud and claimant fraud?
6. What is the difference between a Ponzi and a pyramid scheme?
7. What does BEC stand for?
8. What are three common intrusion indicators noted in the visible cyberfraud pages?
9. What are the three visible categories of procurement cost mischarging?
10. Why are new accounts especially risky in financial institution fraud?

---

10. Flashcard-Style Q&A

Q: Legal and ethical gathering of business information.
A: Competitive intelligence.

Q: Illegal or unethical acquisition of protected business information.
A: Corporate espionage.

Q: Core information-security triad.
A: Confidentiality, Integrity, Availability.

Q: Loan against nonexistent property or fabricated collateral.
A: Air loan.

Q: Insurance fraud involving misrepresentation to reduce premiums.
A: Premium fraud.

Q: Insurance fraud involving fabricated or exaggerated loss/injury claim.
A: Claimant fraud.

Q: Fraud scheme paying older investors with newer investors' funds.
A: Ponzi scheme.

Q: Recruitment-driven unlawful compensation structure.
A: Pyramid scheme.

Q: Targeted social-engineering email attack.
A: Spear phishing.

Q: Improper contract charging involving wrong hours, rates, or personnel.
A: Labor mischarge.

---

11. Situational / Application Questions

1. A lender approves a mortgage using inflated appraisals, concealed builder incentives, and a straw borrower. What mortgage-fraud themes are implicated?
2. A company researches a rival using trade journals, public filings, and public websites only. Is that more likely competitive intelligence or espionage?
3. A promoter claims investors will earn high returns from a program, but payouts come from new investor money. What type of scheme is this?
4. An insurer is charged too little because the insured understated payroll and misclassified employees. What type of insurance fraud is this?
5. A contractor bills senior-engineer rates for junior staff and charges labor to the wrong project. What procurement-fraud category does this most clearly indicate?

---

12. 1-Minute Review Version

Part 3 covers specialized fraud families. Learn the main comparisons first: competitive intelligence vs espionage, premium fraud vs claimant fraud, Ponzi vs pyramid, phishing vs spear phishing vs BEC, and flipping vs flopping. Then remember the main domains: data/IP theft, mortgage fraud, insurance fraud, consumer fraud, cyberfraud, and procurement fraud. This part is easier once you focus on how the benefit is generated and what makes each scheme distinct from similar ones.

---

13. 5-Minute Review Version

Start with corruption and data/IP theft. Conflict schemes involve undisclosed personal benefit, while data/IP theft turns on confidentiality, integrity, and availability. Competitive intelligence is lawful; espionage is not.

Mortgage fraud includes builder bailouts, air loans, foreclosure rescue scams, loan modification fraud, short-sale abuse, flopping, equity skimming, reverse mortgage abuse, and new account fraud. Financial institution fraud questions often test layered deception and false identity or value claims.

Insurance fraud is best understood through the premium-vs-claimant distinction. Premium fraud underpays the insurer; claimant fraud overcollects from the insurer. Consumer fraud often tests Ponzi vs pyramid. Cyberfraud

focuses on impersonation, social engineering, intrusion signs, and payment/data theft, with BEC especially important. Procurement fraud often focuses on cost mischarging: accounting, material, or labor.

Part 4 Reviewer

Law, Rights, Evidence, and Testifying

1. Big Picture Summary

Part 4 explains the **legal and evidentiary framework** around fraud work. Once you know the schemes, you need to know how the law classifies them, what rights exist during examinations, how evidence is handled, what privileges may protect information, and how fraud examiners testify. This part is built mainly from the manuals covering **securities fraud**, **tax fraud**, **individual rights during examinations**, **basic principles of evidence**, and **testifying**.

This part is highly testable because many exam questions shift from:

- "What scheme is this?"
  to:
- "Is this a security?"
- "Is this tax evasion or tax avoidance?"
- "Can the employer do that in an investigation?"
- "Is this privileged?"
- "What kind of witness is this?"
- "What evidentiary problem exists here?"

---

2. Must-Know Points

HIGH YIELD

- Not every investment-looking arrangement is automatically a security. Classification matters.
- Traditional securities visible in the materials include:
  - stocks
  - bonds
  - certificates of deposit.
- The visible pages also cover:
  - futures contracts
  - options
  - OTC options
  - investment contracts.

- **Investment contracts** are high-yield because many fraud schemes may qualify as securities even if labeled something else.
- **Tax evasion** is illegal; **tax avoidance** is generally lawful. Willfulness is critical in evasion.
- Common tax-fraud indicators include:
    - misrepresentation of facts
    - hidden income/assets
    - double books
    - secret accounts
    - overstated deductions
    - fictitious transactions.
- Employees may have duties to cooperate in investigations, but they may also have privacy, contractual, labor, and whistleblower protections depending on jurisdiction.
- Core evidence themes include:
    - chain of custody
    - impeachment
    - privileges and protections
    - witness roles.
- A fraud examiner may testify as a **fact witness**, an **expert witness**, or in some cases both.

---

3. Key Concepts and Explanations

A. Securities Fraud Framework

The securities-fraud material explains that many products and arrangements can fall under securities law, and fraud analysis often depends first on understanding what kind of instrument or arrangement is involved. Visible categories include stocks, bonds, certificates of deposit, futures, options, and investment contracts.

Why it matters:
An exam question may describe a product that sounds informal or private, but if it functions like an investment contract, securities principles may still apply.

B. Futures and Options

This is a classic distinction.

Futures contract

A futures contract is an agreement to buy or sell an asset at a specified future time and price. The visible material discusses margin, maintenance margin, clearing, cash settlement, physical delivery, and mark-to-market concepts.

Option

An option gives the holder a **right**, not an obligation. The visible pages distinguish:

- **call option** = right to buy
- **put option** = right to sell.

High-yield distinction

- **Futures** = obligation
- **Options** = right for the holder, obligation for the writer/seller.

This is one of the most likely comparison questions in this part.

C. Investment Contracts

The visible pages describe a framework where an arrangement may qualify as an investment contract if it involves:

- an investment of money or something of value,
- a common enterprise,
- an expectation of profit,
- and profits derived from the efforts of others.

Why it matters:
Many frauds disguise themselves as:

- partnerships,
- pooled investments,
- notes,
- life-settlement interests,
- metals/mineral ventures,
- offshore programs,
- hedge-fund structures.

Exam lesson:
Substance matters more than label.

D. Securities-Related Fraud Schemes

Visible examples include:

- Ponzi schemes
- illegal pyramid schemes

- prime bank note schemes
- precious metals/stones schemes
- viatical settlements
- hedge-fund misconduct
- partnership/joint venture abuses
- oil, gas, and mineral interests.

Why it matters:
These schemes often overlap with Part 3, but here the legal question is whether they may fall under securities regulation and fraud standards.

E. Tax Fraud

The tax-fraud material defines fraud broadly in the tax setting and emphasizes the distinction between lawful and unlawful tax reduction.

Tax evasion

Illegal effort to evade or defeat taxes. Willfulness matters.

Tax avoidance

Lawful minimization of taxes through legal methods.

Why it matters:
This is one of the highest-yield legal distinctions in the whole reviewer.

F. Indicators and Types of Tax Evasion

The visible pages identify indicators such as:

- misrepresentation of facts,
- hiding income/assets,
- double books,
- secret bank accounts under false names,
- overstated deductions,
- fictitious transactions.

Visible scheme categories include:

- income and wealth tax evasion,
- falsifying deductions,

- tax-credit schemes,
- consumption tax schemes.

Visible consumption-tax examples include:

- omitted transactions,
- understated transaction value,
- disguising taxable transactions,
- missing trader arrangements,
- smuggling to avoid excise tax.

G. Defenses to Tax Evasion Allegations

The visible material includes several defenses or arguments often raised:

- no tax deficiency,
- lack of willfulness,
- tax avoidance rather than evasion,
- objectively reasonable position,
- claim of right,
- reliance on advice,
- innocent spouse,
- statutes of limitation,
- mental illness in some settings.

Why it matters:
Exams may ask not only what the fraud is, but what legal defense is being asserted.

H. Individual Rights During Examinations

This section is very important for internal investigations. The visible pages show that while employees may have duties to cooperate, employers and investigators do not have unlimited freedom. Relevant themes include:

- duty to preserve evidence,
- contractual rights,
- collective bargaining / labor implications,
- privacy rights,

- whistleblower protections,
- data-protection limits,
- monitoring and notice considerations.

Why it matters:
Internal access to systems or employees does not automatically erase privacy, labor, or legal limits.

I. Duty to Preserve and Spoliation Risk

The visible material emphasizes preservation obligations where litigation or proceedings are anticipated. Destroying or failing to preserve relevant records can create sanctions or evidentiary problems.

Exam lesson:
Once preservation duty is triggered, routine deletion or careless destruction becomes dangerous.

J. Basic Principles of Evidence

The evidence material highlights practical legal concerns in fraud work:

- authenticity,
- credibility,
- admissibility arguments,
- custody,
- privilege,
- witness challenges.

A high-yield theme is that evidence is not just “useful information.” It must be handled and presented properly.

K. Chain of Custody

The visible pages define chain of custody as documenting who had possession or access to an item and what was done with it from collection to production.

Good practices shown include:

- describe what the item is,
- record receipt/removal,
- note location and dates,
- maintain a continuous record of handling.

Why it matters:
Weak custody undermines authenticity and credibility.

L. Impeachment

Impeachment is attacking a witness's credibility. Visible methods include:

- showing bias,
- showing inability to observe or remember,
- showing prior inconsistent statements,
- using some criminal convictions,
- challenging truthfulness reputation.

Why it matters:
Exam questions may describe a witness problem and ask what evidentiary concept it implicates.

M. Privileges and Protections

The visible pages discuss several privileges and protections:

- attorney-client / legal professional privilege
- legal advice privilege
- litigation privilege / work-product
- self-evaluation privilege
- marital privilege
- informant identity privilege
- accountant-client privilege in some jurisdictions
- cross-border privilege complications.

High-yield distinction

- **Attorney-client privilege** protects confidential communications for legal advice.
- **Work-product / litigation privilege** protects materials prepared in anticipation of litigation.

These are related but not identical.

N. Testifying

The visible pages distinguish between:

- **testimonial evidence** generally,
- **fact witnesses**,

- **expert witnesses**,
- and differences between adversarial/common-law and inquisitorial systems.

Fact witness

Testifies from firsthand observation or personal involvement.

Expert witness

Provides specialized opinion or explanation based on expertise.

Why it matters:
A fraud examiner may appear in one role or both, but must stay within the appropriate boundaries of that role.

---

4. Important Terms and Definitions

Stock — equity security representing ownership interest.

Bond — debt security representing borrowing relationship.

Certificate of deposit — banking investment instrument discussed as a traditional security in the visible pages.

Futures contract — agreement to buy or sell an asset at a future time and price.

Option — right, but not obligation, to buy or sell an asset.

Call option — right to buy.

Put option — right to sell.

Investment contract — arrangement involving investment, common enterprise, profit expectation, and reliance on efforts of others.

Tax evasion — illegal effort to avoid taxes.

Tax avoidance — lawful effort to minimize taxes.

Willfulness — intentional unlawful effort; key concept in tax evasion.

Chain of custody — documented history of evidence possession and handling.

Impeachment — challenge to witness credibility.

Attorney-client / legal professional privilege — protection for confidential legal-advice communications.

Work-product / litigation privilege — protection for materials prepared in anticipation of litigation.

Fact witness — witness testifying from firsthand knowledge.

Expert witness — witness providing specialized opinion.

---

5. Comparisons and Distinctions

Futures vs Options

- **Futures**: obligation to buy or sell.
- **Options**: right for the holder, not obligation.

Call vs Put

- **Call**: right to buy.
- **Put**: right to sell.

Tax Evasion vs Tax Avoidance

- **Evasion**: unlawful.
- **Avoidance**: lawful.

Fact Witness vs Expert Witness

- **Fact witness**: what I saw / did / know firsthand.
- **Expert witness**: what my specialized knowledge allows me to explain or opine on.

Attorney-Client Privilege vs Work-Product

- **Attorney-client**: confidential legal communications.
- **Work-product**: materials prepared in anticipation of litigation.

Information vs Evidence

- Information may guide an investigation.
- Evidence must be properly preserved, handled, and presented. Supported by the evidence-handling themes in the visible pages.

---

6. Memory Hooks

Securities categories

S-B-C / F-O-I

- **S**tocks
- **B**onds
- **C**Ds
- **F**utures
- **O**ptions
- **I**nvestment contracts

Tax distinction

E-A-W

- **E**vasion = illegal
- **A**voidance = legal
- **W**illfulness matters

Evidence core

C-I-P-T

- **C**ustody
- **I**mpeachment
- **P**rivilege
- **T**estimony

Witness roles

F = Firsthand, E = Expertise

- **F**act witness = firsthand
- **E**xpert witness = expertise

---

7. Likely Exam / High-Yield Points

- A scheme may still be a security even if it is not called a stock or bond, if it functions like an investment contract.
- The biggest tax-fraud distinction is usually not “how aggressive was the tax position?” but “was there willful unlawful conduct?”
- Privilege issues are high-yield because people confuse legal-advice communications with all materials connected to lawyers. They are not always the same.
- Weak chain of custody does not necessarily mean the evidence never existed, but it creates credibility and admissibility problems.
- A fraud examiner who testifies outside personal knowledge without expert basis creates role problems.

---

8. Quick Recall Sheet

Main blocks in Part 4

- securities fraud framework
- tax fraud
- rights during examinations
- evidence

- privilege
- testifying.

Highest-yield distinctions

- futures vs options
- tax evasion vs tax avoidance
- fact witness vs expert witness
- attorney-client vs work-product

Best Part 4 recall rule

When the question feels legal, ask:

1. What is this thing legally?
2. What rights or protections apply?
3. What evidentiary issue is present?
4. What role is the witness playing?

---

9. Recall Questions

1. What is the main difference between a futures contract and an option?
2. What is a call option? What is a put option?
3. What factors make an arrangement an investment contract?
4. What is the difference between tax evasion and tax avoidance?
5. Why is willfulness important in tax fraud?
6. Name four visible indicators of tax fraud.
7. What is chain of custody?
8. What is impeachment?
9. What is the difference between attorney-client privilege and work-product protection?
10. What is the difference between a fact witness and an expert witness?

---

10. Flashcard-Style Q&A

Q: Agreement to buy or sell an asset at a future time and price.
A: Futures contract.

Q: Right, but not obligation, to buy or sell an asset.
A: Option.

Q: Option giving the right to buy.
A: Call option.

Q: Option giving the right to sell.
A: Put option.

Q: Illegal effort to evade taxes.
A: Tax evasion.

Q: Lawful minimization of taxes.
A: Tax avoidance.

Q: Continuous documented record of evidence handling.
A: Chain of custody.

Q: Attack on witness credibility.
A: Impeachment.

Q: Protection for confidential legal-advice communications.
A: Attorney-client / legal professional privilege.

Q: Witness testifying from firsthand observation.
A: Fact witness.

---

11. Situational / Application Questions

1. A promoter calls an arrangement a “private club membership,” but investors contribute money, expect profits, and depend on the promoter’s work. What legal classification issue is raised first?
2. A taxpayer keeps two sets of books and hides funds in an undeclared account. What tax-fraud themes are implicated?
3. During an internal investigation, management wants to search employee data broadly without regard to notice, policy, or privacy restrictions. What rights-related issue is raised?
4. A key document passed through multiple hands, but no one documented when or where. What evidentiary problem is most obvious?
5. A fraud examiner begins offering opinions in court about matters outside firsthand observation and outside established expertise. What testimony-role issue is triggered?

---

12. 1-Minute Review Version

Part 4 is the law-and-evidence section. Learn the key distinctions first: futures vs options, tax evasion vs tax avoidance, fact witness vs expert witness, and attorney-client privilege vs work-product. Then remember that internal investigations still operate within legal limits, especially around privacy, contracts, whistleblower protections, and preservation duties. Chain of custody and credibility are central.

---

13. 5-Minute Review Version

Start with securities. Traditional securities include stocks, bonds, and CDs, but many fraud schemes may also be securities if they function as investment contracts. Futures create obligations; options give rights to the holder. Calls buy, puts sell.

Then tax fraud: tax evasion is illegal and depends heavily on willfulness; tax avoidance is legal. Watch for hidden income, double books, false-name accounts, fictitious transactions, and overstated deductions.

Then rights and evidence: employees may have duties to cooperate, but privacy, contracts, labor issues, and whistleblower protections still matter. Preserve evidence once duty attaches. Chain of custody tracks possession and handling. Impeachment attacks credibility. Privilege protects some communications or litigation-prep materials. A fraud examiner may testify as fact witness, expert witness, or both, but must stay within the correct role.

Investigation Execution and Reporting

1. Big Picture Summary

Part 5 is the **how-to-do-the-work** section. After learning the fraud schemes and the legal/evidentiary rules, this part shows how a fraud examination is actually carried out from start to finish: planning the case, collecting evidence, using information sources, handling digital evidence, tracing illicit transactions, seeking asset recovery, and writing the report. It also includes sample fraud examination reports that show what good work product looks like in practice.

This part is very high-yield because exam questions often ask:

- what should happen first,
- what should be documented,
- what should be preserved,
- what should or should not be disclosed,
- how digital evidence should be handled,
- how cross-border recovery works,
- and what makes a report defensible.

---

2. Must-Know Points

HIGH YIELD

- A fraud examination should begin with a **clear plan** covering goals, scope, time frame, roles, operational issues, confidentiality, and escalation/notification needs.
- The visible investigation chapter identifies three core evidence types:
    - testimonial
    - documentary
    - digital.
- Information sources include:

    - internet searches
    - public records
    - public-record vendors
    - investigative service companies
    - archived websites
    - social media
    - background checks
    - due diligence sources.
- Important search practices include:
    - exact phrases
    - advanced operators
    - multiple search engines
    - variant spellings/synonyms
    - source validation.
- In digital forensics, the central principle is preserving the **integrity of evidence**.
- **Volatile data** may be lost if a running device is powered down.
- Good digital-forensic practice includes:
    - chain of custody
    - restricting access
    - proper packaging
    - write-blocking
    - forensic imaging
    - analyzing copies rather than originals.
- Asset recovery generally follows:

1. evaluate recovery potential
2. commence legal process
3. secure assets
4. obtain judgment
5. enforce judgment.

- Good reports are:

    - accurate
    - clear
    - impartial and relevant
    - timely.
- Fraud examiners should not improperly state legal guilt or innocence in their reports.

---

3. Key Concepts and Explanations

A. Planning and Conducting a Fraud Examination

The visible investigation-planning pages show that a fraud examination should not begin as random fact gathering. It should begin with a structured plan. Before planning is complete, the visible pages say the team should:

- review what is known,
- define goals,
- identify who should be informed,
- determine scope,
- set time frame,
- consider law-enforcement notification or assistance,
- assign member roles,
- address operational issues,
- outline the course of action,
- adapt resources,
- and prepare the organization.

Why it matters:
The biggest early investigation failure is usually not "missing a fact." It is **starting without enough structure**.

B. Goals of a Fraud Examination

Visible examples of investigation goals include:

- preventing further loss or exposure,
- determining whether misconduct is ongoing,
- securing evidence,
- minimizing and recovering losses,
- assessing root cause and prevention,

- supporting legal or disciplinary action,
- protecting legal privileges.

This is important because exam questions may ask what the first objective should be, and the answer depends on context:

- stop ongoing loss,
- protect evidence,
- define exposure,
- or preserve rights.

C. Scope, Time Frame, Roles, and Confidentiality

Scope

The visible pages explain that scope may be limited by:

- subject matter,
- department,
- location,
- resources,
- law/procedure,
- policy,
- culture,
- timing.

Time frame

Should account for:

- deadlines,
- expected deliverables,
- reporting dates,
- governance expectations,
- complexity of the allegation.

Roles

Responsibilities and reporting lines must be defined. Otherwise, the case can become inconsistent or chaotic.

Confidentiality

The visible pages recommend:

- limiting information to need-to-know persons,
- avoiding casual discussion,
- securing documents,
- considering off-hours work where appropriate,
- avoiding suspect alert,
- using privileged channels when appropriate.

Why it matters:
Confidentiality failures can destroy evidence, alert suspects, or weaken legal strategy.

D. Collecting Evidence

The visible opening pages of the evidence-collection chapter identify three major evidence types:

- testimonial,
- documentary,
- digital.

Why it matters:
This simple classification is a useful memory anchor for the whole investigation process:

- what people say,
- what records show,
- what systems/devices contain.

E. Sources of Information

The visible sources-of-information material shows that fraud examiners increasingly rely on external and online sources. These include:

- search engines,
- public records,
- aggregated databases,
- archived internet content,
- social media,
- background-check sources,
- due diligence tools.

Search practices

Visible guidance includes:

- use exact phrase searching in quotation marks,
- try multiple search engines,
- use exclusions/minus operators,
- search by file type,
- try variants and synonyms,
- search beyond the first page,
- use browser find tools to scan results.

Why it matters:
The best search is not the broadest search. It is the most **iterative, precise, and validated** one.

F. Public Records, Databases, and Source Validation

The visible pages explain that public information can come from:

- original government sources,
- public-record vendors,
- investigative service companies.

But they also warn that vendor databases may be:

- incomplete,
- outdated,
- abstract-only,
- inconsistent across jurisdictions,
- affected by privacy restrictions.

Why it matters:
A database hit is often a **lead**, not final proof.

G. Archived Web Content and Social Media

The visible pages discuss archived sites and social-media content as useful sources for:

- finding removed or changed statements,
- locating people or witnesses,

- researching accused persons or accusers,
- identifying images, locations, business links, travel, or affiliations.

Social-media evidence collection

Visible best practices include:

- screenshots,
- screen recordings,
- print/PDF capture,
- preserving context,
- documenting URLs and timing,
- preserving embedded content where possible.

Why it matters:
Social-media content changes quickly. Delayed capture can mean lost evidence.

H. Digital Forensics

The visible digital-forensics material is highly practical. The core principle is to preserve the **integrity** of the digital evidence.

Key issues include:

- whether the device is on or off,
- what volatile data might be lost,
- who should touch the system,
- how access is restricted,
- how the evidence is packaged,
- whether a forensic image is taken,
- and whether analysis is done on the copy instead of the original.

I. Volatile Data and Running Systems

Visible examples of volatile data include:

- memory/RAM,
- encryption keys or passwords in memory,
- active sessions,

- running processes,
- network connections,
- current device or OS state,
- some logs.

Why it matters:
If a device is running, shutting it down may destroy important data. But interacting with it may also alter evidence. That is why specialist support is often important.

J. Securing and Imaging Digital Evidence

Visible best practices include:

- disconnecting or isolating devices,
- prohibiting unauthorized access,
- maintaining chain of custody,
- using write-blockers,
- documenting device condition and actions taken,
- making a forensic image.

Forensic image

A bit-for-bit copy used for analysis so the original is preserved.

Why it matters:
The default principle is **analyze the image, preserve the original**.

K. Cloud and Mobile Forensics

Visible cloud-forensics challenges include:

- limited direct access,
- unclear storage location,
- jurisdiction issues,
- chain-of-custody challenges,
- multitenancy/resource sharing,
- discovery complications.

Visible mobile-forensics themes include logical extraction of:

- messages,

- images,
- audio,
- video,
- contacts,
- calendar entries,
- tasks,
- multimedia.

Why it matters:
Cloud and mobile evidence are common in modern cases but are often harder to preserve and interpret than a traditional local hard drive.

L. Tracing Illicit Transactions and Asset Recovery

The visible asset-recovery material explains that recovery is not just a financial exercise; it is a **legal and strategic process**. It includes:

- identifying likely jurisdictions,
- contacting foreign counterparts,
- researching local law,
- locating proceeds and ownership evidence,
- choosing civil/criminal or hybrid strategy.

Visible cross-border tools include:

- mutual legal assistance requests,
- letters rogatory,
- tax-information exchange agreements.

M. Civil vs Criminal Recovery

The visible pages distinguish:

- **civil action** = compensation/remedy-focused
- **criminal action** = punishment/public-law process, though restitution may result in some cases.

Why it matters:
Criminal prosecution does not automatically mean the victim gets all money back.

N. Report Writing

The visible report-writing pages are among the most practical in the manuals. They identify two report families:

- fraud examination reports
- expert reports.

Visible quality characteristics are:

- accuracy
- clarity
- impartiality and relevance
- timeliness.

Why it matters:
A strong investigation can still fail if the report is biased, vague, unsupported, or poorly organized.

O. Conclusions and Opinions

This is one of the highest-yield report-writing topics. The visible pages explain that:

- conclusions must be supported by the examination,
- opinions must stay within proper scope and expertise,
- reports should avoid improper statements of legal guilt or innocence,
- facts and inconsistencies should be described clearly without overreaching.

Why it matters:
This is often tested as a wording or professionalism question.

P. Organizing the Report

The visible material notes that information may be organized:

- chronologically,
- or by transaction / scheme.

Why it matters:
The right structure depends on what makes the case most understandable to the intended audience.

Q. Sample Fraud Examination Reports

The sample reports show practical formats such as:

- interview memoranda,

- phone-call memoranda,
- meeting summaries,
- invoice exhibits,
- canceled-check reviews,
- surveillance logs,
- courthouse-record reviews,
- anonymous-tip documentation.

What they teach:
Good case documentation is:

- factual,
- date/time anchored,
- exhibit-backed,
- and clear about what was observed, reviewed, or reported.

---

4. Important Terms and Definitions

Case plan / investigation plan — structured plan for conducting the fraud examination. Supported by the planning chapter.

Testimonial evidence — evidence from what people say.

Documentary evidence — evidence from records and documents.

Digital evidence — electronically stored or device-based evidence.

Volatile data — data likely lost when power is removed or state changes.

Write-blocker — tool preventing writes to media during acquisition.

Forensic image — bit-for-bit copy of digital media used for analysis.

Deep web — web content not indexed by ordinary search engines.

Dark web — specially accessed anonymity-oriented part of the deep web.

Public-record vendor — aggregated source of public-record data, often faster but not always complete.

MLA request — mutual legal assistance request used in cross-border legal cooperation.

Letters rogatory — formal cross-border judicial request tool.

Fraud examination report — report documenting results of the fraud exam.

Expert report — report containing specialized expert opinion where appropriate.

---

5. Comparisons and Distinctions

Investigation Plan vs Final Report

- **Plan**: what you will do and why.
- **Report**: what you found and how it is supported.

Lead vs Proof

- **Lead**: initial information pointing somewhere.
- **Proof**: verified, supported information. Public-record database hits are often leads, not final proof.

Original Source vs Aggregated Database

- **Original source**: often more authoritative.
- **Aggregated vendor source**: faster but may be incomplete or stale.

Live Collection vs Traditional Shutdown

- **Live collection**: preserves volatile data but risks altering the system.
- **Shutdown-first**: may protect some integrity but lose volatile evidence.

Civil Recovery vs Criminal Recovery

- **Civil**: compensation/remedy oriented.
- **Criminal**: punishment oriented, though restitution may arise.

Conclusion vs Opinion

- **Conclusion**: supported inference from evidence.
- **Opinion**: interpretive judgment, acceptable only in proper context and expertise.

---

6. Memory Hooks

Investigation flow

P-E-S-D-R

- **P**lan
- **E**vidence
- **S**ources
- **D**igital handling
- **R**eport / recovery

Evidence types

T-D-D

- **T**estimonial
- **D**ocumentary
- **D**igital

Digital forensics

P-I-C-C

- **P**reserve
- **I**mage
- **C**hain of custody
- **C**heck/analyze the copy

Asset recovery

E-S-J-E

- **E**valuate
- **S**ecure
- **J**udgment
- **E**nforce

---

7. Likely Exam / High-Yield Points

- The first major mistake in an investigation is often poor planning, not poor interviewing.
- Public-record and internet sources are useful, but failure to validate them is a major weakness.
- Digital evidence questions often hinge on whether the machine was running and whether volatile data could be lost.
- Fraud reports should not sound accusatory without factual support and should avoid statements of legal guilt.
- Social-media evidence is highly useful but can disappear quickly and can raise authenticity issues if not preserved properly.

---

8. Quick Recall Sheet

Part 5 flow

- plan the case
- collect evidence
- use information sources

- preserve digital evidence
- trace assets
- write the report.

Core evidence classes

- testimonial
- documentary
- digital.

Digital evidence rule

Preserve integrity first. Analyze the image, not the original.

Report-writing rule

Accurate, clear, impartial, timely.

Best Part 5 recall rule

When asked what to do next, think:
Plan → Preserve → Verify → Document → Report

---

9. Recall Questions

1. What should be included in an investigation plan?
2. What are the three major evidence types identified in the visible investigation chapter?
3. Why is a public-record database hit not always enough by itself?
4. What is volatile data?
5. Why is a forensic image used?
6. What is a write-blocker?
7. What are the five visible basic steps in asset recovery?
8. What are the four quality characteristics of a good report listed in the visible report-writing pages?
9. Why should a fraud examiner avoid stating legal guilt in the report?
10. What do the sample fraud examination reports teach about documentation style?

---

10. Flashcard-Style Q&A

Q: Structured plan for how the fraud examination will be conducted.
A: Investigation plan / case plan.

Q: Evidence from what people say.
A: Testimonial evidence.

Q: Evidence from documents and records.
A: Documentary evidence.

Q: Data likely lost when a powered-on device is shut down.
A: Volatile data.

Q: Tool preventing writes to media during acquisition.
A: Write-blocker.

Q: Bit-for-bit copy used for digital forensic analysis.
A: Forensic image.

Q: Cross-border legal assistance mechanism.
A: MLA request.

Q: Report quality feature meaning unbiased and relevant.
A: Impartiality and relevance.

Q: Organizing report facts by event sequence.
A: Chronological organization.

Q: Organizing report facts by scheme or transaction set.
A: Transaction-based organization.

---

11. Situational / Application Questions

1. A fraud team starts interviewing widely before defining scope, roles, or confidentiality limits. What investigation-control problem appears first?
2. An examiner finds a useful record in an online vendor database. What should be done before relying heavily on it?
3. A suspect laptop is powered on and likely encrypted. What major digital-forensics issue becomes critical immediately?
4. A victim wants to recover fraud proceeds located abroad. What cross-border legal tools or strategies may need to be considered?
5. A manager asks the examiner to state in the report that the suspect “is guilty.” How should the examiner respond based on the visible guidance?

---

12. 1-Minute Review Version

Part 5 is the practical investigation section. Start with a case plan: goals, scope, roles, time frame, confidentiality, and escalation. Remember the three evidence classes: testimonial, documentary, and digital. Use public records and social media carefully, but validate important leads. In digital forensics, preserve integrity, protect volatile data when needed, use write-blocking and imaging, and analyze the copy. Asset recovery is legal and strategic, not just financial. Reports must be accurate, clear, impartial, and timely, and should not state legal guilt.

13. 5-Minute Review Version

A fraud examination starts with structure, not improvisation. Define goals, scope, roles, timing, confidentiality, and escalation paths. Keep the suspect from being alerted unnecessarily. Evidence can be testimonial, documentary, or digital. Use external sources like public records, archived web content, social media, and due diligence tools, but validate key findings back to reliable sources.

Digital forensics is one of the highest-yield areas here. If a system is running, volatile data may disappear if powered down, but interacting with the system may also alter evidence. Restrict access, document everything, use chain of custody, apply write-blocking where appropriate, create a forensic image, and analyze the image instead of the original. Cloud and mobile evidence add complexity.

Tracing and recovery involve cross-border tools, legal strategy, and sequencing: evaluate, secure, obtain judgment, and enforce. Good reports are accurate, clear, impartial, and timely. Use supported conclusions, not unsupported accusations or guilt statements. The sample reports show the expected practical style: factual, exhibit-based, date/time anchored, and clearly documented.

Fraud Prevention, White-Collar Crime, Governance, and Fraud Risk Assessment

1. Big Picture Summary

Part 6 explains **why fraud happens, why organizations fail to stop it early, and how they can systematically prevent and deter it**. This is the conceptual and preventive core of the full reviewer. It combines:

- white-collar crime concepts,
- occupational fraud theory,
- ACFE occupational fraud patterns and statistics,
- behavioral red flags,
- anti-fraud controls,
- corporate governance,
- and fraud risk assessment.

This part is crucial for certification exams because many questions ask:

- why otherwise normal people commit fraud,
- which conditions make fraud more likely,
- which controls reduce loss and duration,
- what governance bodies should do,
- and how fraud risk should be assessed and prioritized.

This part answers the big prevention question:

How do frauds start, why do they continue, and what should organizations do before a case exists?

2. Must-Know Points

HIGH YIELD

- **White-collar crime** arises in occupational and organizational settings where pressure, culture, opportunity, obedience, and rationalization may support misconduct.
- **Cressey's Fraud Triangle** consists of:
    - non-shareable financial pressure
    - perceived opportunity
    - rationalization.
- Cressey's model explains that the trust violation typically occurs when **all three elements** are present.
- **Albrecht's Fraud Scale** uses:
    - situational pressure
    - opportunity
    - personal integrity.
- The visible ACFE data shows:
    - **asset misappropriation** is the most common occupational fraud category,
    - **financial statement fraud** is the least common but costliest,
    - **corruption** is between them.
- The visible pages show that **tips** are the most common initial detection method.
- Common anti-fraud controls associated with lower losses and/or shorter duration include:
    - code of conduct
    - external audit of financial statements
    - internal audit department
    - management certification
    - anti-fraud policy
    - training
    - hotline
    - proactive data monitoring/analysis
    - surprise audits
    - job rotation / mandatory vacation
    - employee support programs.

- A fraud risk assessment should identify:
    - inherent risks
    - likelihood
    - significance
    - processes involved
    - existing preventive and detective controls
    - residual risk
    - response actions.
- Fraud risk assessment is not just about transactions; it also includes:
    - environment and culture
    - leadership behavior and communication
    - quality of complaint and response protocols.

---

3. Key Concepts and Explanations

A. White-Collar Crime

The visible material presents white-collar crime as misconduct arising in occupational or organizational settings, often influenced by social, economic, and cultural conditions rather than just direct greed. Pressure, status concerns, obedience to authority, performance demands, and organizational normalization of misconduct all matter.

Why it matters:
Certification exams often test not only the scheme, but the **conditions that made it possible**. This section gives you that lens.

B. Compliance vs Deterrence

A useful conceptual distinction in the visible pages is:

- **Compliance approach** = encourage people and organizations to follow rules voluntarily
- **Deterrence approach** = increase certainty and cost of punishment so misconduct becomes unattractive.

Why it matters:
A strong anti-fraud program usually needs both:

- values, training, culture, reporting channels, and leadership support,
- plus meaningful accountability and consequences.

C. Occupational Fraud

The visible material connects white-collar crime to occupational fraud by focusing on misconduct committed through one's occupation, position, trust, or access. This bridges the theory in Part 6 with the scheme details you learned in Parts 2 and 3.

Why it matters:
It reminds you that fraud is usually not random. It happens where someone has:

- trust,
- access,
- knowledge,
- and perceived ability to conceal the act.

D. Cressey's Fraud Triangle

This is one of the most important concepts in the entire reviewer.

The visible pages explain that occupational fraud tends to arise when three elements come together:

1. Non-shareable financial pressure

A problem the person feels cannot be openly discussed or solved legitimately. Visible examples and themes include debt, status pressure, personal reversals, hidden obligations, or fear of embarrassment.

2. Perceived opportunity

The person believes they can exploit a weakness in controls, trust, oversight, or access.

3. Rationalization

The person finds a way to preserve self-image while committing fraud, such as:

- "I'm only borrowing it,"
- "I deserve it,"
- "I'll pay it back,"
- "This is temporary,"
- or "they owe me."

High-yield conclusion

The visible material states that the trust violation occurs when these factors align.

Why it matters:
If the exam asks what best reduces fraud risk, often the answer is something that reduces **opportunity**, weakens **rationalization**, or addresses **pressure**.

E. Albrecht's Fraud Scale

Albrecht's model reframes the problem using:

- situational pressure,
- opportunity,
- personal integrity.

This is similar to the Fraud Triangle, but instead of emphasizing rationalization, it emphasizes the person's integrity as the balancing factor.

High-yield distinction

- **Fraud Triangle** = pressure, opportunity, rationalization
- **Fraud Scale** = pressure, opportunity, integrity.

Why it matters:
This is a classic comparison question.

F. ACFE Occupational Fraud Patterns

The visible ACFE material presents several very testable themes.

Most common vs costliest

- **Asset misappropriation** = most common
- **Financial statement fraud** = least common but highest median loss
- **Corruption** = middle ground.

This is one of the most likely direct exam questions.

Estimated loss

The visible material notes the well-known ACFE estimate that organizations lose about **5% of revenue** to fraud annually, while also recognizing that global fraud loss is only an estimate.

G. Duration and Loss Relationship

The visible pages show that:

- median duration for all cases was **12 months**,
- longer-running frauds cause larger losses,
- early detection significantly reduces damage.

Why it matters:
This strongly supports investment in:

- tips,

- monitoring,
- internal audit,
- data analytics,
- and surprise reviews.

H. Detection Methods

The visible pages show that **tips** are the most common initial detection method. Employees are the largest source of tips, with customers, anonymous sources, vendors, and others also contributing. Internal audit and management review are also major detection methods.

Why it matters:
This is one of the strongest practical lessons in the prevention section:
speak-up channels matter.

I. Anti-Fraud Controls

The visible pages list multiple controls associated with lower losses or shorter fraud duration, including:

- code of conduct
- anti-fraud policy
- employee support programs
- training
- hotline
- management review
- internal audit department
- external financial statement audit
- management certification
- proactive data monitoring/analysis
- surprise audits
- job rotation / mandatory vacation
- reward structures for tips in some contexts.

Why it matters:
Exam questions often ask which control is most likely to reduce loss or improve detection. The visible material supports multiple controls, but especially active detection and governance mechanisms.

J. Behavioral Red Flags

The visible behavioral-red-flag chart includes common warning signs such as:

- living beyond means
- financial difficulties
- unusually close relationship with vendor/customer
- unwillingness to share duties
- control issues / refusal to delegate
- irritability or suspiciousness
- wheeler-dealer attitude
- family problems
- addiction problems.

Important nuance:
The visible material also indicates that many perpetrators had **no prior criminal record** and many had **no prior employment discipline**.

Why it matters:
A “clean background” does not eliminate fraud risk.

K. Corporate Governance

The later visible pages in the same manual move into governance and oversight. They identify major governance actors such as:

- the board of directors
- the audit committee
- compensation committee
- nominating committee
- management
- shareholders.

The visible governance principles include:

- accountability
- transparency
- fairness
- responsibility.

Why it matters:
Fraud prevention is not just an operations issue. It is a **governance issue**.

L. Why the Audit Committee Matters

Although many governance bodies matter, the audit committee is especially important because it supports oversight of:

- financial reporting,
- internal control,
- audit,
- whistleblowing/reporting mechanisms,
- and fraud governance. This emphasis aligns with the visible governance section and the later audit-responsibility materials.

M. Fraud Risk Assessment

This is where the theory becomes operational.

The visible fraud-risk-assessment material explains that organizations conduct these assessments to:

- identify vulnerable processes and schemes,
- identify who or what creates the greatest risk,
- evaluate anti-fraud controls,
- prioritize mitigation,
- and support compliance with regulations and standards.

Core framework steps visible

1. Identify potential inherent fraud risks and schemes
2. Assess likelihood
3. Assess significance
4. Evaluate existing preventive and detective controls
5. Evaluate control effectiveness
6. Determine residual risk
7. Develop or assign response actions.

Why it matters:
This is one of the most likely practical framework questions in the prevention section.

N. What Makes a Good Fraud Risk Assessment

The visible material emphasizes that a strong fraud risk assessment depends on:

- a senior and credible sponsor,
- independence/objectivity,
- deep knowledge of the business,
- broad participation,
- trust and candor from participants,
- active use rather than one-time form filling,
- thinking like a fraudster.

Why it matters:
A weakly facilitated risk assessment may look complete on paper but miss the real risks.

O. Fraud Risk Categories

The visible pages identify broad categories such as:

- fraudulent financial reporting
- asset misappropriation
- corruption
- external fraud
- regulatory/legal misconduct
- reputational risk
- technology risk.

Why it matters:
This helps organize risk inventories and prevents assessments from focusing only on cash theft.

P. Likelihood, Significance, Controls, and Residual Risk

The visible material explains that risks should be rated by:

Likelihood

Based on factors like prior incidents, industry prevalence, control weaknesses, transaction volume, culture, complaints, and support for prevention.

Significance

Based on financial, legal, operational, reputational, morale, and investigation impact.

Controls

Both preventive and detective controls should be mapped and assessed for operating effectiveness.

Residual risk

The risk that remains after existing controls are considered.

Q. Leadership Behavior and Complaint Response

This is one of the most valuable sections in the visible material because it shows that fraud prevention is not only technical.

Visible leadership questions include:

- Do leaders' actions match their words?
- Are leaders open to bad news?
- Are leaders transparent?
- Do they avoid unrealistic pressure?
- Do they model rule-following behavior?

Visible complaint/response questions include:

- Is there a hotline?
- Do people trust it?
- Are complaints investigated?
- Are escalation rules clear?
- Are people held accountable consistently?
- Are root causes addressed?

Why it matters:
Even good controls can fail in a poor culture.

---

4. Important Terms and Definitions

White-collar crime — crime arising in occupational or organizational settings, often involving trust, position, or professional activity. Supported by the visible theory/governance pages.

Occupational fraud — fraud committed through one's occupation, position, or access.

Fraud Triangle — pressure, opportunity, rationalization model.

Non-shareable financial pressure — pressure the person feels cannot be openly discussed or legitimately solved.

Perceived opportunity — belief that the fraud can be committed and concealed.

Rationalization — internal justification allowing the fraudster to preserve self-image.

Fraud Scale — pressure, opportunity, integrity model.

Corporate governance — oversight framework involving board, committees, management, and shareholders.

Fraud risk assessment — structured evaluation of fraud risks, controls, and residual exposure.

Inherent fraud risk — fraud risk before considering controls.

Residual risk — remaining risk after controls are considered.

Preventive control — control designed to stop fraud before it occurs.

Detective control — control designed to identify fraud after or as it occurs.

Fraud risk portfolio — consolidated view of assessed fraud risks and responses. Supported by the visible framework material.

---

5. Comparisons and Distinctions

Fraud Triangle vs Fraud Scale

- **Fraud Triangle**: pressure, opportunity, rationalization
- **Fraud Scale**: pressure, opportunity, integrity.

Compliance vs Deterrence

- **Compliance**: encourage rule-following
- **Deterrence**: increase cost/certainty of punishment.

Most Common vs Costliest Fraud

- **Asset misappropriation**: most common
- **Financial statement fraud**: least common but costliest
- **Corruption**: in between.

Inherent Risk vs Residual Risk

- **Inherent risk**: before controls
- **Residual risk**: after controls.

Preventive vs Detective Controls

- **Preventive**: stop fraud before it happens
- **Detective**: find fraud after or during occurrence.

Strong Policy vs Strong Culture

- **Policy**: written formal expectation

- **C**ulture: actual behavior, reporting trust, accountability, leadership example. Supported by the visible leadership/culture themes.

---

6. Memory Hooks

Fraud Triangle

P-O-R

- **P**ressure
- **O**pportunity
- **R**ationalization

Fraud Scale

P-O-I

- **P**ressure
- **O**pportunity
- **I**ntegrity

Fraud risk assessment

L-S-C-R

- **L**ikelihood
- **S**ignificance
- **C**ontrols
- **R**esidual risk

Anti-fraud control effectiveness

T-H-A-D

- **T**ips
- **H**otline
- **A**udit
- **D**ata monitoring

Governance principles

A-T-F-R

- **A**ccountability
- **T**ransparency

- **F**airness
- **R**esponsibility

---

7. Likely Exam / High-Yield Points

- Fraud risk is not just about controls; it is also about **culture and leadership behavior**.
- Tips are the most common detection method, so hotline trust and complaint handling matter greatly.
- Longer-running frauds cause more damage, which means early detection is one of the strongest controls.
- A person can commit fraud without prior conviction or discipline, so screening alone is not enough.
- A fraud risk assessment that lacks independence, candid participation, or business knowledge is likely weak even if the template is complete.
- Unrealistic performance pressure can strengthen the pressure side of the Fraud Triangle and weaken culture.

---

8. Quick Recall Sheet

Part 6 core flow

- understand why fraud happens
- know the pattern data
- watch for red flags
- strengthen governance
- assess fraud risk
- map controls and responses.

Highest-yield concepts

- Fraud Triangle
- Fraud Scale
- most common vs costliest fraud
- tips as top detection source
- inherent vs residual risk
- preventive vs detective controls

Best Part 6 recall rule

When a prevention question appears, ask:

1. What pressure/opportunity/rationalization or integrity issue exists?
2. What governance or culture issue exists?
3. What control or risk-assessment response best addresses it?

---

9. Recall Questions

1. What are the three elements of the Fraud Triangle?
2. What are the three elements of the Fraud Scale?
3. Which occupational fraud category is most common?
4. Which occupational fraud category is least common but costliest?
5. What is the most common initial detection method in the visible ACFE data?
6. Name four common behavioral red flags shown in the visible chart.
7. What is the difference between inherent fraud risk and residual fraud risk?
8. What is the difference between preventive and detective controls?
9. Why does leadership behavior matter in fraud risk assessment?
10. What broad fraud-risk categories are listed in the visible fraud-risk-assessment material?

---

10. Flashcard-Style Q&A

Q: Pressure, opportunity, and rationalization model.
A: Fraud Triangle.

Q: Pressure, opportunity, and integrity model.
A: Fraud Scale.

Q: Most common occupational fraud category.
A: Asset misappropriation.

Q: Least common but highest-loss occupational fraud category.
A: Financial statement fraud.

Q: Most common initial detection method.
A: Tip.

Q: Fraud risk before considering controls.
A: Inherent fraud risk.

Q: Fraud risk after considering controls.
A: Residual risk.

Q: Control designed to stop fraud before it occurs.
A: Preventive control.

Q: Control designed to find fraud after or during occurrence.
A: Detective control.

Q: Governance principles highlighted in the visible governance material.
A: Accountability, transparency, fairness, responsibility.

---

11. Situational / Application Questions

1. A company has a detailed anti-fraud policy, but leaders punish bad news and reward only results. What major fraud-risk-assessment weakness does this suggest?
2. An employee has no criminal record and no prior disciplinary history, but shows financial stress, unwillingness to share duties, and a very close vendor relationship. What prevention lesson does this illustrate?
3. An organization wants to lower fraud loss quickly. Based on the visible materials, which is more promising: ignoring speak-up systems or strengthening tip channels and active detection?
4. A fraud risk assessment rates a risk high before controls but low after strong controls are mapped and tested. What changed conceptually?
5. A business unit says fraud risk assessment should only cover theft of money, not reputational, technology, or regulatory misconduct. What does the visible framework suggest?

---

12. 1-Minute Review Version

Part 6 is the prevention and theory section. Learn the Fraud Triangle and Fraud Scale first. Then memorize the ACFE patterns: asset misappropriation is most common, financial statement fraud is least common but costliest, and tips are the top detection source. Know the common behavioral red flags and anti-fraud controls. Finish with fraud risk assessment: identify inherent risk, rate likelihood and significance, map preventive/detective controls, then assess residual risk. Remember that culture and leadership matter as much as formal controls.

---

13. 5-Minute Review Version

Start with white-collar crime and occupational fraud theory. Pressure, opportunity, and rationalization explain why fraud becomes possible; Albrecht's model replaces rationalization with personal integrity. These are foundational because they explain why controls matter and why culture matters.

Next, learn the ACFE occupational-fraud patterns. Asset misappropriation is most common, corruption is in the middle, and financial statement fraud is least common but most expensive. Frauds that last longer create larger losses. Tips are the leading detection method, so hotlines and speak-up culture are critical. Many perpetrators had no prior conviction or discipline, so red flags and control design matter more than assumptions about background.

Then move into governance and fraud risk assessment. Fraud prevention depends on good governance, accountability, transparency, and leadership behavior. Fraud risk assessments should identify risks, rate likelihood and significance, assess control design and effectiveness, and determine residual risk. They should also evaluate culture, leadership, complaint handling, and response quality, not just transaction-level controls.

Ethics, Professional Standards, and Auditors' / Internal Auditors' Fraud Responsibilities

1. Big Picture Summary

Part 7 is the **professional-responsibility** section of the reviewer. After learning the schemes, the law, the investigation process, and prevention frameworks, this final part explains **how fraud examiners, external auditors, and internal auditors are expected to behave and perform their roles**. It brings together:

- the **ACFE Code of Professional Ethics**,
- the **CFE Code of Professional Standards**,
- **external auditors' fraud-related responsibilities**,
- and **internal auditors' fraud-related responsibilities**.

This part is highly testable because many exam questions ask:

- what a professional should disclose,
- what they should avoid saying,
- what level of assurance auditors provide,
- what professional skepticism means,
- how management override should be addressed,
- and what role internal audit has in fraud governance.

This part answers the question:

Once fraud risk or fraud work exists, what are professionals expected to do properly, ethically, and within their role?

---

2. Must-Know Points

HIGH YIELD

- The ACFE ethics material requires **complete reporting of material matters** if omission would distort the facts.
- Materiality depends on whether a user of the report or results would consider the matter important.
- CFEs must maintain:
    - integrity
    - objectivity
    - competence
    - due professional care
    - confidentiality.
- CFEs should not knowingly make false statements, including while testifying.

- Reports must be based on sufficient, reliable, and relevant evidence.
- A CFE **must not express an opinion on the legal guilt or innocence** of any person or party.
- External auditors are responsible for obtaining **reasonable assurance**, not absolute assurance, that financial statements are free from material misstatement due to fraud.
- External-audit fraud themes include:
    - professional skepticism
    - engagement-team fraud discussion
    - inquiries of management and governance
    - fraud-risk factors
    - management override
    - communication
    - documentation.
- Management override is a major fraud risk, and visible responses include:
    - testing journal entries and adjustments
    - reviewing estimates for bias
    - evaluating significant unusual transactions.
- Internal audit is **not the sole owner** of fraud prevention, but it plays a key role in assurance over fraud governance, fraud risk management, and controls.

---

3. Key Concepts and Explanations

A. ACFE Code of Professional Ethics

The visible ethics material emphasizes that fraud examiners must act in a way that protects truthfulness, fairness, reliability, and trust in the profession. A major visible duty is to **report all material matters discovered during the examination if omission would distort the facts**.

Why it matters:
This means a fraud examiner cannot selectively present only facts that support a preferred narrative while ignoring important contradictory or clarifying information.

B. Complete Reporting of Material Matters

This is one of the highest-yield topics in the ethics material.

The visible pages explain that:

- a matter is **material** if it is important enough to influence the user's understanding or decision,

- omission can distort facts just as much as exaggeration can,
- and a report may become misleading by what it leaves out, not only by what it says.

Why it matters:
Exam questions may ask what a fraud examiner must disclose or whether withholding a fact is acceptable. The correct answer often turns on materiality and distortion.

C. Integrity and Objectivity

Visible standards require CFEs to act with integrity and objectivity. This includes:

- avoiding false statements,
- avoiding misleading conduct,
- disclosing actual, potential, or perceived conflicts before accepting work,
- and avoiding conduct discreditable to the profession.

Why it matters:
A technically correct investigation can still become professionally improper if the examiner is biased, conflicted, or misleading.

D. Professional Competence and Continuing Improvement

The visible standards require CFEs to accept only assignments for which they are competent or can become competent with appropriate support, and to continue developing professionally.

Why it matters:
This is a common ethics principle across professions:
Do not take work beyond your competence without proper support, supervision, or preparation.

E. Due Professional Care

Visible standards explain that due professional care includes:

- diligence,
- critical analysis,
- skepticism,
- adequate planning,
- proper supervision,
- and sufficient evidentiary support for conclusions.

Why it matters:
This concept links ethics to actual investigation performance. It is not just about attitude; it is also about process quality.

F. Confidentiality

The visible standards require confidentiality over confidential or privileged information unless disclosure is authorized, required by law, or compelled by proper legal process.

Why it matters:
Fraud work often involves highly sensitive facts, allegations, documents, and legal issues. Mishandling confidentiality can create ethical, legal, and strategic problems.

G. Communication with Client or Employer

The visible standards emphasize that there should be a clear understanding with the client or employer about:

- scope,
- objectives,
- responsibilities,
- and changes in limitations or expectations.

Why it matters:
This helps avoid scope confusion, role confusion, and unfair assumptions about what the professional was engaged to do.

H. Standards of Examination and Reporting

The visible pages require evidence that is:

- sufficient,
- reliable,
- relevant,
- and organized in a way that supports conclusions and proper chain of custody and reporting.

Why it matters:
This reinforces the link between Part 5 and Part 7:
good process and good evidence handling are part of professional standards, not just good technique.

I. No Opinion on Legal Guilt or Innocence

This is one of the most important exam points in this part.

The visible standards state that the CFE must **not express an opinion on whether someone is legally guilty or innocent**.

Why it matters:
The fraud examiner's role is to present supported facts, analyses, and professional conclusions within scope—not to replace the judge, jury, or court.

J. External Auditors' Fraud-Related Responsibilities

The visible audit-responsibility material explains that external auditors are responsible for obtaining **reasonable assurance** that the financial statements are free of material misstatement due to fraud.

This is not the same as guaranteeing detection of all fraud.

Why it matters:
This distinction between **reasonable assurance** and **absolute assurance** is one of the most likely direct exam questions in the audit section.

K. Professional Skepticism

The visible material repeatedly emphasizes that auditors must maintain **professional skepticism** throughout the audit. This means remaining alert to the possibility that fraud-related misstatement may exist, even if management has appeared honest in the past.

Why it matters:
This is a central mindset requirement in the fraud-related auditing material.

L. Engagement-Team Fraud Discussion

The visible pages note that the engagement team should discuss:

- how and where the financial statements may be susceptible to fraud,
- possible incentives/pressures,
- management override possibilities,
- possible misappropriation,
- and how audit procedures should respond.

Why it matters:
This shows that fraud consideration should be active and collaborative, not passive or assumed.

M. Fraud-Risk Factors

The visible auditor material refers to the classic fraud-risk-factor elements:

- incentive or pressure

- opportunity
- rationalization.

This aligns with the Fraud Triangle from Part 6 and shows how theory becomes audit application.

N. Required Inquiries and Considerations

The visible pages indicate that auditors may inquire of:

- management,
- those charged with governance,
- internal audit where present.

Auditors also consider:

- unusual or unexpected relationships,
- information suggesting fraud risk,
- internal-control weaknesses relevant to fraud,
- and the implications of identified misstatements.

Why it matters:
This is a practical fraud-response framework inside audit work.

O. Management Override of Controls

This is one of the most important audit topics.

The visible material stresses that management override is a significant fraud risk because management may be able to bypass otherwise effective controls. Visible audit responses include:

- testing journal entries and adjustments,
- reviewing accounting estimates for bias,
- evaluating significant unusual transactions outside normal business.

Why it matters:
If you see an exam question asking what auditors should do in response to override risk, this is the core answer area.

P. Communication and Documentation by External Auditors

The visible pages note that auditors may need to communicate fraud-related matters to:

- management,
- those charged with governance,

- regulatory or enforcement authorities in some situations.

Documentation includes:

- understanding of the entity and environment,
- fraud-risk assessment,
- responses to assessed risks,
- results of procedures,
- communications made.

Why it matters:
Fraud-related auditing is not just about doing procedures. It is also about how those procedures and outcomes are documented and escalated.

Q. Internal Auditors' Fraud-Related Responsibilities

The visible material then shifts to internal audit and references the **IIA Global Internal Audit Standards**, the **Three Lines Model**, and the **Practice Guide on Internal Audit and Fraud**.

Visible internal-audit responsibilities/themes include:

- demonstrating competency,
- exercising due professional care,
- planning strategically,
- developing the internal audit plan,
- communicating effectively,
- communicating risk acceptance,
- planning engagements effectively,
- identifying significant risks including fraud,
- evaluating fraud risk governance and controls,
- supporting continuous improvement.

Why it matters:
Internal audit is not expected to single-handedly prevent all fraud, but it is expected to provide meaningful assurance over the organization's fraud framework.

R. Internal Audit's Role vs Management's Role

A critical implied point from the visible materials is:

- **Management** owns operations, controls, and fraud-risk response.

- **Internal audit** provides assurance and insight over whether governance, risk management, and control processes are adequate and effective.

Why it matters:
This distinction is frequently tested in internal-audit and governance questions.

S. Communicating Acceptance of Risk

The visible internal-audit standards-related content includes communication of accepted risks. This means that where management accepts a level of risk that may be inappropriate, internal audit may need to escalate or communicate that acceptance through proper channels.

Why it matters:
This is highly relevant for fraud-risk governance and for practical internal-audit judgment.

---

4. Important Terms and Definitions

Material matters — matters important enough that omission could distort user understanding or decision-making.

Complete reporting of material matters — obligation to disclose material matters if omission would distort facts.

Integrity — acting honestly and avoiding misleading conduct.

Objectivity — maintaining impartial judgment free from inappropriate bias or conflict.

Professional competence — possessing or obtaining the necessary knowledge and skill for the assignment.

Due professional care — diligence, skepticism, planning, supervision, and sufficient evidence support.

Confidentiality — protection of confidential or privileged information absent proper authority or legal requirement.

Reasonable assurance — high but not absolute level of assurance in an audit.

Professional skepticism — alert, questioning mindset recognizing the possibility of fraud-related misstatement.

Management override — management's ability to bypass normal controls to perpetrate or conceal fraud.

Those charged with governance — persons or bodies responsible for oversight of the entity, such as the board or audit committee. Supported by the visible audit content.

Three Lines Model — governance model distinguishing management, risk/compliance oversight, and independent assurance roles. Referenced in the visible internal-audit pages.

---

5. Comparisons and Distinctions

Complete Reporting vs Selective Reporting

- **Complete reporting**: include all material matters necessary to avoid distortion.
- **Selective reporting**: omit important matters and mislead users.

Integrity vs Objectivity

- **Integrity**: honesty and moral soundness.
- **Objectivity**: unbiased professional judgment.

Competence vs Due Professional Care

- **Competence**: having the right knowledge/skill.
- **Due professional care**: applying that knowledge properly and diligently.

Reasonable Assurance vs Guarantee

- **Reasonable assurance**: high, but not absolute.
- **Guarantee**: impossible standard in fraud auditing because concealment, override, and collusion may exist.

External Auditor vs Internal Auditor

- **External auditor**: focuses on material misstatement in financial statements and provides an audit opinion.
- **Internal auditor**: provides broader assurance/advisory value over governance, risk management, and controls, including fraud-risk governance.

Supported Conclusion vs Legal Guilt Opinion

- **Supported conclusion**: evidence-based professional inference within scope.
- **Legal guilt opinion**: determination reserved to legal process, not the CFE.

---

6. Memory Hooks

CFE ethics core

I-O-C-C-D

- **I**ntegrity
- **O**bjectivity
- **C**ompetence
- **C**onfidentiality
- **D**ue care

Reporting rule

M-O-D

- **M**aterial matters
- don't **O**mit
- avoid **D**istortion

Auditor override response

J-E-U

- **J**ournal entries
- **E**stimates
- **U**nusual transactions

External vs internal audit

F vs G

- External audit = **F**inancial statement assurance
- Internal audit = broader **G**overnance/risk/control assurance

---

7. Likely Exam / High-Yield Points

- A CFE may describe evidence and supported conclusions, but may not state that a person is legally guilty or innocent.
- Omission can be as misleading as an outright false statement when the omitted fact is material.
- Professional skepticism is required even where management has previously appeared trustworthy.
- Management override is always a major concern because even strong controls can be bypassed at the top.
- Internal audit does not own fraud prevention, but it does have a real responsibility to evaluate and communicate on fraud governance and control adequacy.
- Accepting work beyond competence without appropriate support is an ethics issue, not just a technical issue.

---

8. Quick Recall Sheet

Part 7 core areas

- CFE ethics
- professional standards
- external-audit fraud responsibilities
- internal-audit fraud responsibilities.

Highest-yield concepts

- complete reporting of material matters
- no guilt/innocence opinion
- reasonable assurance
- professional skepticism

- management override
- internal audit's assurance role

Best Part 7 recall rule

When a responsibility question appears, ask:

1. What is my role?
2. What is my evidence basis?
3. What must I disclose?
4. What must I avoid saying?
5. What must I communicate or escalate?

---

9. Recall Questions

1. What does complete reporting of material matters require?
2. What makes a matter material?
3. What are the core ethics/professional qualities emphasized in the visible CFE standards pages?
4. Can a CFE express an opinion on legal guilt or innocence?
5. What is reasonable assurance?
6. What is professional skepticism?
7. Why is management override such a major fraud risk?
8. What three visible response areas are especially important for override risk?
9. What is the difference between external auditors' and internal auditors' fraud-related roles?
10. When might internal audit need to communicate accepted risk upward?

---

10. Flashcard-Style Q&A

Q: Obligation to disclose material matters if omission would distort facts.
A: Complete reporting of material matters.

Q: Acting honestly and not misleading users.
A: Integrity.

Q: Maintaining unbiased professional judgment.
A: Objectivity.

Q: Protecting confidential or privileged information unless properly authorized or required.
A: Confidentiality.

Q: High but not absolute level of audit assurance.
A: Reasonable assurance.

Q: Alert, questioning mindset recognizing fraud risk may exist.
A: Professional skepticism.

Q: Ability of management to bypass otherwise effective controls.
A: Management override.

Q: Three major external-audit response areas to management override.
A: Journal entries, estimates, unusual transactions.

Q: Governance model referenced in the visible internal-audit material.
A: Three Lines Model.

Q: CFE statement that must be avoided in reports.
A: Opinion on legal guilt or innocence.

---

11. Situational / Application Questions

1. A fraud examiner finds evidence strongly suggesting misconduct and wants to write, "The suspect is guilty of fraud." What professional-standard issue does this raise?
2. An auditor sees unusual late journal entries and inconsistent explanations from management. What major fraud-response area is triggered?
3. A CFE accepts a complex digital-forensics assignment with no relevant skill, no supervision, and no specialist support. What ethics/professional issue arises?
4. Internal audit concludes management has accepted a fraud-related risk far above tolerance. What communication responsibility may arise?
5. A report omits a contradictory but important fact because it weakens the preferred narrative. What ethics/reporting issue is implicated?

---

12. 1-Minute Review Version

Part 7 is about professional responsibility. CFEs must report material matters completely, maintain integrity, objectivity, competence, due care, and confidentiality, and avoid opinions on legal guilt or innocence. External auditors provide reasonable assurance, not guarantees, and must apply professional skepticism, especially regarding management override. Internal audit provides assurance over fraud governance, risk management, and controls, but does not own fraud prevention alone.

---

13. 5-Minute Review Version

Start with CFE ethics: disclose material matters completely, avoid distortion, act with integrity and objectivity, maintain competence, apply due professional care, and protect confidentiality. Reports must be evidence-based and must not state legal guilt or innocence.

Then external-audit responsibilities: auditors provide reasonable assurance that financial statements are free from material misstatement due to fraud. They must maintain professional skepticism, discuss fraud risk within the team, inquire of management and governance, assess fraud-risk factors, and respond to management override by testing journal entries, reviewing estimates for bias, and evaluating unusual transactions.

Finally, internal audit: internal audit is not the owner of fraud prevention, but it plays an important assurance role over fraud governance, fraud risk management, and controls. It must demonstrate competence, due care, strategic planning, clear communication, and appropriate escalation where management accepts inappropriate risk.

Final Master Cram Reviewer

Fraud Examiners Manual — Certification Exam Review Set

This master set reorganizes the 20 uploaded manuals into the most retention-friendly sequence:

1. Foundations: accounting and financial statement fraud
2. Core occupational fraud schemes
3. Specialized fraud schemes
4. Law, rights, evidence, and testifying
5. Investigation execution and reporting
6. Fraud prevention, white-collar crime, governance, and fraud risk assessment
7. Ethics, professional standards, and auditors' / internal auditors' fraud responsibilities.

Ultra-Condensed Exam Cheat Sheet

The 25 things to remember first

1. **Assets = Liabilities + Owners' Equity.**
2. Main financial statements: balance sheet, income statement, changes in equity, cash flow statement.
3. Accrual accounting records when earned/incurred, not when cash moves.
4. Financial statement fraud usually means fictitious revenues, timing differences, improper asset valuation, concealed liabilities/expenses, or improper disclosures.
5. Concealed liabilities/expenses usually **overstate profit**.
6. Billing schemes = false, inflated, duplicate, or unauthorized invoices.
7. Shell company = fake/controlled vendor. Real vendor + stolen refund = pay-and-return.
8. Ghost employee = fictitious, former, or nonworking person on payroll.
9. Conflict of interest = undisclosed personal interest affecting duty to employer.
10. Competitive intelligence is legal/ethical; espionage is illegal/covert/unethical.
11. CIA = confidentiality, integrity, availability.

12. Mortgage fraud: know air loans, builder bailouts, foreclosure rescue, flopping, equity skimming, reverse mortgage abuse, new account fraud.
13. Premium fraud underpays insurer; claimant fraud overcollects.
14. Ponzi = fake investment returns; pyramid = recruitment-driven structure.
15. Cyberfraud: phishing, spear phishing, BEC, vishing, smishing, pharming, catfishing.
16. Procurement fraud: accounting, material, and labor mischarges.
17. Futures = obligation; options = right for holder. Call = buy, put = sell.
18. Tax evasion = illegal; tax avoidance = lawful. Willfulness matters.
19. Evidence basics: chain of custody, impeachment, privilege, fact vs expert witness.
20. Investigation flow: plan, preserve, verify, document, report.
21. Digital forensics rule: preserve integrity, capture volatile data when justified, image before analysis.
22. Asset recovery flow: evaluate, secure, obtain judgment, enforce.
23. Fraud Triangle = pressure, opportunity, rationalization. Fraud Scale = pressure, opportunity, integrity.
24. Most common occupational fraud = asset misappropriation. Costliest = financial statement fraud. Most common detection = tip.
25. CFE cannot opine on legal guilt or innocence. External auditors give reasonable assurance, not a guarantee. Management override is always high risk.

Master Cram Reviewer

Part 1: Foundations

Think in five distortion lenses: **recognition, valuation, classification, timing, disclosure**. Most Part 1 questions can be solved by asking which of those five was manipulated. Main red flags and tools here are vertical analysis, horizontal analysis, ratio analysis, odd payable/liability patterns, and profit/cash-flow mismatch. Improper capitalization shifts expense to assets; concealed liabilities understate obligations; improper disclosures often involve contingencies, subsequent events, related parties, management fraud, and accounting changes.

Part 2: Core Occupational Fraud

Most common internal schemes hide in purchasing, payables, payroll, and approvals. Learn the sequence:

- billing schemes,
- shell company schemes,
- nonaccomplice vendor schemes,
- pay-and-return,
- personal purchases,
- payroll fraud,

- ghost employees,
- conflicts of interest.
  Across all of them, ask who controlled setup, approval, payment, and review. Weak vendor master controls, self-approval, poor receiving evidence, weak payroll change controls, and poor termination controls are recurring enablers.

Part 3: Specialized Fraud Schemes

This part is all about distinctions:

- competitive intelligence vs espionage,
- premium fraud vs claimant fraud,
- Ponzi vs pyramid,
- phishing vs spear phishing vs BEC,
- flipping vs flopping,
- material vs labor mischarges.
  Mortgage fraud is usually layered deception. Insurance fraud often turns on timing, documents, claim narrative, and provider patterns. Cyberfraud often turns on impersonation, urgency, or intrusion indicators. Procurement fraud often looks like legitimate contracting until cost allocation is examined.

Part 4: Law, Rights, Evidence, Testifying

Key legal distinctions:

- futures vs options,
- tax evasion vs tax avoidance,
- fact witness vs expert witness,
- attorney-client privilege vs work-product.
  A scheme can be a security even if not labeled as one if it functions like an investment contract. Internal investigations still have limits: privacy, contracts, labor issues, preservation duties, and whistleblower protections matter. Evidence is only as good as its handling, custody, authenticity, and admissibility posture.

Part 5: Investigation Execution and Reporting

Best mental model:
Plan → Collect → Validate → Preserve → Trace → Report.
A fraud exam should start with scope, goals, roles, timing, confidentiality, and escalation. Social media and databases are useful but need validation and preservation. Digital evidence requires volatility awareness, restricted access, write-blocking where appropriate, imaging, and analysis on copies. Good reports are accurate, clear, impartial, relevant, and timely, and should not state legal guilt.

Part 6: Prevention, Theory, Governance, FRA

This is the prevention core:

- Fraud Triangle,

- Fraud Scale,
- ACFE occupational fraud patterns,
- behavioral red flags,
- anti-fraud controls,
- governance,
- fraud risk assessment.
  Remember: asset misappropriation is most common, financial statement fraud is costliest, tips are the top detection source, longer-running frauds cause larger losses, and culture plus leadership matter as much as written controls. Fraud risk assessment is not just scheme listing; it is rating likelihood/significance, evaluating controls, and identifying residual risk, while also assessing culture, leadership behavior, and complaint-response processes.

Part 7: Ethics, Standards, Auditor Roles

CFE standards require:

- complete reporting of material matters,
- integrity,
- objectivity,
- competence,
- due professional care,
- confidentiality,
- evidence-based reporting,
- no guilt/innocence opinion.
  External auditors provide reasonable assurance and must apply professional skepticism, especially around management override. Internal audit is not the sole owner of fraud prevention, but it has a core assurance role over fraud governance, risk management, and controls.

---

100 Flashcards

Foundations 1–15

1. **Q:** Basic accounting equation?
   A: Assets = Liabilities + Owners' Equity.
2. **Q:** Main statement showing financial position at a point in time?
   A: Balance sheet / statement of financial position.
3. **Q:** Main statement showing revenues and expenses over a period?
   A: Income statement / statement of profit or loss.

4. **Q:** Main difference between cash basis and accrual basis?
   A: Cash basis tracks cash movement; accrual basis tracks earned/incurred economic activity.

5. **Q:** Two broad recognition conditions?
   A: Probable future economic benefit and reliable measurement.

6. **Q:** Recording a current expense as an asset is called what?
   A: Improper capitalization.

7. **Q:** Concealing liabilities usually affects profit how?
   A: It overstates profit by understating obligations/expenses.

8. **Q:** Five major financial statement fraud categories?
   A: Fictitious revenues, timing differences, improper asset valuation, concealed liabilities/expenses, improper disclosures.

9. **Q:** Three basic financial statement analysis tools?
   A: Vertical, horizontal, and ratio analysis.

10. **Q:** Failure to disclose a material related-party transaction is what kind of issue?
    A: Improper disclosure.

11. **Q:** Possible obligation depending on uncertain future events?
    A: Contingent liability.

12. **Q:** Event after reporting date that may need disclosure or adjustment?
    A: Subsequent event.

13. **Q:** Best 5-part distortion checklist?
    A: Recognition, valuation, classification, timing, disclosure.

14. **Q:** Strong profits with weak operating cash flow may suggest what?
    A: Possible manipulated results, including omitted liabilities or other financial statement fraud.

15. **Q:** Why are omitted liabilities harder to detect sometimes?
    A: Omissions may leave less obvious trail than fabricated recorded transactions.

Core Occupational Fraud 16–35

16. **Q:** Broad scheme where company pays false or improper invoices?
    A: Billing scheme.

17. **Q:** Fake or controlled vendor used to bill employer?
    A: Shell company.

18. **Q:** Legitimate vendor unaware of the fraud?
    A: Nonaccomplice vendor.

19. **Q:** Intentional overpayment followed by theft of refund?
    A: Pay-and-return scheme.

20. **Q:** Personal items bought using company money or processes?
    A: Personal purchases scheme.

21. **Q:** Broad category for unauthorized compensation payments?
    A: Payroll fraud.

22. **Q:** Fictitious, former, or nonworking person on payroll?
    A: Ghost employee.

23. **Q:** Four-step ghost employee logic?
    A: Enter, generate pay, process payment, collect/divert funds.

24. **Q:** Hidden personal economic interest affecting employer duty?
    A: Conflict of interest.

25. **Q:** Use of employer assets for private benefit?
    A: Resource diversion.

26. **Q:** Can appearance of conflict matter?
    A: Yes, appearance itself can be problematic.

27. **Q:** Shared employee/vendor address suggests what?
    A: Shell company or conflict-of-interest red flag.

28. **Q:** High-risk AP control weakness?
    A: Same person controls vendor setup and invoice approval.

29. **Q:** Duplicate invoice numbers or weak invoice quality suggest what?
    A: Billing or vendor fraud red flags.

30. **Q:** Why do terminated employees matter in payroll fraud?
    A: Poor termination controls can allow continued payments.

31. **Q:** Hidden family/vendor relationship affecting procurement decision?
    A: Conflict of interest.

32. **Q:** Broad control theme across billing and payroll fraud?
    A: Segregation of duties.

33. **Q:** What should be reviewed independently in payroll-fraud prevention?
    A: Payroll master file changes, onboarding, termination, and payment distribution.

34. **Q:** Complaints about favored vendors may indicate what?
    A: Conflict of interest or shell/billing scheme issues.

35. **Q:** Shell company vs pay-and-return in one line?
    A: Shell = fake vendor; pay-and-return = real vendor, stolen refund.

Specialized Schemes 36–60

36. **Q:** Lawful and ethical gathering of business information?
    A: Competitive intelligence.

37. **Q:** Illegal/covert/unethical acquisition of proprietary information?
    A: Corporate espionage.

38. **Q:** CIA stands for what?
    A: Confidentiality, Integrity, Availability.

39. **Q:** Loan against nonexistent property or fabricated transaction?
    A: Air loan.

40. **Q:** Builder-driven scheme using concealed incentives/inflated values to move inventory?
    A: Builder bailout.

41. **Q:** Short-sale abuse followed by quick hidden-profit resale?
    A: Flopping / short-sale flopping.

42. **Q:** Taking rent/proceeds while mortgage obligations fail?
    A: Equity skimming.

43. **Q:** Why are new accounts high-risk?
    A: Fraud may occur before normal activity patterns exist.

44. **Q:** Insurance fraud involving reduced premium through misrepresentation?
    A: Premium fraud.

45. **Q:** Insurance fraud involving fabricated or exaggerated loss/injury?
    A: Claimant fraud.

46. **Q:** Insurance red flag: no forced entry but burglary alleged. What does that suggest?
    A: Suspicious claim narrative / possible fraud.

47. **Q:** Fraud paying earlier investors with later investors' money?
    A: Ponzi scheme.

48. **Q:** Recruitment-driven unlawful scheme?
    A: Pyramid scheme.

49. **Q:** Broad impersonation-based credential theft attack?
    A: Phishing.

50. **Q:** Targeted phishing attack?
    A: Spear phishing.

51. **Q:** Trusted business-context impersonation for payments/data?
    A: Business email compromise (BEC).

52. **Q:** Voice-based phishing?
    A: Vishing.

53. **Q:** SMS-based phishing?
    A: Smishing.

54. **Q:** Redirecting users to fake websites?
    A: Pharming.

55. **Q:** Fake online persona used to exploit emotionally or financially?
    A: Catfishing.

56. **Q:** Three procurement cost-mischarging types?
    A: Accounting, material, labor.

57. **Q:** Charging wrong goods/costs/inventory across jobs?
    A: Material mischarge.

58. **Q:** Charging wrong hours/rates/personnel to job/contract?
    A: Labor mischarge.

59. **Q:** Key cyber intrusion indicators?
    A: Unusual traffic, odd logins, abnormal file access, large transfers, changed profiles.

60. **Q:** Premium fraud vs claimant fraud in one line?
    A: Premium fraud underpays insurer; claimant fraud overcollects.

Law, Rights, Evidence 61–75

61. **Q:** Traditional securities named in the visible material?
    A: Stocks, bonds, certificates of deposit.

62. **Q:** Agreement to buy/sell at future time and price?
    A: Futures contract.

63. **Q:** Right, not obligation, to buy or sell?
    A: Option.

64. **Q:** Call option gives right to what?
    A: Buy.

65. **Q:** Put option gives right to what?
    A: Sell.

66. **Q:** Four broad investment-contract elements?
    A: Investment, common enterprise, profit expectation, efforts of others.

67. **Q:** Illegal effort to avoid taxes?
    A: Tax evasion.

68. **Q:** Lawful minimization of taxes?
    A: Tax avoidance.

69. **Q:** Core concept separating evasion from honest mistake?
    A: Willfulness.

70. **Q:** Double books and false-name accounts suggest what?
    A: Tax fraud indicators.

71. **Q:** What duty arises when litigation is anticipated?
    A: Duty to preserve relevant evidence/information.

72. **Q:** Continuous documented history of evidence handling?
    A: Chain of custody.

73. **Q:** Attack on witness credibility?
    A: Impeachment.

74. **Q:** Protection for confidential legal-advice communications?
    A: Attorney-client / legal professional privilege.

75. **Q:** Protection for materials prepared in anticipation of litigation?
    A: Work-product / litigation privilege.

Investigation and Reporting 76–90

76. **Q:** Three evidence types in the investigation chapter?
    A: Testimonial, documentary, digital.

77. **Q:** What should come before broad investigative activity?
    A: A clear investigation plan with goals, scope, roles, timing, and confidentiality.

78. **Q:** Useful online-source categories?
    A: Search engines, public records, vendors, archives, social media, due diligence/background sources.

79. **Q:** Why are aggregated public-record databases limited?
    A: They may be incomplete, stale, abstract-only, or jurisdiction-limited.

80. **Q:** Web content not indexed by normal search engines?
    A: Deep web.

81. **Q:** Anonymity-oriented part of deep web requiring special access tools?
    A: Dark web.

82. **Q:** Data likely lost when a device is powered down?
    A: Volatile data.

83. **Q:** Tool preventing writes to media during acquisition?
    A: Write-blocker.

84. **Q:** Bit-for-bit copy used for analysis?
    A: Forensic image.

85. **Q:** Rule for digital analysis?
    A: Analyze the image/copy, preserve the original.

86. **Q:** Cross-border assistance mechanism for evidence/recovery?
    A: MLA request.

87. **Q:** Formal judicial request across borders?
    A: Letters rogatory.

88. **Q:** Four report quality characteristics?
    A: Accurate, clear, impartial/relevant, timely.

89. **Q:** Two common ways to organize report facts?
    A: Chronologically or by transaction/scheme.

90. **Q:** Practical lesson from sample reports?
    A: Use factual, date/time-anchored, exhibit-backed documentation.

Prevention, Ethics, Auditor Roles 91–100

91. **Q:** Fraud Triangle?
    A: Pressure, opportunity, rationalization.

92. **Q:** Fraud Scale?
    A: Pressure, opportunity, integrity.

93. **Q:** Most common occupational fraud category?
    A: Asset misappropriation.

94. **Q:** Least common but costliest occupational fraud category?
    A: Financial statement fraud.

95. **Q:** Most common initial detection method?
    A: Tip.

96. **Q:** Fraud risk before controls?
    A: Inherent fraud risk.

97. **Q:** Fraud risk after controls?
    A: Residual risk.

98. **Q:** CFE reporting rule requiring disclosure if omission distorts facts?
    A: Complete reporting of material matters.

99. **Q:** Audit mindset requiring alert, questioning evaluation of fraud possibility?
    A: Professional skepticism.

100. **Q:** Three major auditor responses to management override?
     A: Test journal entries, review estimates for bias, evaluate unusual transactions.