AUD Study Sheet

Auditing & Attestation

50 Essential Topics for CPA Exam Success

PassTheCPANow.com

AUDIT REPORTS

Types of Audit Opinions

Unmodified Opinion: F/S are fairly presented in accordance with GAAP

Qualified Opinion: Misstatement or scope limitation is MATERIAL but NOT PERVASIVE

- Uses 'except for' language

Adverse Opinion: Misstatement is MATERIAL AND PERVASIVE

- States F/S are NOT fairly presented

Disclaimer: Cannot obtain sufficient evidence, scope limitation is pervasive

- Auditor expresses NO opinion

Opinion Decision Matrix

GAAP Departure: Material = Qualified, Pervasive = Adverse

Scope Limitation: Material = Qualified, Pervasive = Disclaimer

Tip: Pervasive = affects multiple accounts or fundamental to users' understanding.

Standard Report Sections

1. Opinion Section (comes FIRST)
2. Basis for Opinion
3. Responsibilities of Management
4. Auditor's Responsibilities
5. Other Matter Paragraphs (going concern, emphasis)

AUDIT RISK & MATERIALITY

Audit Risk Model

Audit Risk = Inherent Risk × Control Risk × Detection Risk

Inherent Risk: Risk of misstatement before controls (nature of account)

Control Risk: Risk controls fail to prevent/detect (client's controls)

Detection Risk: Risk audit procedures miss misstatement (auditor controls this)

$DR = AR \div (IR \times CR)$

Tip: Higher IR/CR means lower DR needed = MORE substantive testing.

Materiality

Overall Materiality: Amount influencing user decisions (5% pretax income typical)

Performance Materiality: Lower than overall (50-75%) for margin of safety

Trivial Threshold: Clearly inconsequential (3-5% of overall)

AUDIT EVIDENCE

Evidence Reliability

- External > Internal sources
- Direct auditor knowledge > Indirect evidence
- Documentary > Oral evidence
- Originals > Copies

Audit Procedures

Inspection: Examine documents, records, tangible assets

Observation: Watch process being performed

External Confirmation: Direct response from third party

Recalculation: Check mathematical accuracy

Reperformance: Re-execute controls/procedures

Analytical Procedures: Evaluate relationships and trends

Inquiry: Seek information (least reliable alone)

Management Assertions

Balance Sheet: Existence, Rights/Obligations, Completeness, Valuation

Income Statement: Occurrence, Completeness, Accuracy, Cutoff, Classification

- Existence tests for OVERSTATEMENT (confirm, inspect)
- Completeness tests for UNDERSTATEMENT (search for unrecorded)

INTERNAL CONTROL

COSO Framework - Five Components

1. **Control Environment:** Tone at top, ethics, governance
2. **Risk Assessment:** Identify and analyze risks
3. **Control Activities:** Policies, procedures, segregation
4. **Information & Communication:** Capture and share info
5. **Monitoring:** Ongoing and separate evaluations

Control Deficiencies

Deficiency: May communicate to TCWG

Significant Deficiency: MUST communicate in writing to TCWG

Material Weakness: MUST communicate in writing (most severe)

Segregation of Duties

Separate: Authorization, Custody, Recording, Reconciliation

Tip: One person should not authorize AND have custody of related assets.

AUDIT SAMPLING

Types of Sampling

Statistical: Random selection, measure sampling risk mathematically

Non-Statistical: Judgmental selection, still valid if properly applied

Attribute Sampling (Tests of Controls)

Estimates deviation rate (% of items with errors)

- Tolerable deviation ↑ = Sample size ↓
- Expected deviation ↑ = Sample size ↑
- Desired confidence ↑ = Sample size ↑

Variables Sampling (Substantive Tests)

Estimates dollar amounts

Monetary Unit Sampling (MUS): Probability proportional to size

- Good for OVERSTATEMENT testing
- Not good for understatement

Sampling Risk

- Risk of assessing control risk too LOW (dangerous)
- Risk of incorrect acceptance (dangerous)

Tip: Incorrect acceptance and assessing control risk too low affect audit effectiveness.

PROFESSIONAL RESPONSIBILITIES

Independence

In Fact: State of mind - objectivity

In Appearance: How others perceive auditor

Threats: Self-interest, Self-review, Advocacy, Familiarity, Intimidation

Professional Skepticism

- Questioning mind, critically assess evidence
- Alert to inconsistencies
- Neither assumes honesty nor dishonesty

Fraud Triangle

1. **Incentive/Pressure:** Motivation (bonuses, financial stress)
2. **Opportunity:** Weak controls, ability to override
3. **Rationalization:** Justification for fraud

Tip: Revenue recognition is PRESUMED to be a fraud risk on every audit.

OTHER ENGAGEMENTS

SSARS Engagements (Non-Issuers)

Preparation: No assurance, no report, independence NOT required

Compilation: No assurance, report issued, independence NOT required

Review: LIMITED assurance, conclusion, independence REQUIRED

SSAE Attestation

Examination: Reasonable assurance, opinion

Review: Limited assurance, conclusion

Agreed-Upon Procedures: No assurance, findings only

SOC Reports

SOC 1: Controls over financial reporting (for user auditors)

SOC 2: Security, availability, processing, confidentiality, privacy

SOC 3: Same as SOC 2 but general use (public)

Type 1: Design at point in time | **Type 2:** Design + operating over period

DOCUMENTATION & COMMUNICATION

Documentation Requirements

- Sufficient for experienced auditor to understand work
- Assembly deadline: 60 days after report
- Retention: 5 years (7 for issuers)

Communications with TCWG

Before Audit: Planned scope and timing

During/After: Significant findings, difficulties, disagreements

In Writing: Significant deficiencies and material weaknesses

Subsequent Events

Type 1 (Adjust F/S): Condition existed at B/S date

Type 2 (Disclose): Condition arose after B/S date

- Through report date: Active procedures
- After report, before issuance: Inquiry
- After issuance: No duty to search

QUALITY CONTROL & IT

Quality Control Elements

1. Leadership Responsibilities
2. Ethical Requirements (Independence)
3. Acceptance and Continuance
4. Human Resources
5. Engagement Performance
6. Monitoring

IT General Controls

Access Controls: Authentication, authorization, physical security

Program Change Controls: Testing, approval, segregation

Computer Operations: Backup, disaster recovery

IT Application Controls

Input: Data validation, edit checks, batch totals

Processing: Run-to-run totals, limit tests

Output: Report distribution, reconciliation

Using Work of Others

Internal Auditors: Assess competence/objectivity; external auditor responsible

Specialists: Evaluate competence; auditor responsible for conclusions

Service Organizations: Obtain SOC reports, consider complementary controls