Prevention and Detection of Fraud Through Auditing

Charles W. Hester
CPA/CFF/CFE/CGFM/CFIP

Course Objectives

- Designed for the auditors newly assigned to work in the fraud field and for those auditors that have been conducting audits for a while, this session will provide essential nuts-and-bolts guidance on how to approach a fraud examination or how to respond if fraud is discovered during an audit.

Course Objectives - Continued

- Identify auditor responsibilities for the prevention and detection of fraud
- Describe where fraud is committed and who commits it
- Identify common indication and detection techniques associated with illegal activity and abuse

Course Outline

- Definitions and Descriptions
- Audit Guidelines and Standards
- Prevention and Internal (Management) Controls
- Detection
- Computer Fraud
- The Investigative Process

I. Definitions and Descriptions

- Define fraud, waste, and abuse
- Describe the five elements of fraud
- Describe the four types of fraud
- Describe the criminal statutes related to fraud
- Identify control weaknesses
**Definitions**

- **Fraud** is a type of illegal act involving the obtaining of something of value through willful misrepresentation.
- **Waste** is incurring unnecessary costs as a result of inefficient or ineffective practices, systems, or controls.
- **Abuse** is where conduct of an individual falls far short of societal expectations for prudent behavior.

**What Is Fraud?**

- Wikipedia – intentional deception made for personal gain or to damage another individual.
- Webster's Dictionary – deceit, trickery; specifically, intentional perversion of truth to induce another to part with something of value or to surrender a right; an act of deceiving or misrepresenting.
- Black's Law Dictionary – ... all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated; ... it is always positive, intentional.

**Examples of Fraud**

- Bribery
- Skimming cash
- Lapping
- Check tampering
- Fraudulent disbursements (billing, payroll, expense reimbursement schemes)
- Kickbacks

**Examples of Fraud - Continued**

- Falsifying or altering documents, including performance reports
- Illegal gratuities
- Economic extortion
- Forgery
- Making untruthful statements
- Using organization’s assets for personal benefit (e.g., computers, phones, vehicles, time)
- Stealing organization’s equipment

**Incentives/pressures**

- Financial instability or operating conditions may threaten organization.
- Third parties may pressure with requirements or expectations.
- Oversight body and/or management may have personal financial impacts.
- Oversight body may establish unrealistic goals.
Opportunities

- Nature of the industry (related entities, one firm domination, subjective evaluations, etc.)
- Poor internal controls
- Oversight body does not monitor management effectively
- Complex or unstable organizational structure

Reasons for ability to rationalize fraud

- Absence of a strong ethical structure
- Poor communication or enforcement of organization’s values
- Known history of problems
- Failure to correct known problems
- Strained or antagonistic relationship between management and auditors

Why Does Fraud Occur?

Fraud Triangle:
- **Opportunity** – a person sees a way to abuse his/her position of trust and perceives a low risk of getting caught
- **Rationalization** – a person reconciles his/her behavior with commonly accepted notions of decency, honesty, and trust
- **Motivation** – for example, a financial need (real or perceived), work pressures to perform, greed

Analyze the fraud possibilities

- For each Objective/compliance issue:
  - How likely is fraud?
  - How could it occur?
  - How will you detect it?
  - How would you prevent it?
- Decide on actions to take if you find fraud

Five Elements of Fraud

1. False representation or concealment of a material fact
2. Knowledge of falsity or gross negligence
3. Intent to deceive
4. Reliance
5. Injury

Four Types of Fraud

1. Program fraud
2. Contract fraud
3. Corruption of public officials
4. Organizational conflicts of interest
Federal Fraud Statutes

- **Criminal**
  - False Statements - 18 U.S.C. 1001
  - False Claims - 18 U.S.C. 286-287
  - Embezzlement/Theft - 18 U.S.C. 641
  - Mail/Wire Fraud - 18 U.S.C. 1341/1343
  - Disclosure of Confidential Information – 18 U.S.C. 1905
  - Bribery - 18 U.S.C. 201
  - Computer Fraud - 18 U.S.C. 1029/1030

- **Civil**
  - False Claims - 31 U.S.C. 3729
  - Program Fraud Civil Remedies Act - 31 U.S.C. 3801-3812
  - Federal Acquisition Regulations - 48 CFR

Who Commits Fraud?

**Results of recent studies by the Association of Certified Fraud Examiners and KPMG:**

<table>
<thead>
<tr>
<th>Age</th>
<th>Gender</th>
<th>Rank and Median Loss</th>
<th>Time at Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;26</td>
<td>Male: 2-5% Female: 12-26%</td>
<td>Staff: 65-87%</td>
<td>&lt; 1 Year: 1-6%</td>
</tr>
<tr>
<td>26-35</td>
<td>12-26%</td>
<td>$50,000</td>
<td>1-5 Years: 39.69%</td>
</tr>
<tr>
<td>36-45</td>
<td>23-33%</td>
<td>Management: 25-38%</td>
<td>5-10 Years: 33.27%</td>
</tr>
<tr>
<td>46-55</td>
<td>7-10%</td>
<td>Sr./Exec. Mgmt: 18-36%</td>
<td>&gt; 10 Years: 25.33%</td>
</tr>
<tr>
<td>&gt;55</td>
<td></td>
<td>$482,000</td>
<td></td>
</tr>
</tbody>
</table>

A study by Marquet International identified similar trends, except for gender, which was reversed.

Who Commits Fraud?

**People in positions of responsibility and trust:**

- **Dr. Joseph Kubacki**, 62, former chair of the ophthalmology department at Temple University’s School of Medicine, sentenced to more than 7 years in prison for stealing $1.8 million through fraudulent Medicare and private insurer billings (March 2012)
- **Silas Potter Jr.**, 60, manager of the Seattle Public School District’s small-business contracting program, convicted of nine counts of using a fraudulent invoice scheme to steal $250,000 (December 2011)
- **Alan Hevesi**, 71, former New York State Comptroller, sentenced to 1-4 years in prison for approving a $250 million pension investment in exchange for nearly $1 million in benefits (April 2011)
- **Elias Castellanos**, 44, former Chief Financial Officer for the Housing Authority of New Orleans, sentenced to 46 months in prison for embezzling more than $900,000 in federal funds from HANO by falsifying time records (October 2010)
- **Silas Potter Jr.**, 60, manager of the Seattle Public School District’s small-business contracting program, convicted of nine counts of using a fraudulent invoice scheme to steal $250,000 (December 2011)

Who Commits Fraud?

**People under pressure to perform:**

- **Silas Potter Jr.**, 60, manager of the Seattle Public School District’s small-business contracting program, convicted of nine counts of using a fraudulent invoice scheme to steal $250,000 (December 2011)

Who Commits Fraud?

**People who conspire with each other:**

- **Mark Clavarella**, 61, and **Michael Conahan**, 59, former judges in Pennsylvania were sentenced to 28 years and 17.5 years in federal prison, respectively, for receiving kickbacks to send youth offenders to privately run detention centers (September 2011)
- **Laura Watson**, 47, former senior accountant at the University of Georgia, and **Kathy Knudson**, 51, former administrative assistant at UGA, were convicted of the fraudulent use of state-issued purchasing cards (July 2011)
Who Commits Fraud?

People who are testing the waters:

LaTisha Raye Reid (right), 43, former auditor at the Oklahoma State Treasurer’s Office, convicted of forgery, conspiracy, false impersonation, and stealing about $30,000 from the state’s unclaimed property fund (April 2012)

Skeeter Manor, 35, former police officer and union treasurer in Lakewood, WA, sentenced to 33 months in federal prison for stealing $47,000 in union dues and $112,000 from a charity fund established to benefit families of fallen police officers (June 2012)

Who Commits Fraud?

People who realize how lucrative fraud can be:

Harriette Walters, 52, former tax assessments manager in Washington, DC, was sentenced to 17½ years for a 20-year, $48 million embezzlement scheme that she accomplished by issuing false property tax refunds averaging $388,000 per check (July 2009)

Rita Crundwell, late 50s, chief financial officer of Dixon, IL, was arrested for stealing more than $50 million in city funds to finance an extravagant lifestyle, including funding her champion horse breeding business and spending $2.1 million on a luxury motor home (April 2012)

Who Commits Fraud?

Given the right circumstances, it could be just about anyone:

- No specific profile of a “typical” fraudster based on age, gender, race, position, years with an organization
- 05/05/90 rule says:
  - 05% of people are crooks
  - 05% of people have such a high level of integrity that they would never steal, regardless of the opportunity
  - 90% of people are basically honest, but would steal under the right circumstances
- KPMG and Marquet studies found that the most trusted people in an organization are statistically more likely to commit fraud

The Cost of Fraud

There are many costs in addition to the actual loss, for example:

- Investigation, prosecution, and other legal fees
- Sanctions from oversight agencies
- Loss of credibility and reputation
- Incarceration
- Unpaid taxes

II. Audit Guidelines and Standards

- Identify GAO Fieldwork and Reporting Standards applicable to fraud, waste, and abuse
- Describe SAS 99 (Statement on Auditing Standards issued by the American Institute of Certified Public Accountants) and what it requires of auditors
  - Including the AICPA’s Redrafting and Revisions of the Standard (SAS 113)
- Discuss IIA’s International Standards for the Professional Practice of Internal Auditing

Role Change in Detection

- Public Law 95-452, The Inspector General Act of 1978 (as amended)
- The President’s Council of the Inspectors General on Integrity and Efficiency (CIGIE)
- Generally Accepted Government Auditing Standards (GAGAS)
- Institute of Internal Auditors’ (IIA) IPPF
History of GAO Auditing Standards
• Initially Issued 1972
• Revisions 1981, 1988 and 1994
• Amendment No. 1, dated May 1999
• Amendment No. 2, dated July 1999
• Amendment No. 3, dated January 2002
• 2003 Revision (2005 Amendments)
• January 2007 Revisions
• July 2007 Revisions
• December 2011 Revisions

GAGAS – Yellow Book
• Chapter 1, Government Auditing: Foundation and Ethical Principles
• Chapter 2, Standards for Use and Application of GAGAS
• Chapter 3, General Standards

GAGAS on Fraud
• Standards for Financial Audits (Chapter 4)
• Standards for Attestation Engagements (Chapter 5)
• Field Work and Reporting Standards for Performance Audits (Chapter 6 & 7)
• Appendix I – Supplemental Guidance
• Appendix II – Conceptual Framework for Independence

Financial Audits
• GAGAS requires auditors to assess the risk of material misstatements due to fraud, waste, or abuse.
• Auditors are also required to design the audit to provide reasonable assurance of detecting material misstatements resulting from illegal acts or violations of awards.
• Auditors should report all instances of fraud and illegal acts unless clearly inconsequential.

Attestation Engagements
• In planning, design the examination-level engagement to provide reasonable assurance of detecting fraud, illegal acts, or violations of contract or grant provisions.
• In planning review-level or agreed-upon-procedures-level engagements, be alert to situations or transactions that could be indicative of fraud, illegal acts, or violations.
• Report all instances of fraud and illegal acts unless clearly inconsequential.
Performance Audits

- Design the audit to provide reasonable assurance of detecting violations of legal and regulatory requirements, contract provisions, or grant agreements, fraud, or abuse.
- The report should include all instance of fraud and illegal acts unless clearly inconsequential.
- GAGAS requires auditors to report fraud and illegal acts outside the auditee in certain circumstances.

GAGAS Appendix I

- Overall Supplemental Guidance
- Examples of Deficiencies in Internal Controls
- Examples of Abuse
- Examples of Indicators of Fraud
- Determining Whether Laws, Regulations, or Provisions of Contracts or Grant Agreements Are Significant

Some examples of fraud

- The entity’s financial stability, viability, or budget is threatened by economic, programmatic, or entity operating conditions.
- Lack of communication and/or support for ethical standards by management.
- Key documentation is lacking or does not exist.

Some examples of abuse

- Creating unneeded overtime
- Having staff perform personal errands
- Misusing position for personal gain
- Making extravagant/expensive travel choices
- Procurements contrary to policy or that are extravagant/expensive

Some examples of internal control deficiencies

- Insufficient control consciousness
- Ineffective oversight
- Systems that did not detect material misstatements
- Ineffective internal audit or risk assessment
- Fraud by senior management
- Intentional overrides of controls

Diagram:

Assess condition or activity for threats to independence

- Threat Identified?
  - YES
  - Assess threat for significance
    - NO
    - Proceed
  - YES
    - Identify and apply appropriate safeguard(s)
      - Assess safeguard effectiveness
        - Is threat eliminated or reduced to an acceptable level?
          - YES
          - No
            - Potential independence impairment; do not proceed
### AICPA Standards

- Generally Accepted Auditing Standards (AU)
- Attestation Standards (AT)
- Standards for Accounting and Review Services (AR)
- Standards for Consulting Services (CS)
- Standards for Valuation Services (VS)
- Quality Control Standards (QC)
- Ethics Standards (ET)

### AICPA’s GAAS

- 10 Generally Accepted Auditing Standards consisting of:
  - 3 General Standards, 3 Standards of Fieldwork, and 4 Standards of Reporting
- Hierarchy of Authority:
  - Category 1 – Standards
  - Category 2 – Interpretive Publications
  - Category 3 – Other Auditing Publications

### AICPA Statements on Auditing Standards

- SAS Number 54, Illegal Acts
- SAS Number 74 (AU-355), Compliance Auditing Considerations in Audits of Governmental Entities and Recipients of Governmental Financial Assistance
- SAS Number 99 (AU-794), Consideration of Fraud in a Financial Statement Audit (SAS 113)
- SAS Number 107 (AU-200), Audit Risk and Materiality in Conducting the Audit

### SAS 99 & SAS 113 – Consideration of Fraud in a Financial Statement Audit

- Issued – October 2002 & November 2006
- Supersedes SAS 82 and Amends SAS 1 (Codification of Auditing Standards and Procedures) and SAS 85 (Management Representations)
- Effective for audits of financial statements for periods beginning on or after December 15, 2002
SAS 99 and SAS 113 guidance for detecting fraud

- Maintain professional skepticism
- Consider the fraud triangle
- Staff must discuss fraud during the audit
- Obtain information to identify and assess the risks of fraud
- Make inquiries of management and others
- Document the steps taken

Auditors must exercise professional skepticism

- Auditors must always consider that fraud could be present
- Do not assume that management is honest or dishonest — require persuasive evidence
- Incorporate an element of unpredictability in the audit procedures

Audit staff regularly communicates about fraud

- Hold a brainstorming session before starting the audit
- Communicate with each other throughout the engagement
- Signer of report ensures there was appropriate communication
- Document the brainstorming session, other activities related to fraud detection, and the communications

Identify and assess the risks of fraud

- Consider the results of analytical procedures
- Consider the fraud risk factors
  - Where is the entity most susceptible to fraud?
  - What kind of fraud is most likely?
  - How would it be concealed?

Make inquiries of management and others

- About management's awareness and understanding of fraud
- Also make inquiries of:
  - Audit committee
  - Internal auditors
  - Operating personnel
  - In-house counsel
  - Others who may have information

Your reputation can be impacted

- You can miss fraud and still meet standards
- But the media usually don't understand
  - "How could you have missed ...?"
- Therefore, be sure you document all the steps you take to look for fraud
Look for compliance violations

• The auditor should design the audit to provide reasonable assurance of detecting material misstatements caused by violations of grant or contract terms

Auditors should follow up on indications of abuse

• Abuse is behavior that a prudent person would consider deficient or improper, including misuse of authority
• Abuse may not involve non-compliance
• Determine whether it occurred and its effect on financial data
• Consider it quantitatively and qualitatively
• As abuse is subjective, auditors are not expected to provide reasonable assurance of detecting it

Purpose of IIA Standards

1. Delineate basic principles that represent the practice of internal auditing as it should be.
   • The use of the word “should” in the Standards represents a mandatory obligation.
2. Provide a framework for performing and promoting a broad range of value-added internal audit activities.
3. Establish the basis for the evaluation of internal audit performance.
4. Foster improved organizational processes and operations.

Understanding the IPPA

International Professional Practice Framework

AUTHORITATIVE Guidance

Mandatory

Non mandatory strongly recommended

International Standards

Code of Ethics

Practice Guides

Mandatory Guidance
IIA’s Statement on Internal Auditing Standard No. 1200

• Proficiency and Due Professional Care
  – 1210.A2 – Internal auditor must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
  • 1220.A.1 – Internal Auditors must exercise due professional care by considering the probability of significant error, fraud or non-compliance.

IIA’s Performance Standard

• 2000 – Managing the Internal Audit Activity
  – 2060 – The CAE must report periodically to senior management and the board on the internal audit activity. Reporting must include significant risk exposures and control issues, including fraud risks.
• 2100 – Nature of Work
  – 2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
• 2200 – Engagement Planning
  – 2210.A.2 – Internal Auditors must consider the probability of significant errors, fraud, non-compliance and other exposures when developing the engagement objectives.

III. Prevention and Internal Controls

• Explain the relationship between fraud, waste and abuse and internal controls
• Describe the phases of an internal control review
• Describe the role of internal controls in preventing cases of fraud
• Identify internal control weaknesses and recommend solutions

Management Accountability and Control Mandates

• Accounting and Auditing Act of 1950
• Federal Managers Financial Integrity Act of 1982
• Chief Financial Officers Act of 1990
• Government Performance and Results Act of 1993
• Government Management Reform Act of 1994
• Federal Financial Management Improvement Act of 1996

Definition of Internal Controls

"The plan of organization and methods and procedures adopted by management to ensure that resource use is consistent with laws, regulations, and policies; that resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained, and fairly disclosed in reports."

Management Control Objectives

• An integral component of an organization’s management that provides reasonable assurance that the following objectives are being achieved:
  – Effectiveness and efficiency of operations,
  – Reliability of financial reporting, and
  – Compliance with applicable laws and regulations
Single Audit Requirement

“...each audit shall determine and report in writing whether the government, department, agency or establishment undergoing the audit has internal control systems to provide reasonable assurance that it is managing federal financial assistance programs in compliance with applicable laws and regulations.”

“COSO”

• Committee of Sponsoring Organizations of the Treadway Commission’s Internal Control – Integrated Framework

What Internal Controls Can Do

• Help achieve performance goals and objectives
• Help prevent loss of resources
• Help ensure reliable reporting
• Help ensure compliance with laws and regulations

What Internal Controls Can Not Do

• Internal Controls can only help an entity achieve its goals and objectives
  – They cannot change inherently poor management or shifts in government policy
  – They cannot provide absolute assurances, only reasonable assurance
  – They cannot prevent simple errors or mistakes
  – They can be circumvented
Control Environment

"Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management."

Risk Assessment

"Internal control should provide for an assessment of the risks the agency faces from both external and internal sources."
**Control Activities**

"Internal control activities help ensure that management’s directives are carried out. The control activities should be effective and efficient in accomplishing the agency’s control objectives."

**Examples of Control Activities**

- Top Level Reviews of Actual Performance
- Reviews by Management at the Functional or Activity Level
- Management of Human Capital
- Controls Over Information Processing
- Physical Control Over Vulnerable Assets
- Establishment and Review of Performance Measures and Indicators

**Examples of Control Activities Continued**

- Segregation of Duties
- Proper Execution of Transactions and Events
- Accurate and Timely Recording of Transactions and Events
- Access Restrictions to and Accountability for Resources and Records
- Appropriate Documentation of Transactions and Internal Control

**Control Activities Specific for Information Systems**

- General Control
- Application Control

**Information and Communications**

"Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities."

**Monitoring**

"Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved."
Green Book Through the Years

1983 → Present

From COSO to Green Book: Harmonization

A Framework → Standards

GAGAS on Internal Control

- Field Work and Reporting Standards for Financial Audits (Chapter 4)
- General, Field Work and Reporting Standards for Attestation Engagements (Chapter 5)
- Field Work and Reporting Standards for Performance Audits (Chapter 6 & 7)

AICPA Internal Control Requirements

- SAS No. 109 – Understanding the Entity and Its Environment and Assessing the Risk of Material Misstatement
- SAS No. 110 – Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained
- SAS No. 112 – Communicating Internal Control Related Matters Identified in an Audit
- SSAE No. 15 & 17 – An Examination of Internal Control Over Financial Reporting Integrated with an Audit of the Entity’s Financial Statements

IIA Internal Control Requirements

- Performance Standard 2130, Control – The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.
  - Practice Advisory 2130-1
  - Practice Advisory 2130.A1.1
  - Practice Advisory 2130.A1.2
OMB Circular A-123, Management’s Responsibility for Internal Control

- Establishing Management Controls
  - Definition of Management Controls
  - Developing Management Controls
  - GAO Standards
- Assessing and Improving Management Controls
  - Sources of Information
  - Identification of Deficiencies
  - Role of A Senior Management Council

OMB Circular A-130, Management of Federal Information Resources

- Revised November 28, 2000
- Provides uniform government-wide information resources management policies
- Includes procedural and analytical guidelines for implementing specific aspects of the policies

Phases of an Internal Control Review

- Consider the types of errors and frauds that could occur
- Determine control procedures and structure that would prevent or detect such error and fraud
- Determine whether the controls are in place and are performing satisfactorily

Steps Performed in a Vulnerability Assessment

- General Control Environment Review
- Analysis of Inherent Risk
- Evaluation of Safeguards
How Is Fraud Prevented and Detected?

By implementing processes (internal controls) to provide reasonable assurance that the organization will achieve its objectives for:

- Effective and efficient operations
- Reliable reporting
- Compliance with applicable laws and regulations

It is important to emphasize to management that it is their responsibility to implement these processes!

How Is Fraud Prevented?

Eliminate the Opportunity!

How Is Fraud Prevented and Detected?

The Control Environment – the most important component because it sets the tone of the organization and provides discipline and structure for the other components; examples include:

- The organization’s commitment to competence
- Management’s philosophy and operating style
- The attention and direction of the organization’s leadership

How Is Fraud Prevented and Detected?

Risk Assessment – a dynamic and iterative process for identifying, analyzing, and managing the financial, compliance, and operational uncertainties facing the organization; potential areas of risk include:

- Financial
- Human Resources
- Health and Safety
- Information Systems

Risks constantly change, so the strategies must remain fluid

Every risk cannot be eliminated or mitigated!

How Is Fraud Prevented and Detected?

Control Activities – the policies and procedures maintained by an organization to address their risk-prone areas; an important component because they eliminate or mitigate risks; examples include:

- Separation of duties
- Reconciling records
- User IDs and passwords; not allowing them to be shared
- Depositing receipts timely
- Supervisory review and approval

How Is Fraud Prevented and Detected?

Information and Communication – identifying, capturing, and exchanging financial, operational, and compliance information in a timely manner; provides the mechanism for effective decision-making; examples include:

- Performance reports
- Financial records and statements
- Payroll reports
- Inventory records
- Verbal communication – e.g., staff meetings
How Is Fraud Prevented and Detected?

Monitoring – assessing the internal control activities for potential and actual breakdowns that could make it difficult for an organization to accomplish its goals; examples include:
- Asking questions about what allowed an error to occur
- Determining the reason for not meeting performance goals
- Investigating why an error that occurred was not identified timely

IV. Detection

- Profile of a White-Collar Criminal
- Identify “Red Flag” indicators of white-collar crime
- Describe detection techniques to identify fraud

Profile of a White-Collar Criminal

- Psychologically normal
- Frequently middle-managers
- Often rationalize fraud
- Usually act alone
- Fraud is committed by people we trust
  - Look for the person who never takes leave
  - Look for the “indispensable person”

Identify “Red Flag” Indicators of White-Collar Crime

- Situational Pressure
  - Employees Against the Company
  - Management on Behalf of the Company
- Opportunity
  - Employee Embezzlement
  - Management Fraud
- Personal Characteristics

Detection Techniques to Identify Fraud

- Accounts Payable - Confirmations
- Accounts Receivable - Confirmations
- Bank Account Balances and Loans from Banks - Confirmations
- Cash Flow Analysis
- Collateral - Checking Collateral
- Computer Matching

Detection Techniques to Identify Fraud - Continued

- Contract Prices - Increasing Through Modification
- Costs - Claiming Unwarranted Costs
- Costs - Questioned Costs
- False Claims/Labor Fraud
- Fraud Indicators
- Hot Lines and Complaint Centers
Detection Techniques to Identify Fraud - Continued

- Internal Controls
- Inventory Cut-Offs
- Kiting
- Lapping
- Net Worth Calculation
- Premature Withdrawals Under a Letter of Credit

- Purchases - Better Quality Items Than Received
- Purchases - Splitting Purchases
- Settling of Claims
- Theft or Illicit Sale of Fixed Assets
- Theft of Inventory
- Theft of Materials and Supplies

Detection Techniques to Identify Fraud - Continued

- Timecards - Making Altered or Erroneous Charges
- Timecards - Labor Charges Posted by Supervisor
- Vendors - Increasing Invoices
- Vendors - Fictitious/Nonexistent Vendors

V. Computer Fraud

- Describe some of the threats to computer-based systems
- Identify safety measures to protect the computer from tampering
- Describe standards to protect computer systems from fraud

Threats to Computer-Based Systems

- Hardware
- Software
- Organization
- Personnel
- Physical Security
- Off-line Input/Output

Threats to Computer-Based Systems - Continued

- External
- Data Communications
- External On-line
- Internal On-line
- EDP Facilities
- Users
Safety Measures for Automated Systems

- Application Controls
  - Input Controls
  - Processing Controls
  - Output Controls
- General Controls
  - Use of the Wrong Files
  - Accidental Destruction
  - Recovery Controls

Internal Control Characteristics for Computer Systems

- Separation of Duties
- Authorized Transactions
- Recording Transactions
- Access to Assets
- Record versus Assets

Control Characteristics for Computer Systems - Continued

- Risks
- Transaction Objectives
- ADP Controls
- Audit Trails

GAO Guidance

- Evaluating Internal Controls in Computer-Based Systems, Audit Guide, June 1988
- Assessing the Reliability of Computer-Processed Data, April 1991 (GAO/OP-8.1.3)
- Preparing, Documenting, and Referencing Microcomputer Data-Based Applications, April 1991 (GAO/IMTEC-11.1.1)

AGA's Online Government Fraud Prevention ToolKit
IIA’s Global Technology Audit Guides

Technology-Based Audit Techniques

- IIA’s Global Technology Audit Guides:
  - GTAG-1: IT Controls, March 2005
  - GTAG-2: Change and Patch Management Controls, June 2005
  - GTAG-3: Continuous Auditing, October 2005
  - GTAG-4: Management of IT Auditing, March 2006
  - GTAG-5: Managing and Auditing Privacy Risks, June 2006
  - GTAG-6: Managing and Auditing IT Vulnerabilities, October 2006
  - GTAG-7: Information Technology Outsourcing, March 2007
  - GTAG-8: Auditing Application Controls, July 2007

- GTAG-11: Developing the IT Audit Plan, July 2008
- GTAG-12: Auditing IT Projects, March 2009
- GTAG-14: Auditing User-developed Applications, June 2010
- GTAG-15: Information Security Governance, June 2010
- GTAG-16: Data Analysis Technologies, August 2011
- GTAG-17: Auditing IT Governance, July 2012
What is GTAG?

GTAG - Global Technology Audit Guide

- To provide easy-to-understand information technology audit guides to Chief Audit Executives, Audit Committees and Executive Management
- To provide a mechanism to quickly address new IT Issues
- To produce technical audit guides on a global scale

Who is GTAG target audience?

Primary target - Chief Audit Executive (CAE)

- Many CAEs face the challenge to understand technology, which is necessary to plan and conduct internal audit.
- CAEs are not well-served by many existing guides, such as Cubit, which tend to target technical IT auditor and IT management.
- Given the broad responsibility of CAEs, GTAG series provide them a high level overview on risk management and control related to IT.

GTAG is practically immeasurable to busy executives who need to quickly understand technology issues and evaluate the impact on their organization.

GTAG-1
Information Technology Controls

It covers:
- Understanding of IT controls
- Importance of IT controls
- Organizational roles and responsibilities for ensuring IT controls
- Analyzing risks
- Monitoring and techniques
- IT control assessment

GTAG-2
Change and Patch Management Controls: Critical for Organizational Success

It covers:
- Why IT change and patch management controls are foundational to a healthy IT environment
- How IT change and patch management controls help manage IT risks and costs
- What works and doesn't work in practice
- Describes sources of change and the likely impact on business objectives

GTAG-3
Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

It covers:
- Role of continuous auditing in today’s internal audit environment
- Relationship of continuous auditing, continuous monitoring, and continuous assurance
- The application and implementation of continuous auditing
- Benefits of a continuous, integrated approach

GTAG-4
Management of IT Auditing

It covers:
- Defining IT
- IT-related Risks
- Defining IT Audit Universe
- Executing IT Auditing
- Managing IT Auditing
- Emerging Issues
GTAG-5
Managing and Auditing Privacy Risks
It covers:
• What is Privacy
• Privacy Principles and Frameworks
• Privacy Impacts and Risk Model
• Privacy Controls
• Good and Bad Performers
• Internal Auditing’s Role
• Auditing Privacy
• CAE’s Top 10 Privacy Questions

GTAG-6
Managing and Auditing IT Vulnerabilities
It covers:
• Define the vulnerability management lifecycle
• The scope of a vulnerability management audit
• Organizational maturity
• Metrics to measure vulnerability management practices
• Top 10 vulnerability management questions

GTAG-7
Information Technology Outsourcing
It covers:
• How to choose the right IT outsourcing vendor?
• What are the best ways to manage outsourcing contract agreements?
• What are the main outsourcing risks and how to mitigate them?
• What are the key outsourcing control considerations from the standpoint of both client operations and service provider operations?
• Which is the most effective framework for establishing outsourcing controls?

GTAG-8
Auditing Application Controls
It covers:
• What is application control?
• What is the relationship between application control and general controls?
• Why rely on application controls?
• How to scope a risk-based application control review?
• What are the steps to conduct an application controls review?
• A list of key application controls
• A sample audit program

GTAG 9 - Identity and Access Management
Matters to consider:
• Who has access to what information?
• Is the access appropriate for the job being performed?
• Is the access and activity monitored, logged and reported appropriately?

GTAG 10 – Business Continuity Management
Matters covered:
• How continuity planning can minimize operation disruptions
• The components of an effective continuity plan
• How impact analysis can help identify which operations need to be recovered first following a disruption
• Ways to maximize audit’s values in continuity planning
GTAG 11 – Developing the IT Audit Plan
- Provides guidance to:
  - Explore the relationship between IT and operation
  - Define IT audit universe
  - Develop IT audit plan from the IT audit universe
  - Provide examples of developing an IT audit plan

GTAG 12 – Auditing IT Projects
- What is covered:
  - The case for auditing IT projects
  - Understanding the impact
  - Statistics on project failures
  - Purpose and benefits of audit involvement
  - Five key focus areas for project audits
  - Project audit planning

GTAG 13 – Fraud Prevention and Detection in an Automated World
- What’s covered:
  - The fraud-related standards
  - Identifying IT fraud risks and schemes
  - Implementing IT fraud risk assessments
  - Using technology to prevent and detect fraud
  - Utilize data analysis to detect fraud

GTAG 14 – Auditing User-developed Applications
- Topics covered:
  - Definitions
  - User-developed applications risks
  - Internal audit’s role
  - Best practices, tools & techniques

GTAG 15 – Information Security Governance
- Major points:
  - Audits can help an organization understand the risks and options to create and effective ISG activity
  - ISG provides a framework for the organization to make appropriate risk mitigation decisions to protect and react to external and internal threats
  - ISG allows continuous feedback from line management to those charged with governance

GTAG 16 – Data Analysis Technologies
- Major points:
  - How can data analysis help auditors
  - Using date analysis technology
  - Elaboration on key concepts
  - Where should auditors begin
GTAG 17 – Auditing IT Governance

Key areas auditor should address:
- Chief IT Officer related roles and responsibilities.
- Accountability and decision-making.
- IT performance monitoring and reporting metrics, including financial management of IT operations and projects.
- CxO level of understanding of how IT supports and enables the achievement of the organization's strategy and objectives.
- Alignment between IT and the organization.
- IT governance risks and controls.

Guide to the Assessment of IT Risk (GAIT)

- The GAIT Methodology, issued August 2007
- GAIT for IT General Control Deficiency Assessment, issued March 2008
- GAIT for Business and IT Risk, issued March 2008
  - Case Studies of Using GAIT, issued September 2008

Definition of Risk

- Risk is the possibility of an event occurring that will have an impact on the achievement of objectives.
  - Risk is measured in terms of impact and likelihood.
- Risk Management is a process to identify, assess, manage and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.
  - Residual Risk is the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

VI. The Investigative Process

- Describe the types of evidence as required in the Government Audit Standards
- Describe the Federal Rules of Evidence
- Identify factors relevant to cooperation with investigators and the timing and content of investigative referrals

Gathering Evidence

- Rules of Evidence
- Definition of Evidence
- Classifications of Evidence
  - Direct Evidence
  - Circumstantial Evidence
  - Oral, Documentary and Real Evidence

Gathering Evidence - Continued

- Relevancy and Competency
- Hearsay
- Best Evidence Rule
- Privileged Relationships
GAGAS on Evidence
• Sufficient
• Competent
• Relevant

Federal Rules of Evidence
2. Judicial Notice
3. Presumption in Civil Actions and Proceedings
4. Relevancy and Its Limits
5. Privileges

Federal Rules of Evidence
Continued
6. Witnesses
7. Opinions and Expert Testimony
8. Hearsay
9. Authentication and Identification
10. Contents of Writings, Recordings, and Photographs
11. Miscellaneous Rules

Purpose of Interviews
• Get leads
• Get interpretations
• Get explanations
• Determine causes
• Save time

Interview Preparation
• Who to interview
• Know your subject
• Prepare agenda
• Organize material
• Appointments
• Arrangements
• Keep an open mind

Conducting the Interview
• Establish rapport
• Note-taking
• Observe interviewee behavior
• Know your interviewee
• Be tactful
• Confidential information
**Concluding the Interview**
- Know when to end
- Check agenda
- Review information
- Allow for re-interview
- Writing up interview
- Verify information

**Reports of Investigation**
- Legal Issues
- Adverse Actions
- Other Potential Uses of Reports

**Legal Issues**
- Accuracy
- Fact Versus Hearsay
- Fact Versus Opinion
- Fact Versus Conclusion
- Wording
- Sources of Evidence

**Legal Issues - Continued**
- JANE DOE Decision
- Rules of Discovery and Inspection
- The Jencks Act
- Brady Material
- Agent’s Rough Notes

**Adverse Actions**
- Statement of Reasons
- Release of Reports
- Support Files
- Evidence and Proof

**Other Uses of Reports**
- Performance Evaluations
- Professionalism and Training
- Pattern or Trends
- Prevent Recurrences
- Investigation’s Effectiveness
- Compile Statistics
Report of Investigation - Content

- To prosecute a case, must basically know:
  - That an offense was committed
  - Who executed it
  - What evidence is available
  - Which witnesses should be subpoenaed or called to testify

Report of Investigation - Format

- To convey the information describe:
  - How fraud conceived
  - Who played what parts
  - Where and how long operated
  - Specific loss
  - Information to comprehend the magnitude, nature and characteristics of the fraud

Standard Report Format

- Synopsis
- Identification (entities and individuals)
- Background
- Statutes
- Witness Listing
- Evidence Listing
- Unproductive Investigations

Standard Report Format - Continued

- Scientific, Technical, or Audit Reports and Schedules
- Table of Contents for Investigative Forms
- Details of Investigation (witness interviews, record searches, etc.)
- Index of Interviews/Records
- Attachments

Auditors work differently than investigators

- Can cause the auditor to get frustrated
- Can cause the investigator to get frustrated
- Can create hostilities
- Can cause inefficiencies
- Can cause investigations to fail

Auditors tend to work from the top down

- Have an extensive workplan
- Evaluate internal controls
- Make risk assessments
- Define objectives
- Draw overall conclusions
- Consider materiality
Investigators work inductively

• Have a more general workplan
• Gather information
• Put information together and draw conclusions
• Interested in specifics
• Materiality is less important

Auditors have an established process

• Advise auditee of the upcoming audit
• Hold a formal entrance conference
• Conduct interviews (not interrogations)
• Accept copies and extracts
• Allow time for auditee to provide
  – Additional data
  – Response to findings

Investigators are looking for an indictment

• Usually start investigation covertly
• Conduct interrogations (not interviews)
• Try to determine whether suspect is telling the truth
• Try to throw target off-balance
• Try to catch targets lying or providing wrong data
• Want original documents

Interviews and interrogations differ substantially

• The objectives are different
• The settings are different
• The techniques are different
• The timing is different
• Questioners often respond differently

Auditors determine scope and extent of the audit

• Determine audit scope and objectives
• Prepare audit program
• Decide on extent of tests
• Determine when the audit is finished
• Decide what to include in the report

Investigators usually work with a prosecutor who determines:

• The crime to be prosecuted
• The evidence needed
• The investigative techniques
• When the case is complete
• Which counts to indict on
Differences can cause investigators to believe that auditors:

- Follow their audit program blindly
- Consider their expertise is superior to other professions
- Have unrealistic expectations for due dates
- Don’t want to cooperate with the prosecutor
- Have no interviewing skills

Prosecutors may consider auditors as a “free resource”

- Don’t appear on prosecutor’s payroll
- If they are fully occupied, the investigation can continue
- Therefore, requests for audit assistance are plentiful
- Auditors are often assigned the “donkey work”

Auditors need to become a partner in the process

- Make sure they know the objectives of the work
- Use their expertise to find more effective techniques
- Don’t let the investigator be the sole point of contact for the prosecutor
- Ask whether all the data requested is really needed

Summing up

- Joint investigations can be very effective
- But the auditors and investigators must understand how each other works
- Each must respect the other’s profession and processes
- They must be working for the same goal
- Agency management must reward both parties equally

Differences can cause auditors to believe that investigators:

- Work haphazardly
- Don’t have any timetables
- Cannot make decisions by themselves
- Have preconceived notions about guilt
- Act unfairly towards targets

Audit management may not value investigations

- They may assign the weak auditors to investigations
- They may resent the loss of audit time
- They may not be rewarded for contributing audit time to investigations
- They may consider that investigations do not benefit programs as much as audits
Summation

• Increased awareness in the 1970’s, 1980’s, 1990’s, and the New Millennium
• White-collar criminals
• Professional Requirements
  - GAO
  - AICPA
  - IIA
  - ACFS

Summation - Continued

• Usually auditors look for:
  - Overall conclusions
  - Large dollar impact
  - Ways to improve operational systems
• Fraud auditing involves:
  - Many individual transactions
  - Frequently, small dollar items
  - Identifying individual errors

Summation - Continued

• Audit programs are designed to provide overall conclusions
  - Conduct risk assessments
  - Develop tests
  - Utilize statistical samples
  - Don’t rely on chance
• But we learn about fraud by chance
  - Allegations
  - Comments by Auditee personnel
  - Observation

Summation - Continued

• Materiality may not be important
  - Amounts are rarely enough for a major finding
  - But public interest is greater than big issues
• Trust your instincts
  - If you suspect fraud, follow up on anything that looks unusual
  - If it “smells” bad, it probably is bad
  - But, be ready to change your mind

Summation - Continued

• Common fraud techniques
  - Most frauds are repeating
  - Too tempting to stop
  - Perpetrator unable to repay
• Be alert to hints from Auditee staff
  - They may want to tell, but are uncomfortable
  - May hint through jokes
  - Make your ground rules clear

Summation - Continued

• You need to “Think Dirty”
  - Who is in the best position to steal?
  - What could I steal?
  - How could I steal?
  - How would anyone find out?
CONCLUSION

• Requirements for success in the fight against fraud
  - An environment that does not tolerate fraud against the organization
  - An environment that does not tolerate fraud for the organization
  - Executives, managers, operating personnel and auditors trained to know fraud indicators and symptoms for their areas