

Managing Fraud Risk September, 2008

Charles A. Petosa, MBA, CPA
Senior Consultant, Relevante Inc.
CPetosa@Relevante.com

1. Fraud Hot Topics; In the Headlines of Business, Financial and Legal Communities
2. The Genesis of Fraud
3. Deterrence and Detection
4. Fraud Risk Management

Fraud Hot Topics

- ▼ Ownership:
 - ▼ Public
 - ▼ Private
 - ▼ Not-For-Profit
 - ▼ Government

- ▼ Responsibility
 - ▼ Corporate
 - ▼ Operating Unit

- ▼ Role
 - ▼ Financial
 - ▼ Non-Financial

- ▼ Focus
 - ▼ Internal
 - ▼ External

- ▼ Common Interest
 - ▼ Impact on stakeholders

Financial Reporting Fraud

- ▼ Manipulation, falsification, alteration of accounting records
- ▼ Misrepresentation or intentional omission of amounts
- ▼ Misapplication of accounting principles
- ▼ Intentionally false, misleading or omitted disclosures

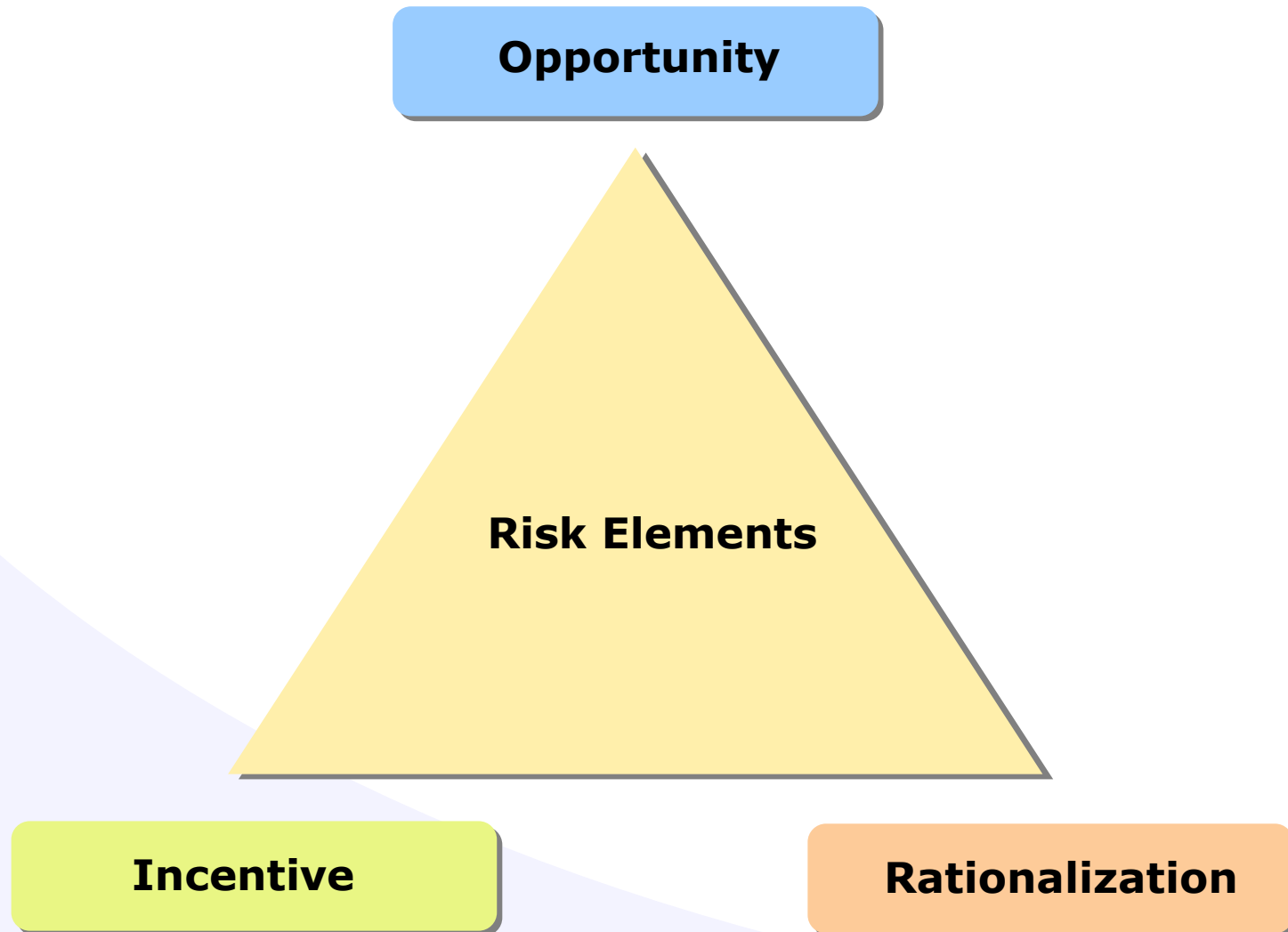
Misappropriation of Assets

- ▼ Theft of tangible assets by internal or external parties
- ▼ Theft/trading in intangible assets
- ▼ Sales of proprietary information
- ▼ Causing improper payments

Corruption

- ▼ Making or receiving improper payments
- ▼ Offering bribes to public or private officials
- ▼ Receiving bribes, kickbacks or other payments
- ▼ Aiding and abetting fraud by others

The Genesis of Fraud



- ▼ Several recent surveys suggest fraud is worsening
- ▼ SOX may not be slowing growth of corporate fraud as once thought
- ▼ Majority of respondents believe fraud is more pervasive
- ▼ Common causes found:
 - “We needed to make the numbers.” - 80%
 - “I’m in it for myself.” - 70%
 - “I won’t get caught.” - 40%
 - “I don’t think it’s fraud anyway.” - 40%

Over half of U.S. companies surveyed reported significant frauds

▼ **Direct financial damage:**

Per tangible incident (asset misappropriations, false pretenses/deception, counterfeiting) - \$1.7 million

▼ **Collateral damage:**

▼ Brand, reputation, staff motivation, business relations

▼ **Incidence Over 2 Years:**

Larger companies (>5,000 employees) – 62%

Smaller companies (<200 employees) – 32%

▼ **Magnitude:**

Smaller companies – 10% reported losing over \$1 million

Larger companies – 6% reported losing over \$10 million

Not Reflected: drop in share prices, increase in audit fees, drop in credit ratings, lawsuits, higher insurance premiums, management displacement.

Fraud Deterrence and Detection

- ▼ **Control Environment** – foundation, tone, integrity
- ▼ **Risk Assessment** – identify and respond to business and financial statement risks
- ▼ **Control Activities** – policies, procedures, activities
- ▼ **Information and Communication** – up, down and across the organization
- ▼ **Monitoring** – regular assessment of performance quality, design and operation of controls, and corrective action and remediation of deficiencies

- ▼ Segregation of duties within ERP and manual systems
- ▼ Personnel rotation and mandatory vacations
- ▼ Training and awareness
- ▼ Background checks
- ▼ Verification of vendor and payroll additions
- ▼ Account Reconciliations – 100% or major balance sheet accounts
- ▼ Spreadsheet Controls – end user computing inventory, testing
- ▼ Trust BUT Verify
- ▼ Trade-Offs – Fraud triangle vs. cost-benefit

- ▼ **Complaints: accounting, internal control, audit, business practice**
- ▼ **Anonymous and confidential: continuously available**
- ▼ **Procedure Documentation:**
 - ▼ **Call receipts**
 - ▼ **Records retention**
 - ▼ **Complaint handling**
- ▼ **Timeliness of response to caller**
- ▼ **Company Guidance:**
 - ▼ **Training and encouragement to use communicated to all employees**
 - ▼ **Advertised widely**
 - ▼ **May be handled by a third-party provider or internally managed**

- ▼ **Strategic Planning, Fraud Risk Assessments** – identify, rank and address business risks
- ▼ **Budgets and Forecasts** – variance analysis, regular updates
- ▼ **On-going Monitoring** – Analysis reports (i.e. dashboard), balanced scorecard, KPI/metrics
- ▼ **Data Extraction Software** – analyzing large volumes of data and transactions for “outliers” or unexpected trends and relationships
- ▼ **Emphasize AS 5, SAS 99, SAS 112, SEC Releases and special studies**
- ▼ **Focus on Financial Statement Close Cycle:**
 - ▼ Unusual Non-standard Journal Entries
 - ▼ Estimates
 - ▼ Related Party Transactions
 - ▼ Management of Results

▼ **General IT Controls**

- ▼ Organization and operation of the IT function
- ▼ Change Control systems development and documentation
- ▼ Hardware and systems software
- ▼ Data and procedural processes
- ▼ Physical and Logical Access

▼ Application Controls

- ▼ Input

- ▼ Processing

- ▼ Output

▼ IT Areas of Fraud Focus Include:

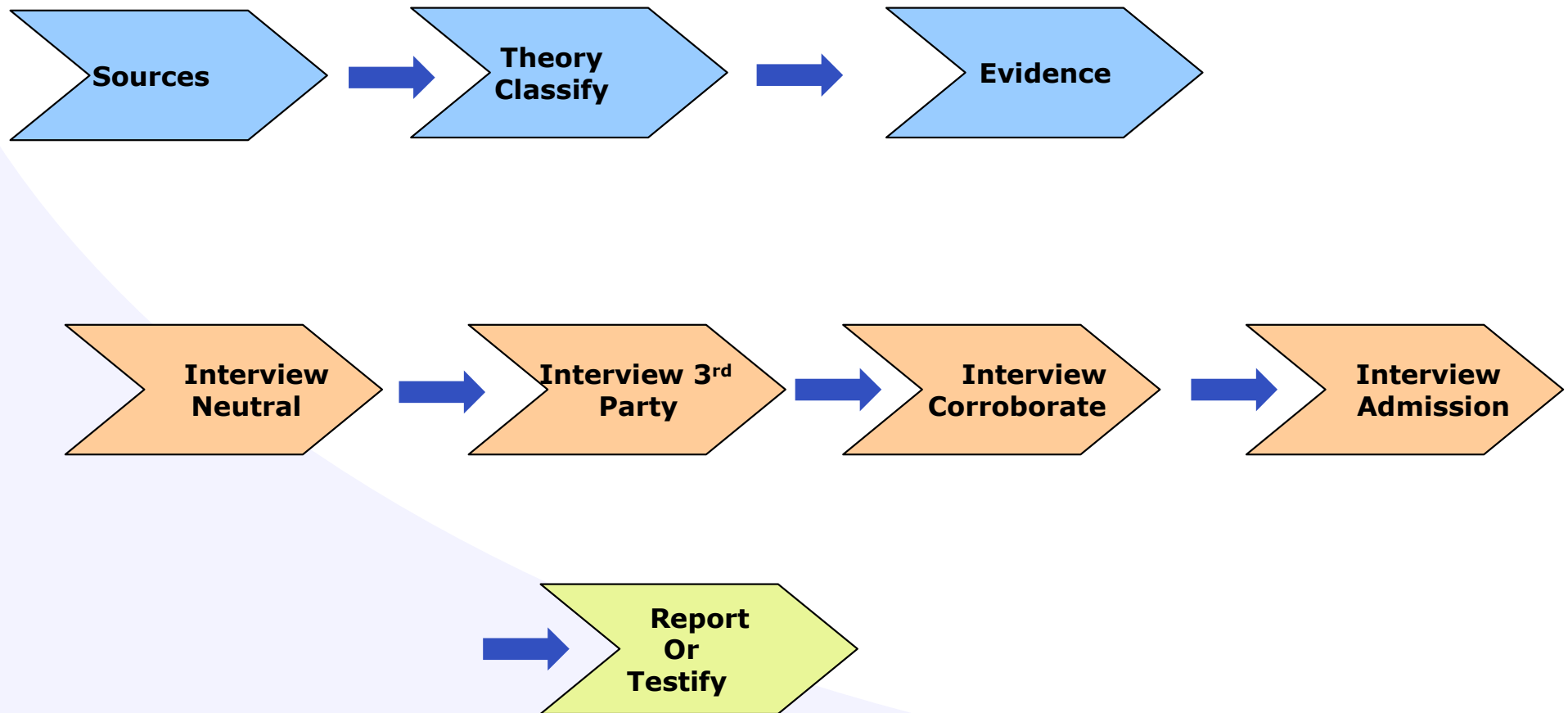
- ▼ Network
- ▼ Disaster Recovery, Business Continuity plans
- ▼ Logical Security, user names and passwords
- ▼ Wireless Area Networks (WANs)
- ▼ Remote workers
- ▼ E-Commerce – online payments, customer data, Electronic Data Interchange (EDI)

▼ Composite Study Results

#1	Tips	40%
#2	Internal Audit	25%
#3	Other Accident	21%
#4	Other Internal Control	14%

Note: *Tips can be internal (employees) or external (media, vendors, customers, regulators). External auditor detection of fraud has increased since Enron.*

- ▼ Male – 85%
- ▼ Average Tenure < 5 Years – 57%
- ▼ College Educated – 38%
- ▼ Company Manager – 52%
- ▼ Age 31 to 50 – 72%



Misappropriation	Financials	Corruption
Larceny	Timing differences	Conflict of interest
Skimming	Fictitious revenues	Bribery
Misuse	Concealed liability	Illegal gratuities
Billing	Asset valuation	Extortion
Payroll	Disclosure	
Reimbursement		
Checks		

Fraud Risk Management

Oversight Efforts

- ▼ **Audit Committee or Board** – evaluate and oversee; awareness and education; potential for management override; information and feedback network
- ▼ **Management** – effective policies and procedures; discharge of duties; technical competence
- ▼ **Internal Audit** – identify indicators of fraud; deterrence and detection
- ▼ **External Audit** – assess management’s processes; candid dialogue with Board; entity’s susceptibility to fraud; higher level of responsibility to consider and detect
- ▼ **Fraud Examiners** – supplement internal audit; direct examinations; consult on preventive measures

- ▼ Tone at the Top – Directors and Officers lead by example
- ▼ Mission Statement – good corporate citizenship
- ▼ Code of Conduct and Ethics – articulate, emphasize, confirm
- ▼ Positive Workplace Environment – cultivate employee morale
- ▼ Hire and Promote Appropriate Employees – values and ethics
- ▼ HR Management – hiring, compensation, promotion, etc.
- ▼ Training – anti-fraud, accountability, communications & expectations
- ▼ Discipline – effective, timely, suitable and communicated

- ▼ Qualified, independent, engaged Board
- ▼ Internal Audit oversight of Board activities
- ▼ Candid self-assessment by Board
- ▼ Clear communication channels with management
- ▼ Code of Conduct, documented and communicated
- ▼ Whistleblower venue
- ▼ Quality and quantity of senior management
- ▼ Effective HR policies, compensation and succession planning for senior management

- ▼ Perspective – future; proactive risk mitigation and controls
- ▼ Focus – enterprise-wide strategic, process and business risk
- ▼ Style – advisory vs. adversarial
- ▼ Responsibility – auditing and consulting
- ▼ Structure – member of the “C” suite
- ▼ Reporting – Audit Committee
- ▼ Independence and Objectivity – litmus tests
- ▼ Technology – real time monitoring and IT auditing
- ▼ Fraud Prevention and Detection – leading the charge

- ▼ Industry or Operational stress
- ▼ Poor Monitoring of Management
- ▼ Instability of Organization
- ▼ Poor Internal Control
- ▼ Economic Conditions,
- ▼ Third Party Expectations,
- ▼ Personal Financial Stake
- ▼ Financial Targets
- ▼ Unethical Behavior (Tone at the Top)
- ▼ Overly Aggressive Approaches
- ▼ Materiality Argument

- ▼ Ease of Misappropriation
 - ▼ Inadequate Control
 - ▼ Management Override

- ▼ Personal Obligations, Adverse Relationships

- ▼ Disregard for Control, Awareness of Wrongdoing, Morale, Lifestyle Changes

- ▼ Level of business done with governmental authorities
- ▼ Level of business done outside U.S.
- ▼ Extent of autonomy granted employees in business dealings
- ▼ Lack of monitoring of business dealings
- ▼ Weak control environment
- ▼ Lack of ethical standards across the organization (i.e. Code of Ethics and Accountability to the Code)

- ▼ **Are internal controls sufficiently weak to induce exploitation?**
 - ▼ **Do employees know controls are weak?**
 - ▼ **Do employees know controls don't exist?**
 - ▼ **Do employees *think* controls don't exist?**

- ▼ **Are existing internal controls susceptible to override?**
 - ▼ **Does monitoring exist?**
 - ▼ **Are there any override mechanisms in place?**

- ▼ **Are potential frauds easily concealed?**
 - ▼ **Is the structure of the organization such that frauds are easy (easier) to conceal?**

- ▼ **Assemble a population of frauds to aid in determining inherent risk**
 - ▼ What types of fraud are likely in your industry, organization, processes?

- ▼ **Assess the likelihood/significance of these inherent risks**
 - ▼ History – has it happened before? Recently?
 - ▼ Put your ear to the ground... what do you hear?
 - ▼ Any significant environmental changes that might exacerbate risks?

- ▼ **Build a Response Mechanism**
 - ▼ Assess appropriate, timely and cost-effective responses to potential risks
 - ▼ Implement a formal response protocol

- ▼ Who is Responsible?
 - ▼ Internal Audit
 - ▼ IT Department
 - ▼ Middle Management
 - ▼ Senior and Operational Management
 - ▼ CFO
 - ▼ CEO
 - ▼ Board of Directors

1. Build a cross-functional team or task force
2. Identify potential schemes
3. Assess likelihood of inherent risk
4. Assess significance of risk
5. Determine staff members or departments potentially involved
6. Analyze existing fraud controls
7. Assess effectiveness of existing controls

8. Determine residual risk after contemplating effects of existing controls
9. Formulate potential responses
10. Subject each to cost-benefit analysis
11. Choose “optimal” response for each
12. Design new response process and integrate it into a formal fraud program

- ▼ American Institute of Certified Public Accountants www.aicpa.org
- ▼ Association of Certified Fraud Examiners www.cfenet.com
- ▼ Financial Executives International www.fei.org
- ▼ Information Systems Audit and Control Association www.isaca.org
- ▼ The Institute of Internal Auditors www.theiia.org
- ▼ Institute of Management Accountants www.imanet.org
- ▼ National Association of Corporate Directors www.nacdonline.org
- ▼ Society for Human Resource Management www.shrm.org
- ▼ Institute for Fraud Prevention www.theifp.org
- ▼ IT Governance Institute www.itgi.org
- ▼ Public Company Accounting Oversight Board www.pcaobus.org
- ▼ CFO Magazine www.cfo.com

- ▼ "Managing the Business Risk of Fraud" a joint effort sponsored by IIA, AICPA, ACFE; 7/2008
- ▼ Essentials of Corporate Fraud by Tracy Coenen
- ▼ CFO.com February 13, 2007; May 1, 2008
- ▼ SEC Rule 13a-15, Definition of Internal Control, extracted from Sarbanes-Oxley Act of 2002
- ▼ AICPA Auditing Standards Section 316, Consideration of Fraud in a Financial Statement Audit, extracted from Statement on Auditing Standards #99, 2002
- ▼ AICPA Training on SAS #99 and Fraud, Chapter 3
- ▼ Journal of Accountancy; January, 2007; "Worldwide: Looters Have a Foothold"
- ▼ PWC Global Economic Crime Survey 2007
- ▼ Sarbanes-Oxley Compliance Journal; "Fraud: Risk and Reward"; Shukla, R.
- ▼ Training Guide "Fraud and the CPA"; Surgent-McCoy, based on SAS#99; also with credit to "Global Audit Watch's Fraud Detection (Codere)" and ACFE Uniform Occupational Fraud Classification
- ▼ Pennsylvania CPA Journal; Spring, 2006; "On The Trail: How Financial Audits Make the Path for Forensic Teams"; Brazina, P.
- ▼ Journal of Accountancy; March, 2007; "Internal Control Guidance Not Just a Small Matter"; Rittenberg, E.; Martens, F.; Landes, C.