

INTERNAL AUDIT INVESTIGATION TECHNIQUES

REUBEN GITAH

FRAUD IN CONTEXT

Definition Fraud is generally defined in the law as an *intentional misrepresentation of material existing fact made by one person to another with knowledge of its falsity and for inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes other statements misleading (USLegla.com).*

FRAUD & INTERNAL AUDIT

Occupational fraud is the most practical categorization related to Internal Audit, and is intentional misuse of financially-related employment matters for personal gain.

- ✖ ACFE Occupational Fraud Categories
 - + Asset misappropriation (high #, low \$)
 - + Financial Statement Fraud (low #, high \$)
 - + Corruption (moderate # and \$)

FRAUD & INTERNAL AUDIT

The auditor mindset towards fraud differs from the other “common” audits; the mindset should be investigative and anomaly-oriented (generally auditors are trained to address the majority risk).

- ✘ Fraud risk impact and residual risk is difficult to measure.

Fraudsters are not who you may think...

- ✘ The most common fraudster profile may contradict your intuition... a well-educated, middle-aged male, with no criminal history.
- ✘ 10% of people will always commit fraud, 10% of people will never commit fraud and 80% of people given the opportunity will commit fraud.
- ✘ Technical expertise is needed in terms of assessing fraud risk, investigation techniques, gathering and maintaining evidence, etc.
- ✘ Consult with internal or external experts if you think your task may be greater than your means.

INTERNAL AUDIT'S ROLE

INTERNAL AUDIT PROFESSIONAL STANDARDS

IIA Standard 1220: Due Professional Care

- ✘ 1220.A1–“Internal auditors must exercise due professional care by considering the: ...Probability of significant errors, fraud, or noncompliance.

IIA Standard 2060: Reporting to Senior Management and the Board

- ✘ “The chief audit executive (CAE) must report periodically to senior management and the board on the internal audit activity’s purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

INTERNAL AUDIT PROFESSIONAL STANDARDS

IIA Standard 2120:Risk Management

- ✘ 2120.A2–“The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.”

IIA Standard 2210:Engagement Objectives

- ✘ 2210.A2–“Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.”

IIA Standard 1200:Proficiency and Due Professional Care

- ✘ 1210.A2–“Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud”.

FRAUD & INTERNAL AUDIT

- ✘ Internal Audit (IA) supports management by determining whether the organization has adequate internal controls and promotes an adequate control environment.
- ✘ Since IA is a centralized, independent, and objective function, it is in a prime position to address fraud risk management programs, and to affect change.
- ✘ Different organizational structures and IA charters affect IA's role and ability to achieve that role.

FRAUD INVESTIGATION

FRAUD INVESTIGATIONS

Internal Audits Role

- ✘ Help management to identify critical indicators of fraud schemes
- ✘ Evaluate gaps in internal controls during the progression of fraud reviews/investigations
- ✘ Conduct ad-hoc forensic accounting investigations
- ✘ Support the Chief Audit Executive to ensure appropriate communication about fraud issues addressed by IA to the Board, the Audit Committee and others.

Digital Forensic Investigation

DIGITAL FORENSIC INVESTIGATION

Definition: establishing facts based on digital evidence

Typically refers to investigations of potential or known crime (including fraud), though broadly speaking many of the same concepts apply to any audit.

For today's purposes, the most practical scope of discussion is occupational fraud -intentional misuse of financially related matters of employment for personal gain.

- + Differs from other crimes outside the work environment (ex. “romance scams”) or that do not result in gain (ex. denial of service) or are not financially related (ex. stealing a password to “spy”).

DIGITAL FORENSICS & INTERNAL AUDIT

While roles and responsibilities vary greatly amongst entities, the overlap between Digital Forensics and Internal Audit is generally:

- + Evidence procedures related to fraud investigations
- + Identity Theft (Information Security)

Several factors challenge Internal Audit's role related to digital forensics:

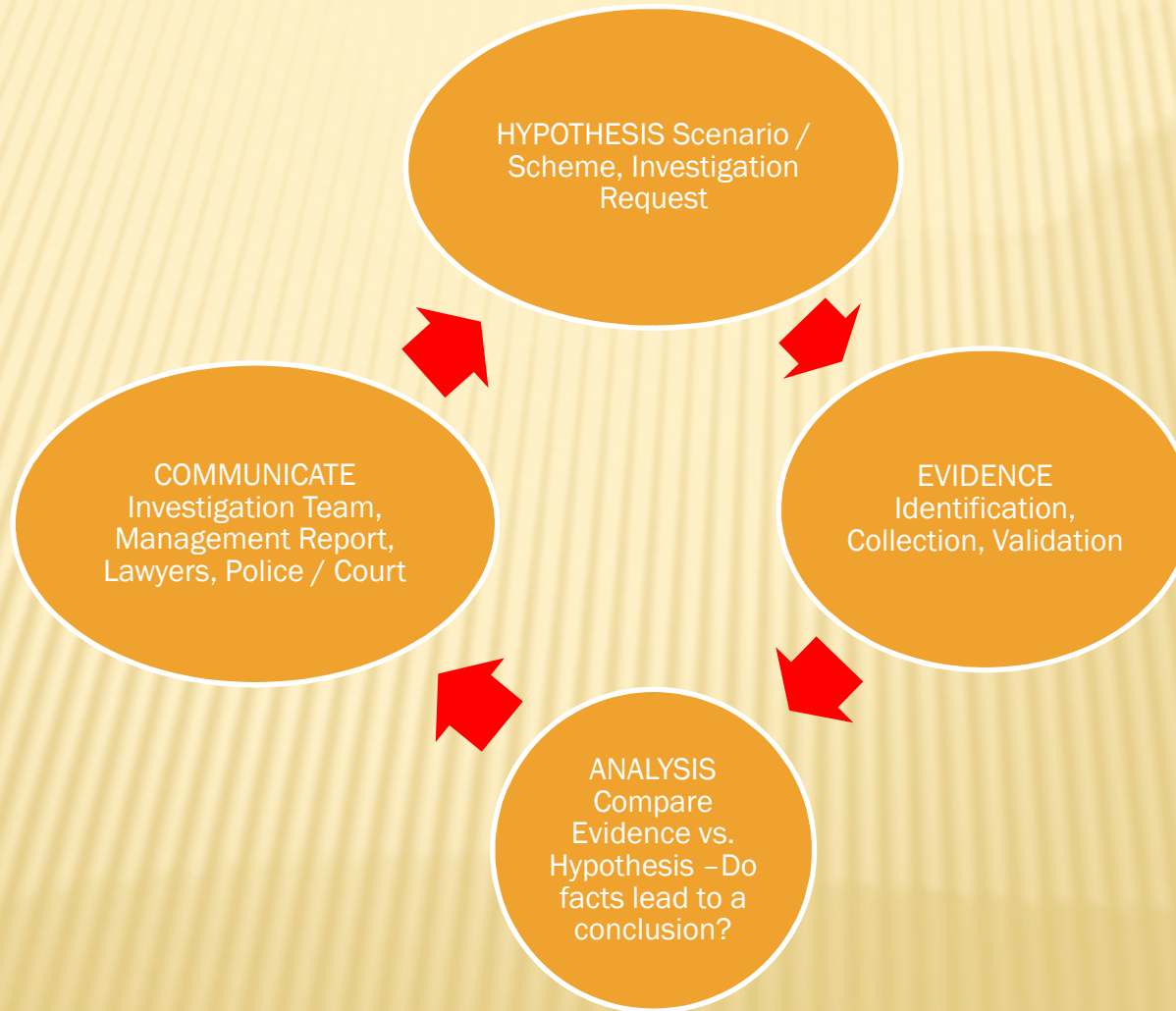
- + Trend from street to computer to online to "mobile" crime
- + Lack of clear responsibilities related to fraud and forensics
- + Senior Management is usually not well-informed on these risks

Internal Auditors should be educated on fraud-related matters:

- + 70% of computer-related malicious acts originate within (Gartner 2005)
- + 30 -60% of accounts no longer valid in large corporations (IDC)
- + "Big Data" & Management's expectations of Internal Audit

Forensic knowledge, tools, and processes should align with entity's risk.

INVESTIGATION PROCESS



DIGITAL FORENSIC INVESTIGATION TECHNIQUES-INVESTIGATION PROCESS

- ✘ The investigative process is iterative.
- ✘ Digital forensic techniques can assist in each phase.
- ✘ A successful investigation depends on evidence that clearly links from hypothesis to communicated conclusion.

HYPOTHESIS & EVIDENCE IDENTIFICATION

Evidence to be collected and associated techniques depend on how well the hypothesis is initially formed.

Targeting: Known issue & source

- + “Bull's-eye” approach emphasizing facts, evidence preservation, and clear results
- + Consider the cost / benefit

Sourcing: Known issue and unknown source

- + Brainstorm and profile considering facts, schemes, flags, and controls
- + Follow the “cash” and audit trails

Exploring: Determining whether any issue exists Analyze risks top-down and bottom-up, be adventurous and discrete

- ✗ Use CAATs to assess risks across populations

If litigation is a possibility, start documenting evidence chain and custody.
Consult with internal & external experts if your task is greater than your means.

EVIDENCE COLLECTION -HARDWARE

Acquiring data from hardware may require different methods depending on data state and the many possible storage forms.

- + Computer Media: drives, RAM, CDs, DVDs, flash drives
- + Mobile devices: phones, PDAs, iPods, GPS
- + Network Infrastructure: printers, servers, O/S, AD, databases, and logs
- + “Cloud”: Apple iCloud & MobileMe, Amazon S3, Google Cloud Storage

Analyze the state of hardware and data before interacting, and never power down hardware before collecting temporarily stored data.

- + Ideally hardware should be collected “in-state” and transported to secured, “pristine” environment for analysis.

Acquired hardware requires validation for completeness and accuracy similar to data validation.

EVIDENCE COLLECTION -DATA

- ✘ Create a visual diagram to identify, track, and communicate data analysis
- ✘ Be sure the source is authoritative / appropriate.
- ✘ Validate any data collected or transferred for completeness and accuracy.
- ✘ Metadata can serve as audit trail, though may need to be validated / corroborated.
- ✘ Deleted data predominantly is not really deleted, though specialized tools may be necessary.

EVIDENCE COLLECTION – BEYOND TECHNOLOGY

- ✘ Digital evidence is only one piece of a bigger puzzle, and evidence in total must corroborate.
 - + Never forget about the human element. People commit fraud using technology, not technology using people.
- ✘ Interviewing, body language, and writing (handwriting, emails, letters, etc.) analysis are their own disciplines for a reason. Expertise should be analyzed and sought out before approaching these topics.
- ✘ “Bullseye” –make every effort not to approach the suspected fraudster until sufficient evidence proves the assumption (know when to hold ‘em).

ANALYSIS -BASICS

Basic analysis techniques

- + Understand the data context (do your homework)...
 - × “Aggregate” –financials, # of employees / locations, hard drive size, # of files / records, etc.
 - × Statistical analysis –stratification, classification
- + Look for anomalies... mining, regression analysis, gaps, duplicates, Benford's, time period comparisons, unusual transaction attributes, etc.
- + Consider lookups / cross-references (especially for shell schemes)
- + Carefully consider whether population or sampling analysis is appropriate
- × Continuously asses how analysis relates to known facts, profile, etc.
- × Conduct analysis with thought of how results may be communicated.
- × Analysis should be recorded with the same rigor as evidence collection.

TECHNIQUES ANALYSIS INTERMEDIATE

Designing and executing analysis from the view of the hypothesized fraud scheme / red flags can effectively identify and analyze data. As examples:

Asset Misappropriation Schemes

- ✘ Segregation of duties in bank statement receipt and reconciliation
- ✘ Rotating duties or mandating vacation for key employees
- ✘ Examining all types of transactions just under required review/approval level, and classifying them by employee, vendor, and/or customer
- ✘ Reconciling inventory and confirming receivables regularly

TECHNIQUES ANALYSIS INTERMEDIATE

Billing -Shell Vendor Schemes

- ✗ Sorting payments by vendor, amount, and invoice number for anomalies to investigate
- ✗ Examining charges in largest expense accounts
- ✗ Verifying service-only vendors' invoices
- ✗ Using CAATs to cross-reference employees' addresses with vendors' addresses

Payroll -Ghost Employee Schemes

- ✗ Reconcile employees / SSNs in payroll file with those in human resource (HR) database.
- ✗ Rotate duties of handling printed checks or require vacation timed with payroll
- ✗ Data mining payroll data for post office box , physical address matches that of another employee (i.e., a “duplicate”), direct deposit account number that matches that of another employee, missing phone number or a phone number that matches either another employee or a work phone, compare dates of paychecks compared to termination dates, employees who have no deductions from paychecks

ANALYSIS ADVANCED

- ✖ Establish the fraud scenarios for ongoing/continuous monitoring
 - + Build and document understanding around related systems and data
 - + Ensure adequate understanding of underlying business, processes and controls
- ✖ Document flow and mapping of system architecture, applications, interfaces and data structures
- ✖ Build inventory of procedures given scenarios and systems understanding
 - + Tools like ACL can retain procedures through logs or scripts
- ✖ Integrate results by communicating to related Internal Audit and other risk management functions

COMMUNICATE

- ✘ Evidence has to corroborate each other (fit with the profile, scheme, initial facts, etc.) or be explained as to why it does not corroborate.
- ✘ Differentiate facts and opinions, and be transparent with any assumptions.
- ✘ Demonstrate how evidence and analysis clearly lead to results.
- ✘ Play “devil’s advocate”... If the case goes to trial, anything can be questioned and possibly sway the outcome.

DATA ANALYSIS & SEARCH TOOLS

Wikipedia Listing of Tools: http://en.wikipedia.org/wiki/List_of_digital_forensics_tools

Investigation Processes

- ✘ EnCase-data acquisition, analysis / workflow, preservation, & reporting:
 - + <http://www.guidancesoftware.com/forensic.html>
- ✘ Symantec & Norton Ghost -disk imaging:
 - + <http://www.symantec.com/themes/theme.jsp?themeid=ghost>
- ✘ Paraben-Mobile Forensics:
 - + <http://www.paraben.com/>

Investigation and Data Analysis Platforms

- ✘ Sleuth Kit -system / file data acquisition and analysis tool with various O/S and data file interoperability and user-defined C language scripting
 - + <http://www.sleuthkit.org/index.php>
- ✘ Picalo-system / file analysis tool with various O/S and data file interoperability, open source (Python*) script community, no record size limit
 - + <http://www.picalo.org/>

DATA ANALYSIS & SEARCH TOOLS

Data Analysis

- ✖ ACL -<http://www.acl.com/products/>
 - + Desktop -"traditional" data analysis tool with various file interoperability, built-in analysis functions, and custom-language scripting / automation abilities
 - + Exchange -data feeds, functions with custom parameters, documentation acquisition and storage, Microsoft Office integration, and data exception identification and workflow
 - + Acerno-Excel Add-In for results analysis
- ✖ IDEA -<http://www.caseware.com/products/idea>: Data analysis tool with various file interoperability, built-in functions, and custom-language scripting / automation
- ✖ Active Data/ Active Audit-Excel Add-Ins for data analysis similar to IDEA and ACL
- ✖ Search Websites
 - + Craigslist / EBay search: <http://www.searchtempest.com/>
 - + Person or Company profiling: <http://www.zoominfo.com/>
 - + Address or Phone search: <http://www.zabasearch.com/>
 - + Social Media search: <http://www.kurrently.com/>
 - + Blog Search: <http://technorati.com/>

REFERENCES & RESOURCES

- ✖ ACFE 2012 Report To The Nation (RTTN) -<http://www.acfe.com/rtnn.aspx>
- ✖ PwC 2011 Global Economic Crime Survey (GECS) -
<http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml>.
- ✖ Internet Crime Complaint Center (IC3) 2011 Internet Crime Report -
<http://www.ic3.gov/media/2012/120511.aspx>
- ✖ PwC 2004 –The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks.
- ✖ Mitigating Business Risk –Example of Anti Fraud Framework from the Australian Standard on Fraud and Corruption Control, AS 8001-2003
- ✖ Grant Thornton –Managing fraud risk: The audit committee perspective
- ✖ Forensic Firms Forensic Strategic <http://www.forensicstrategic.com/>
- ✖ Forensic CPAs -<http://www.forensic-cpas.net/index.html>
- ✖ Financial Forensic & Valuation Group -
<http://www.ffvgroup.com/index.html>

Open Discussion

Questions

reubenborogitahi@gmail.com