BBVA

Fraud and Internal Audit: Current Views, Examples, and Resources

Institute of Internal Auditors,
Birmingham Chapter

September 2012

Contents

1. Fraud in Context
2. Fraud Basics
3. Corporate-Wide Anti-Fraud Framework
4. Internal Audit’s Role
5. Digital Forensic Investigation

References & Resources

Open Discussion / Q&A

1 Fraud in Context

1. 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*).

ACFE Report to the Nations

- Typical entity loses 5% of annual revenue to fraud.
- Global fraud loss estimated at more than $3.5 trillion.
  - U. S. loss estimated at more than $750B (5% of GDP)
- Loss median of $140k and 25% over $1M.
- Median of 18 months before detection.

Traditional View of Fraud Risk

Traditional views have resulted in a fragmented (not integrated / holistic) risk framework and reactive approach to fraud.

- Fraud risk and controls considered as separate, secondary objectives of internal audit and internal control
- Fraud not perceived to be an internal control failure
- Fraud training and awareness not really necessary
- Information and Communication disparaged
- Fraud risk monitoring not perceived as a positive cost-benefit allocation of resources

1. Fraud in Context

Progression of Fraud Related Legislation

- Foreign Corrupt Practices Act 1977 and amended in 1998 by the international Anti-Bribery Act.
  - The SEC investigated over 400 U.S companies that admitted to making illegal payments to government functionaries, e.g. Lockheed and Bananagate.

- What act does the following describe?
  - "…would require auditors to institute ***specific procedures aimed at finding fraud*** or illegalities, regardless of how significant or material to the company`s financial statements. Auditors also would be ***required to evaluate, in writing, the quality of the client company`s internal controls***."
  - Financial Fraud Detection and Disclosure Act of 1986

Progression of Fraud Related Legislation

- U.S Sarbanes-Oxley Act of 2002
  - SEC rules have implemented and expanded on the U.S Sarbanes-Oxley Act of 2002 including § 404 controls related to the prevention, identification and detection of fraud.
  - The Enron Scandal
- Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010
  - Responses to financial crisis of 2007 – 2010
  - CFPB – tracing back from the source…"the customer"…

Prosecution of Corporate Criminals

- From 2002 – 2007 the Corporate Fraud Task Force (CFTF) yielded results of over 1,236 total corporate fraud convictions, including:
  - 214 CEO's and Presidents
  - 53 Chief Financial Officers;
  - 23 Corporate Counsels or Attorneys; and
  - 129 Vice Presidents
- The CFTF was replaced in November of 2009 with the Financial Fraud Enforcement Task Force. By 2011:
  - 1,517 defendants charged, convicted or sentenced, resulting in $3.5B losses recouped.

Impact of Legislation

- Organizations liable for offence and failing to have controls in place
- Demanding anti-fraud programs with a focus on prevention and timely detection
- Increased management responsibility towards fraud risk
- Independent auditors required to evaluate sufficiency in fraud controls

1. Fraud in Context

Current View of Fraud Risk

Current view aims to manage fraud risk holistically and proactively.

- Fraud risk and controls considered an objective of internal control activities
- Fraud perceived to be potential internal control failures
- Fraud training and awareness necessary
- Information and Communication aggregated, concise, and timely
- Fraud risk monitoring perceived as positive cost / benefit (protects revenue and/or recoups losses)

2

Fraud Basics

Defining the basic fraud types

Differentiating fraud risk from other risks

Assessing fraud risks

2. Fraud in Context

Defining Basic Fraud Types

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

- –Differs from other crimes outside the work environment (ex. “romance scams”), that do not result in gain (ex. denial of service), or that are not financially related (ex. stealing another’s possession to “spy”).

ACFE Occupational Fraud Categories

- – Asset misappropriation (high #, low $)
- – Financial Statement Fraud (low #, high $)
- – Corruption (moderate # and $)

Differentiating Fraud Risk

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…

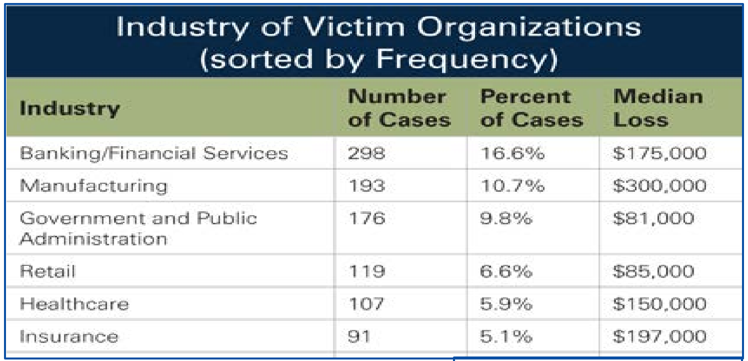
- The **most common fraudster profile may contradict your intuition**… a well-educated, middle-aged male, with no criminal history.
- 10% of people will always commit fraud, 10% of people will never commit fraud and **80% of people given the opportunity will commit fraud**.

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.

Assessing Fraud Risk Top-Down

All industries are not “created equal”…



Industry of Victim Organizations (sorted by Frequency)

Industry	Number of Cases	Percent of Cases	Median Loss
Banking/Financial Services	298	16.6%	$175,000
Manufacturing	193	10.7%	$300,000
Government and Public Administration	176	9.8%	$81,000
Retail	119	6.6%	$85,000
Healthcare	107	5.9%	$150,000
Insurance	91	5.1%	$197,000

Source: ACFE RTTN

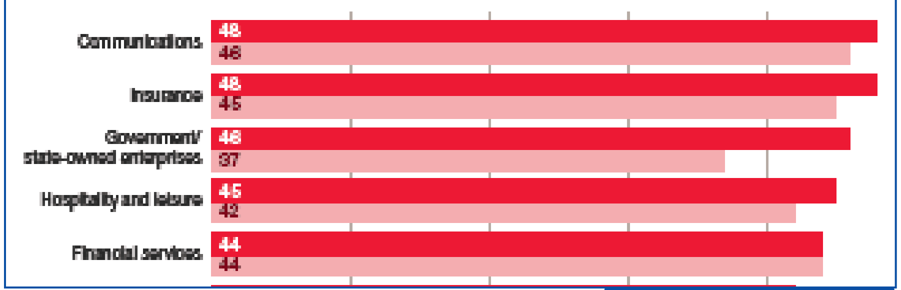
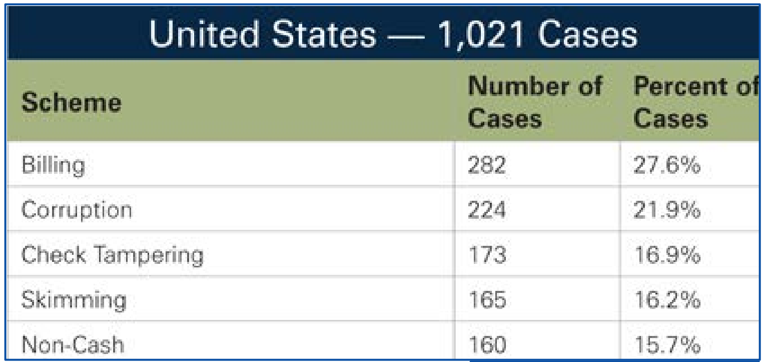


Figure 9: Fraud reported by Industries

Source: PwC GECS

Generally speaking, risks are in cash and other liquid assets…



United States — 1,021 Cases

Scheme	Number of Cases	Percent of Cases
Billing	282	27.6%
Corruption	224	21.9%
Check Tampering	173	16.9%
Skimming	165	16.2%
Non-Cash	160	15.7%

Source: ACFE RTTN

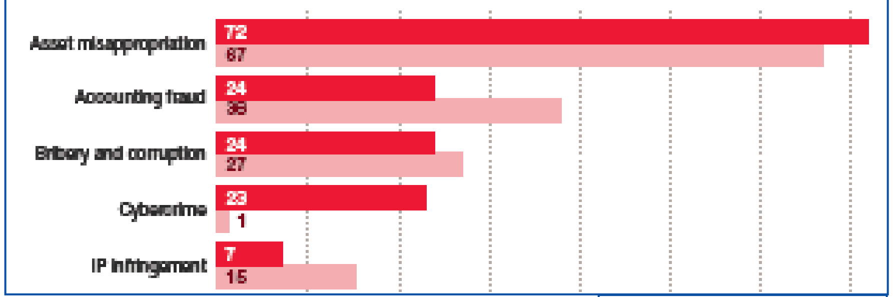
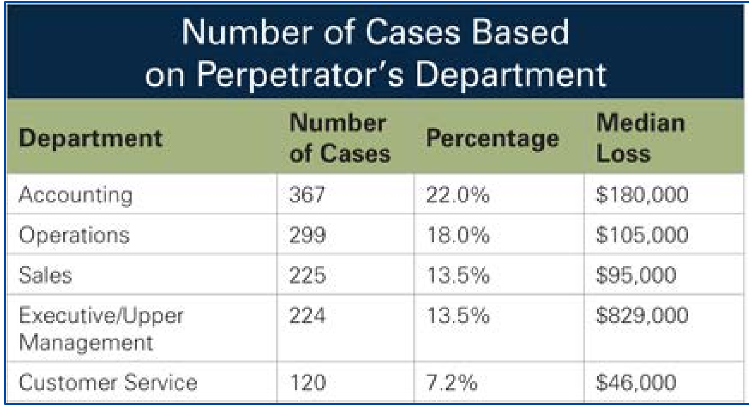


Figure 11: Types of economic crime

Source: PwC GECS

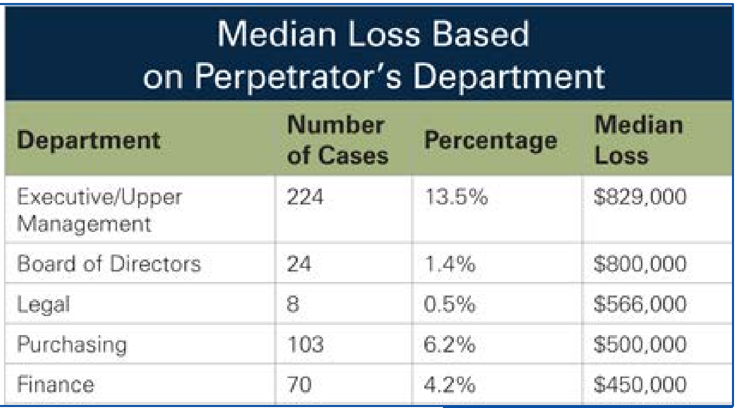
Assessing Fraud Risk Top-Down

Certain areas and position levels most commonly experience fraud



Number of Cases Based on Perpetrator's Department

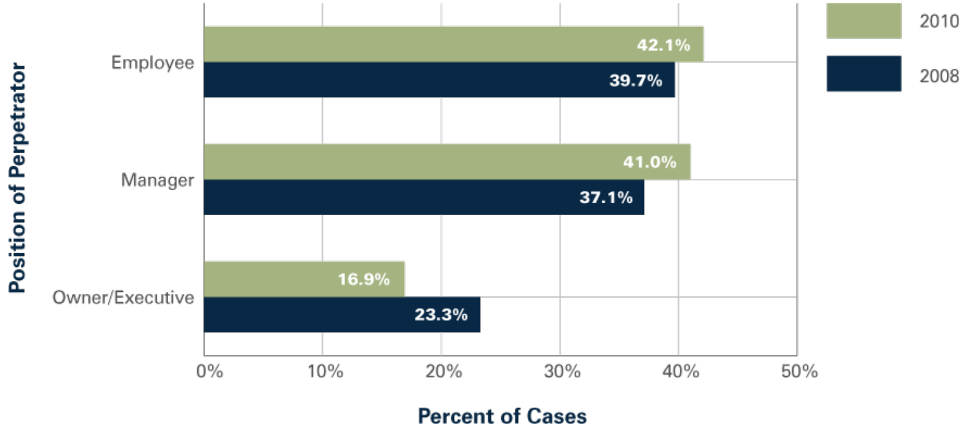
Department	Number of Cases	Percentage	Median Loss
Accounting	367	22.0%	$180,000
Operations	299	18.0%	$105,000
Sales	225	13.5%	$95,000
Executive/Upper Management	224	13.5%	$829,000
Customer Service	120	7.2%	$46,000



Median Loss Based on Perpetrator's Department

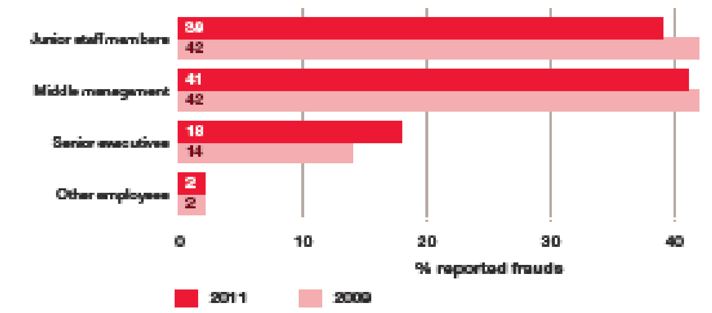
Department	Number of Cases	Percentage	Median Loss
Executive/Upper Management	224	13.5%	$829,000
Board of Directors	24	1.4%	$800,000
Legal	8	0.5%	$566,000
Purchasing	103	6.2%	$500,000
Finance	70	4.2%	$450,000

Source: ACFE RTTN



Source: ACFE RTTN

Figure 15: Profile of internal fraudsters



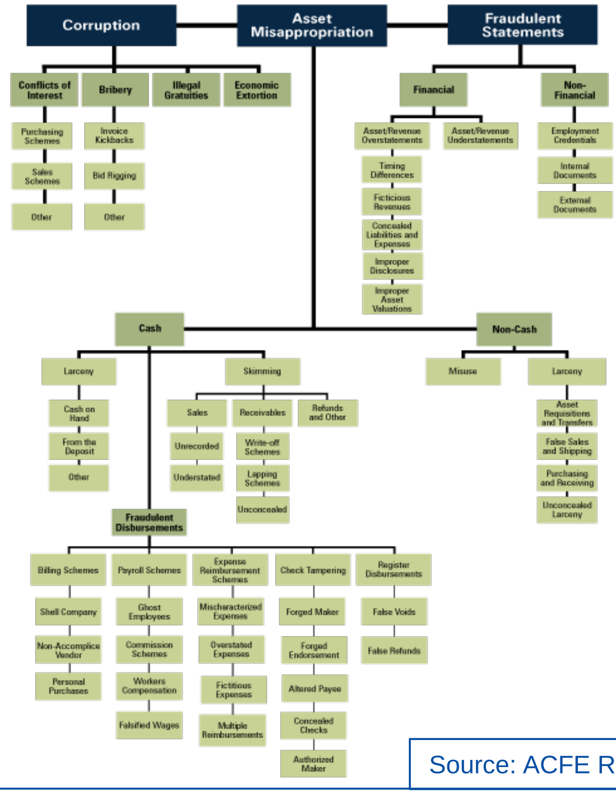
% respondents who reported that an internal employee was the main perpetrator of fraud

Source: PwC GECS

Assessing Fraud Risk Top-Down

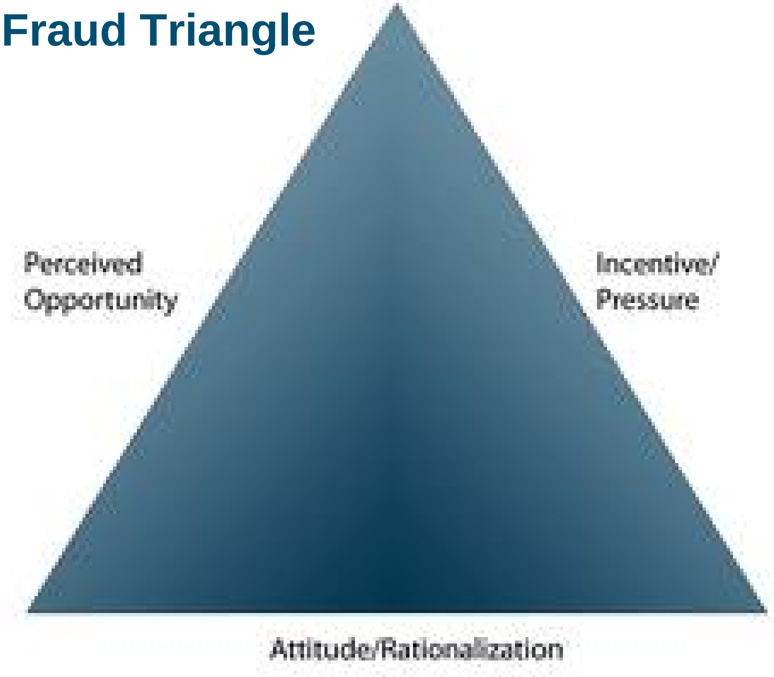
Based on overarching fraud risk, scheme/scenario-based risk assessment can be effective, using red flags associated with the scheme and the fraud triangle to further refine articulation of residual risk.

Fraud Tree and Schemes



Source: ACFE RTTN

Fraud Triangle

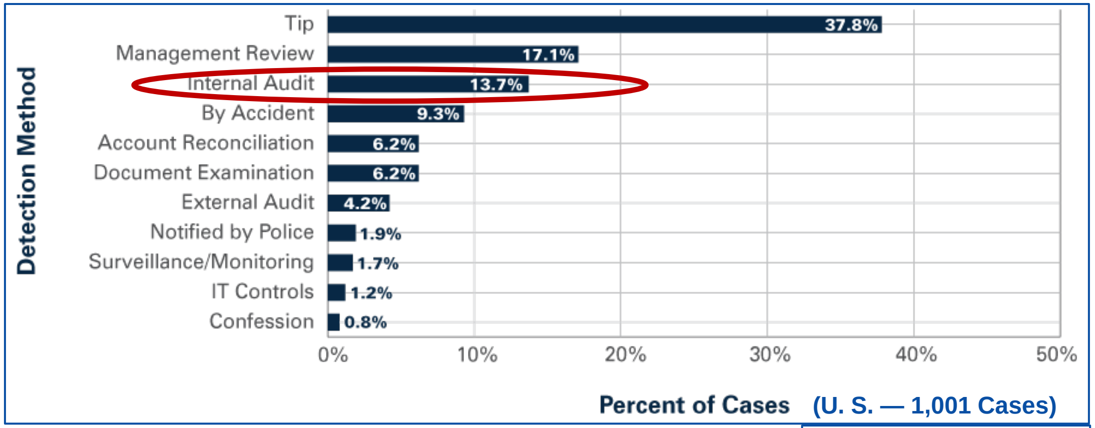


Source: ACFE RTTN

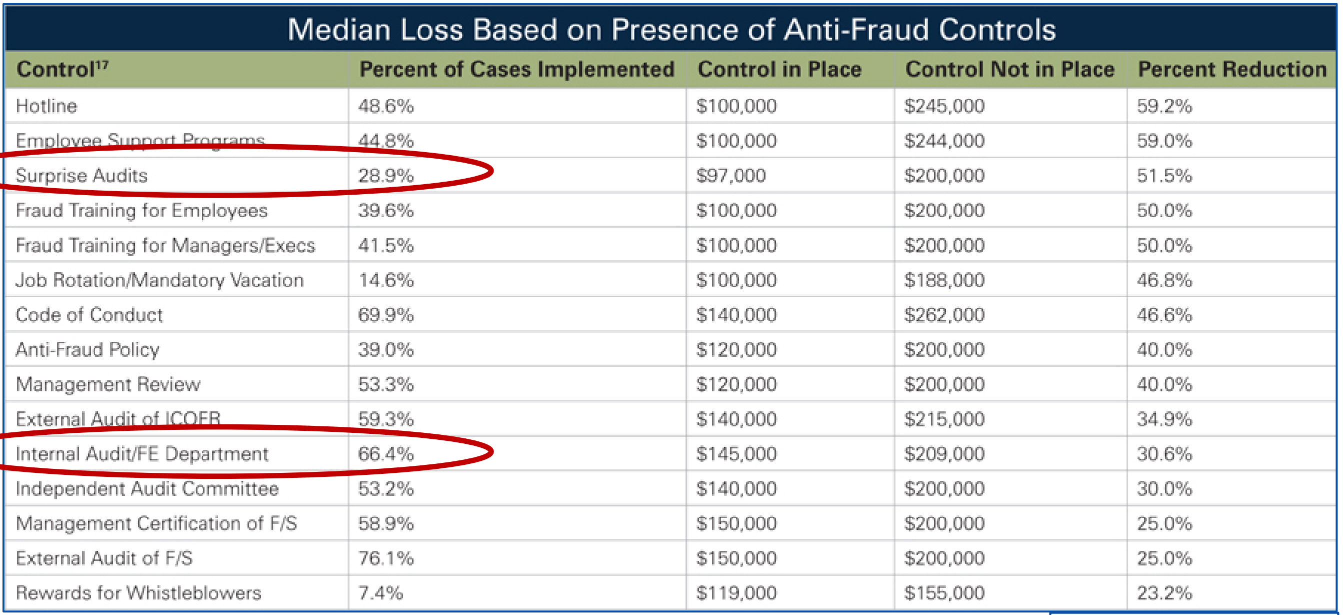
2. Fraud in Context

Assessing Fraud Risk Mitigation

Research consistently reflects the most common detection methods and effective anti-fraud controls.



Source: ACFE RTTN



Median Loss Based on Presence of Anti-Fraud Controls

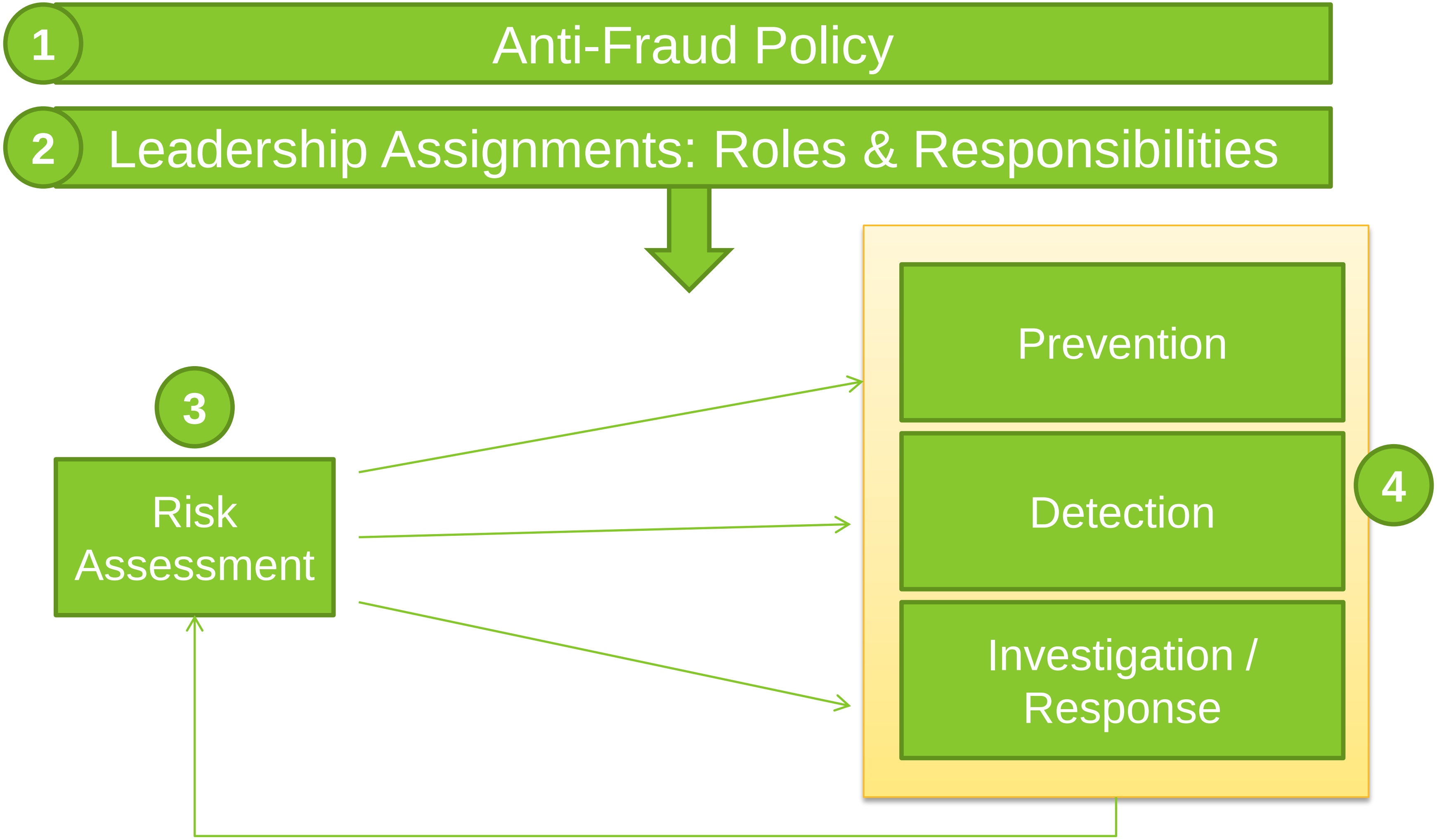
Control[17]	Percent of Cases Implemented	Control in Place	Control Not in Place	Percent Reduction
Hotline	48.6%	$100,000	$245,000	59.2%
Employee Support Programs	44.8%	$100,000	$244,000	59.0%
Surprise Audits	28.9%	$97,000	$200,000	51.5%
Fraud Training for Employees	39.6%	$100,000	$200,000	50.0%
Fraud Training for Managers/Execs	41.5%	$100,000	$200,000	50.0%
Job Rotation/Mandatory Vacation	14.6%	$100,000	$188,000	46.8%
Code of Conduct	69.9%	$140,000	$262,000	46.6%
Anti-Fraud Policy	39.0%	$120,000	$200,000	40.0%
Management Review	53.3%	$120,000	$200,000	40.0%
External Audit of ICOFR	59.3%	$140,000	$215,000	34.9%
Internal Audit/FE Department	66.4%	$145,000	$209,000	30.6%
Independent Audit Committee	53.2%	$140,000	$200,000	30.0%
Management Certification of F/S	58.9%	$150,000	$200,000	25.0%
External Audit of F/S	76.1%	$150,000	$200,000	25.0%
Rewards for Whistleblowers	7.4%	$119,000	$155,000	23.2%

Source: ACFE RTTN

3 Corporate-Wide Anti-Fraud Framework

3. Corporate-Wide Anti-Fraud Framework

Anti-Fraud Model



Anti-Fraud Policy

Starts with the Tone at the Top

Does your organization have an Anti-Fraud Policy approved by the board of directors?

The concepts incorporated in an Anti-Fraud Policy are developed to detect and prevent fraud and to implement effectively and homogeneously the policies and objectives set by management.

Convey the expectations of the board of directors and senior management regarding fraud risk and control.

Leadership, Assignments, Roles & Responsibilities

Typical organization responsibilities include:

- Tone at the Top – Executive Leadership
- Establish Internal Controls – Management/Accounting
- Code of Conduct - Legal
- Employee Assistance Program – Human Resources
- Hotline Administration – Various Resources
- Referral to Law Enforcement – Corporate Security

Who is responsible for the implementation of an Anti-Fraud Framework?

- Even though management is ultimately responsible …
- Everybody has a part to play in the prevention, detection and investigation of fraud.

Fraud Risk Assessment

- Risk assessment should be both periodic and continuous
- Assessment should include…
  - Consideration of the most likely fraud schemes / scenarios (based on external and internal factors)
  - Root cause analysis of fraud that has occurred and the evaluation of fraud risks
  - Analysis of the affectivity of prior measures
  - Prioritization and design of new measures
- Reviews of anti-fraud measures and controls should be considered in terms of coverage, frequency and results

3. Corporate-Wide Anti-Fraud Framework

Fraud Prevention & Mitigation

- Due Diligence carried out on all employees and third parties.
- Code of Conduct Agreement & Renewal
- Training & Communication
- Revision of critical controls in processes and operations
- Annual continuous leave for key employees
  - If a person leaves their position for e.g. 2 weeks will another employee that takes over their role likely identify a fraud given the controls in place?
- Conflict of Interest Policy

Fraud Detection

- Whistleblower Channels
  - Protection of employees reporting suspected fraud
  - External anonymous reporting
  - Investigation referral email address
- Internal Audit relationships in lines of business may facilitate “tips” / investigation requests
- Management Review
- Alerts
  - Running fixed routines on data to detect anomalies.

Fraud Detection - Investigation Considerations

- Internal Investigations
  - Audit Director Roundtable has a Taxonomy of investigations and corresponding roles
- External Investigative Resources
  - Corporate Security
  - Investigations
- Documentation of the results of the investigation
  - Index of exhibits
- Fidelity Guarantee

Fraud-Related Reporting

In the end … you want to give **assurance** to the Board that adequate controls are in place to detect and prevent fraud.

Consider…

- Recommended changes to Anti-Fraud Policy
- Quarterly reports
- Risk assessment results
- Material cases of fraud

3. Corporate-Wide Anti-Fraud Framework

Summary

4

Internal Audit's Role

4. Internal Audit's Role

Internal Audit Standards

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".

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."

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."

Role & Organizational Structure

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.

An Example… Internal Audit Fraud Unit at BBVA Compass

4. Internal Audit's Role

Internal Audit Fraud Risk Policy

- Identifies the CAE with the primary responsibility for dealing with among others, investigation when the involvement of Internal Audit is deemed necessary.

- **Establishment of a Specific Unit within Internal Audit to address Fraud Risk.**

- The policy applies to **any irregularity or suspicious activity involving**…Employees, Board of Directors, consultants, vendors and any other parties that have a relationship with the Organization.

- General Principles: **Purpose** is guided by …Company Charter, IA Policy, code of ethics…etc…**Authority** in determining Fraud Scope, performing work and communicating results with unrestricted access to Organization records **Independence, Objectivity & Continuous Education** …**Scope of Activities** Fraud Prevention and Investigation

4. Internal Audit's Role

Fraud Risk Assessment

A Fraud Risk Assessment (**FRA**) is a process aimed at proactively identifying and addressing an organization's vulnerabilities to both Internal and External Fraud. A FRA is a key element of anti-fraud programs including Annual Audit Planning.

A FRA assists auditors to comply with **professional standards**:

AICPA. Statement on Auditing Standards No. 99. and Nos.104-111

PCAOB. Auditing Standard No. 8-15

IIA. Practice Advisory 1210.A2-1. And Proposed Standard 2120.A2

Particular goals are:

- Highlight the **Fraud Focus Points (High)** where the performance of an audit may need to be adjusted within the 2012 annual plan,
- Provide assurances that the risk of Fraud is being effectively **incorporated** within the Internal Audit Risk Assessment, and,
- Minimize the **risk of overlooking** fraud during Internal Audit planning stages

FRA Methodology – Scenarios

Define a list of fraud scheme scenarios based on experience of the IA Fraud Team together with internal & external data.

Ranking^	Possible Fraud	Group	Origen
1	**Check Fraud**	Misappropriation	External
2	**Deposit Fraud**	Misappropriation	Int/Ext
3	**Debit/ATM Card Fraud**	Misappropriation	External
4	**Inappropriate Banking/Commercial Practices**	Others & Reputational	Internal
5	**Other Loans Fraud Schemes**	Misappropriation	Internal
6	**Credit Card Fraud**	Misappropriation	External
7	**Money Laundering**	Others & Reputational	Int/Ext
8	**Cashier's Check Fraud**	Misappropriation	Internal
9	**Mortgage Loan Fraud**	Misappropriation	Int/Ext
10	**Wire Transfer Fraud**	Electronic	Int/Ext
11	**ACH Fraud**	Electronic	External
12	**CD/Savings Embezzlement**	Misappropriation	Int/Ext

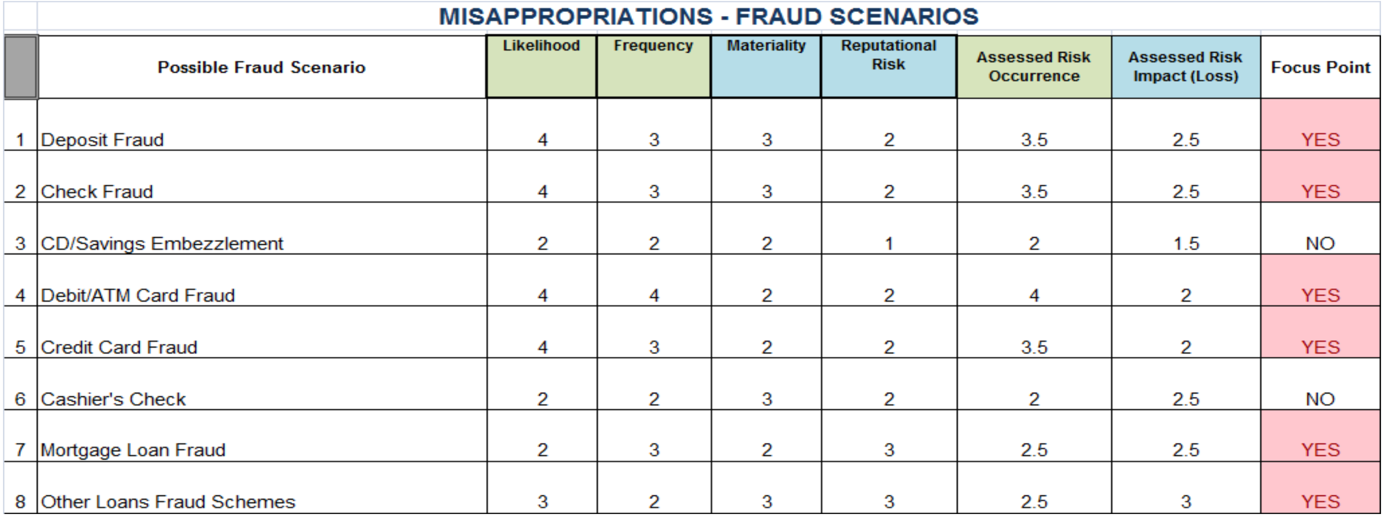
FRA Methodology – Risk Model

A risk model maps and assess the Organization’s vulnerability to identified fraud scenarios, with a scale is defined to evaluate each of the factors as follows:

Factor	4	1
Likelihood	High Probability	Rarely Occurring
Frequency	Widespread	Only selected areas
Materiality	High dollar Amount	Low dollar amount
Reputational Risk	Significant loss of reputation or loss of public trust	Minimal loss of reputation or loss of public trust

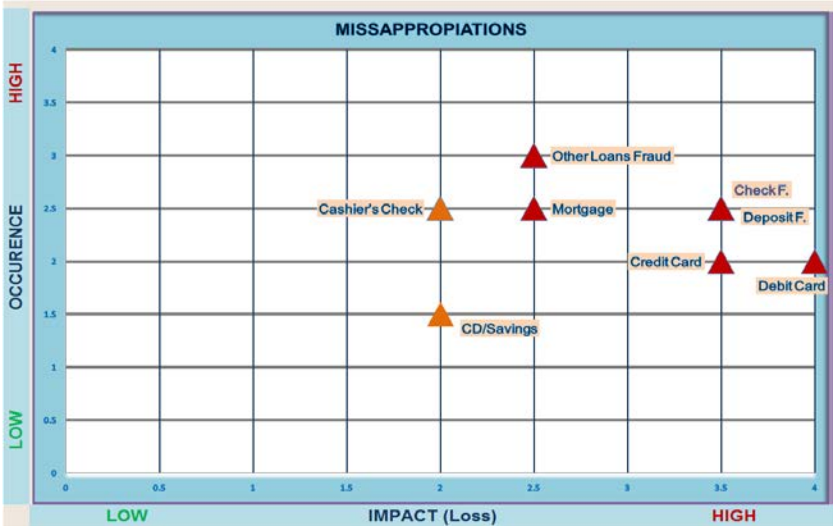
4. Internal Audit’s Role

FRA Methodology – Results & Focus Points



MISAPPROPRIATIONS - FRAUD SCENARIOS

	Possible Fraud Scenario	Likelihood	Frequency	Materiality	Reputational Risk	Assessed Risk Occurrence	Assessed Risk Impact (Loss)	Focus Point
1	Deposit Fraud	4	3	3	2	3.5	2.5	YES
2	Check Fraud	4	3	3	2	3.5	2.5	YES
3	CD/Savings Embezzlement	2	2	2	1	2	1.5	NO
4	Debit/ATM Card Fraud	4	4	2	2	4	2	YES
5	Credit Card Fraud	4	3	2	2	3.5	2	YES
6	Cashier's Check	2	2	3	2	2	2.5	NO
7	Mortgage Loan Fraud	2	3	2	3	2.5	2.5	YES
8	Other Loans Fraud Schemes	3	2	3	3	2.5	3	YES



Focus Points

▲ Low	▲ High
▲ Medium	▲ Critical

4. Internal Audit’s Role

Assisting in Annual Planned Audits

A Fraud Unit within Internal Audit can specifically design anti-fraud tests and integrate fraud audit techniques into the IA process of **Ongoing Reviews**.

Include Investigation results and analysis in the scope and planning of an audit.

Include processes for addressing fraud in the audit universe and plan as an unavoidable element of the annual risk assessment process.

Fraud Testing

- Design and carry out fraud prevention and detection programs for areas of the organization with functions related to Risk, Compliance, and other LOB’s

- Help management to identify and assess risks that may result in a material misstatement due to fraud, through monitoring of financial statements.

- Carry out detective fraud investigations through suggested automatic examination methods, CAAT’s, as well as data mining software.

4. Internal Audit’s Role

Fraud Investigation

- 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.

Internal Fraud Audit Development Considerations

Foster Sponsorship & Support

- Executive Sponsorship - Have clear visibility with the Board/Audit Committee
- Exposure and Networking with other areas of the organization
- Respect from Legal, Human Resources, Investigations, LOB’s (large source of cases)
- There must be clearly defined roles & responsibilities. Present those to the different areas involved.

Acquire & Develop Expertise

- Look for specific skill sets. CPA, CFE, CIA, Data Analytics and law enforcement experience (especially good for interviewing techniques)
- Legal elements of a fraud investigation
- Data Analytics - ACL, IDEA…
- Interviewing techniques
- Digital forensics

Build a Reputation

- Give out a good quality product, who are your customers?
  - Internal Audit Report
  - Report for the Insurance Carriers
  - Legal Exhibits
- Think outside the box: Send out questionnaires to identify custom and practice versus policy and procedure

Demonstrate Value

- Promote Results
- Calculate recoveries
- Audit Committee Assurance
- Consistent approach to managing Fraud Risk

Anticipate & Overcome Obstacles

- Not easy to access Databases
- Improperly Staffed
- No budget
- Improperly positioned within the organization
- Lack of policies and procedures

5 Digital Forensic Investigation

5. Digital Forensic Investigation - Context

Context of Digital Forensics

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").

5. Digital Forensic Investigation - Context

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.

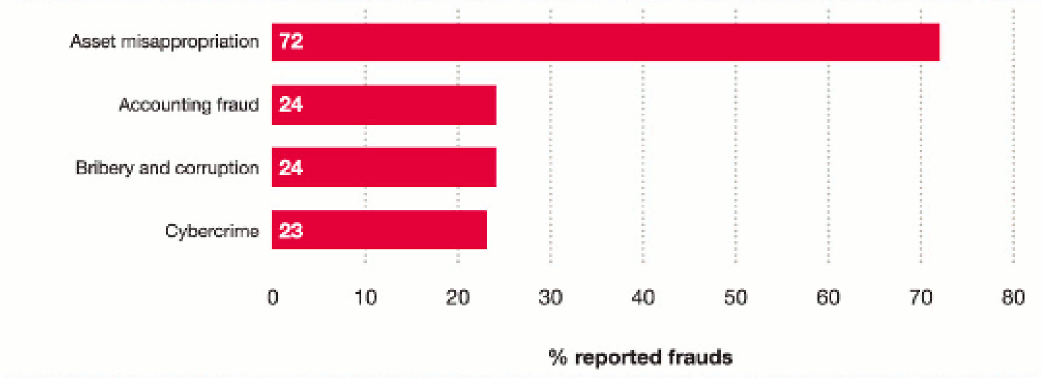
5. Digital Forensic Investigation - Context

Fraud Overview – Economic Crime

PwC Global Economic Crime Survey

- Cybercrime (“digital fraud”) #4 in most common reported economic crimes
  - 48% experiencing crime in last year perceive rising cybercrime risks
  - 40% say biggest fear is reputational damage from cybercrime
  - 40% don’t have capability to detect and prevent cybercrime
- 56% said the most serious fraud was an ‘inside job’
- Senior Execs. made up almost 50% who didn’t know if a fraud occurred

Figure 1: Top four types of economic crime reported



% respondents who experienced economic crime in the last 12 months

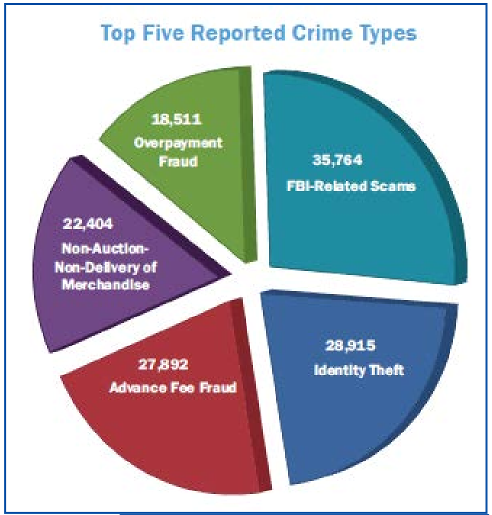
Source: Ref. 2 – PwC GECS

5. Digital Forensic Investigation - Context

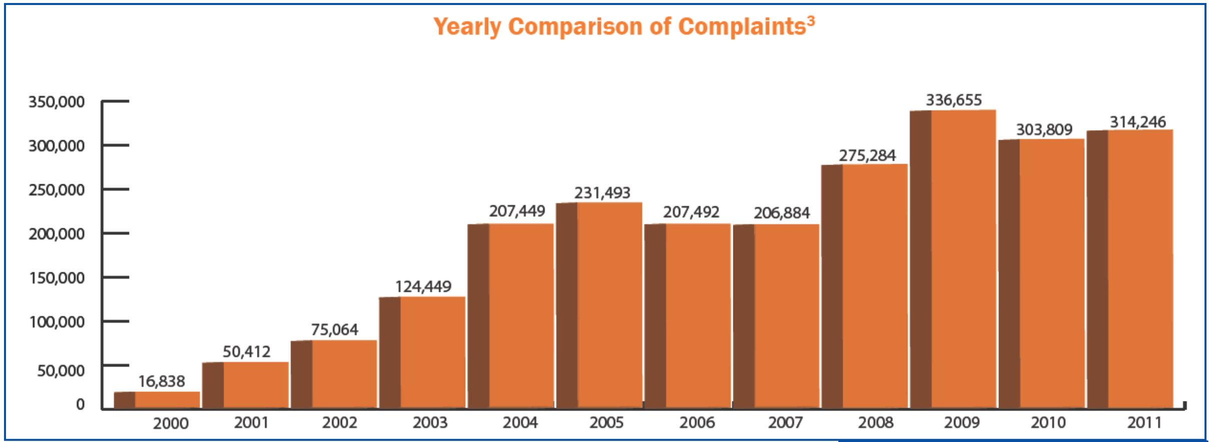
Fraud Overview – Internet Crime

IC3 – 2011 Statistics

- Total complaints received / reporting loss: 314k / 116k
- Total estimated loss: $485M
- Median dollar loss for those reporting a loss: $636
- Average dollar loss for those reporting loss: $4,187



Source: Ref. 3 – IC3 ICR



Source: Ref. 3 – IC3 ICR

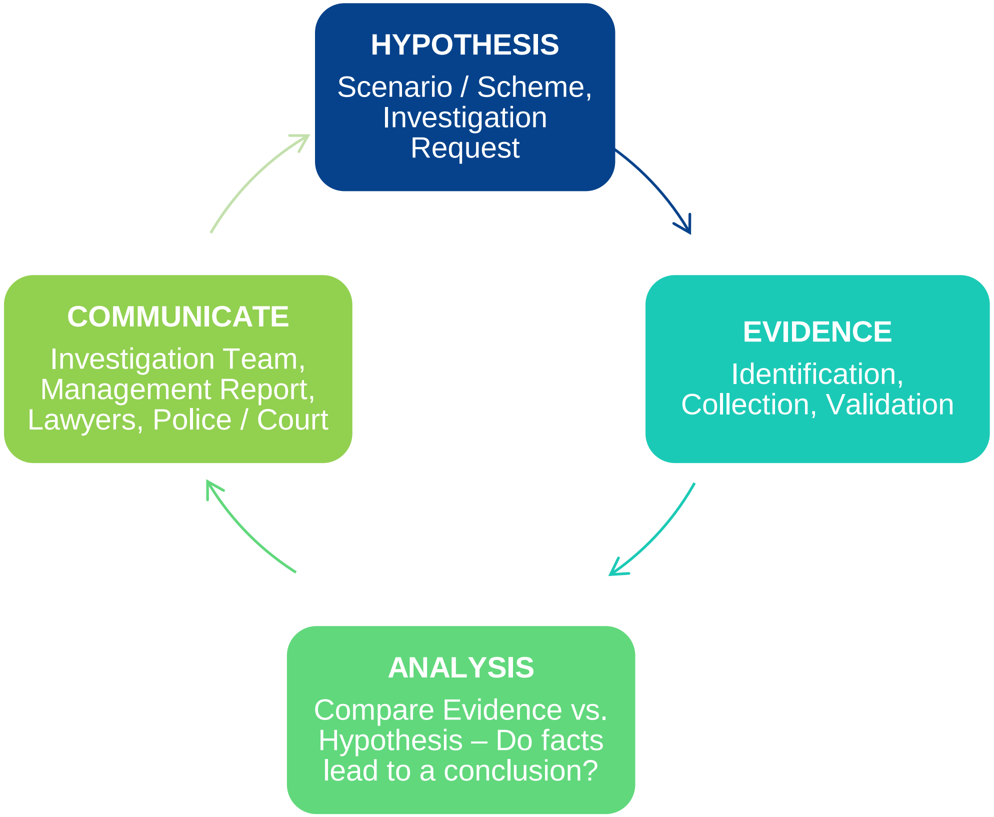
5. Digital Forensic Investigation - Techniques

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
Scenario / Scheme, Investigation Request

EVIDENCE
Identification, Collection, Validation

ANALYSIS
Compare Evidence vs. Hypothesis – Do facts lead to a conclusion?

COMMUNICATE
Investigation Team, Management Report, Lawyers, Police / Court

5. Digital Forensic Investigation - Techniques

Hypothesis & Evidence Identification

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

- **Targeting:** Known issue & source
  - “Bullseye” 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.

5. Digital Forensic Investigation - Techniques

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 there 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).

5. Digital Forensic Investigation - Techniques

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.

5. Digital Forensic Investigation - 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

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

5. Digital Forensic Investigation - Techniques

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

5. Digital Forensic Investigation - Techniques

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.

5. Digital Forensic Investigation - Tools

Forensic Investigation 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.htm
- 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/

5. Digital Forensic Investigation - Tools

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
- ActiveData / ActiveAudit - Excel Add-Ins for data analysis similar to IDEA and ACL

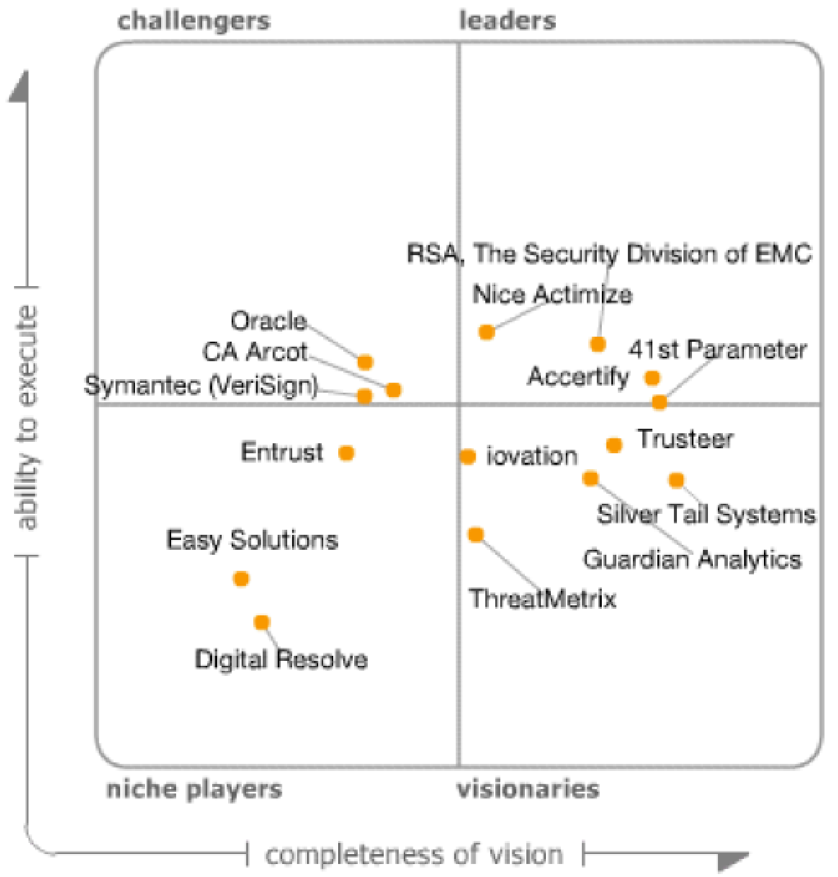
Search Websites

- 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/
- Whois search: www.networksolutions.com

5. Digital Forensic Investigation - Tools

Cyber Crime & Identity Theft Tools

Figure 1. Magic Quadrant for Web Fraud Detection



As of April 2011

References & Resources

- ACFE 2012 Report To The Nation (RTTN) - http://www.acfe.com/rttn.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
- Local 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

Peter.Hickey@bbvacompass.com

Aaron.Singleton@bbvacompass.com

BBVA

Fraud and Internal Audit: Current Views, Examples, and Resources

Institute of Internal Auditors,
Birmingham Chapter

September 2012