

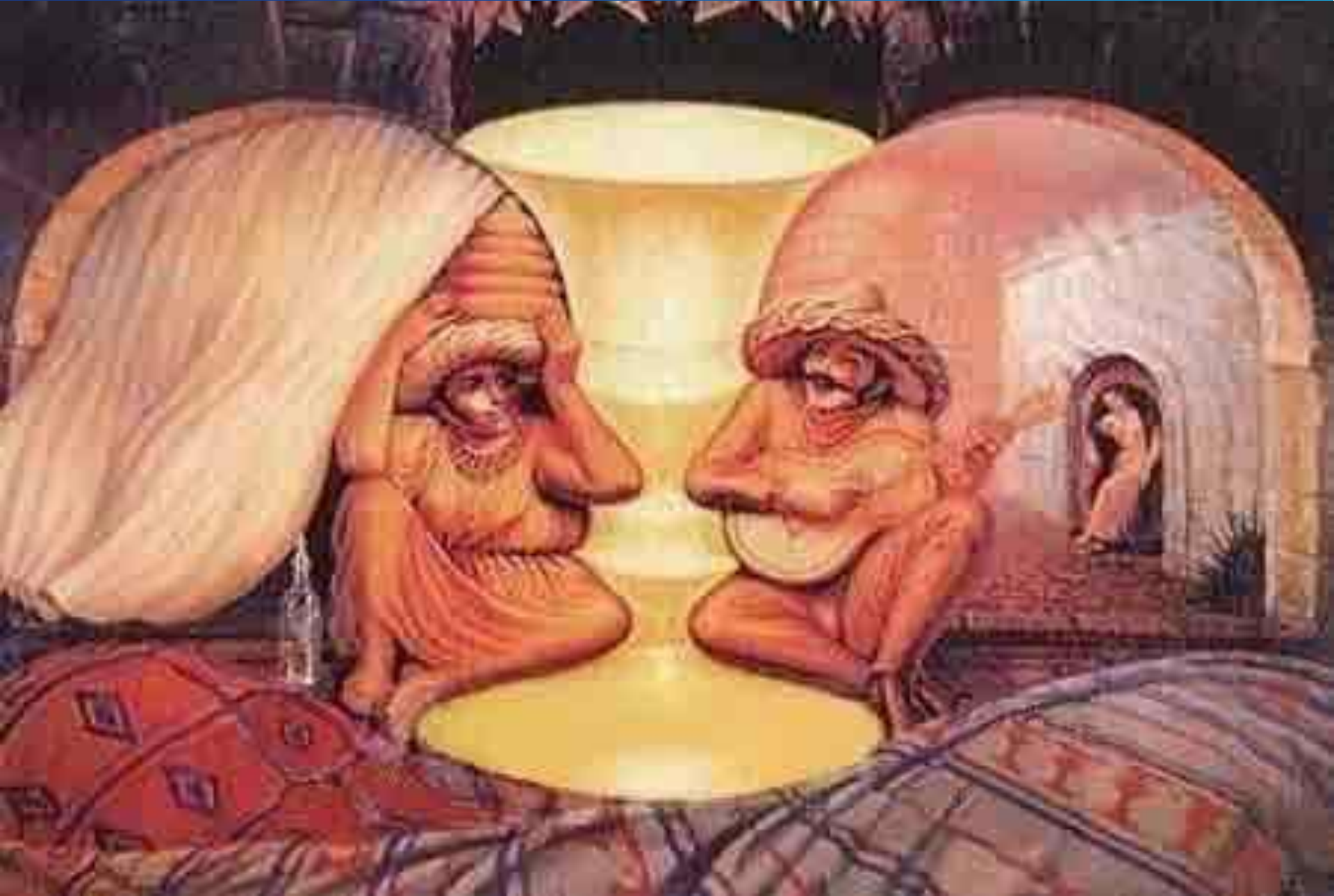


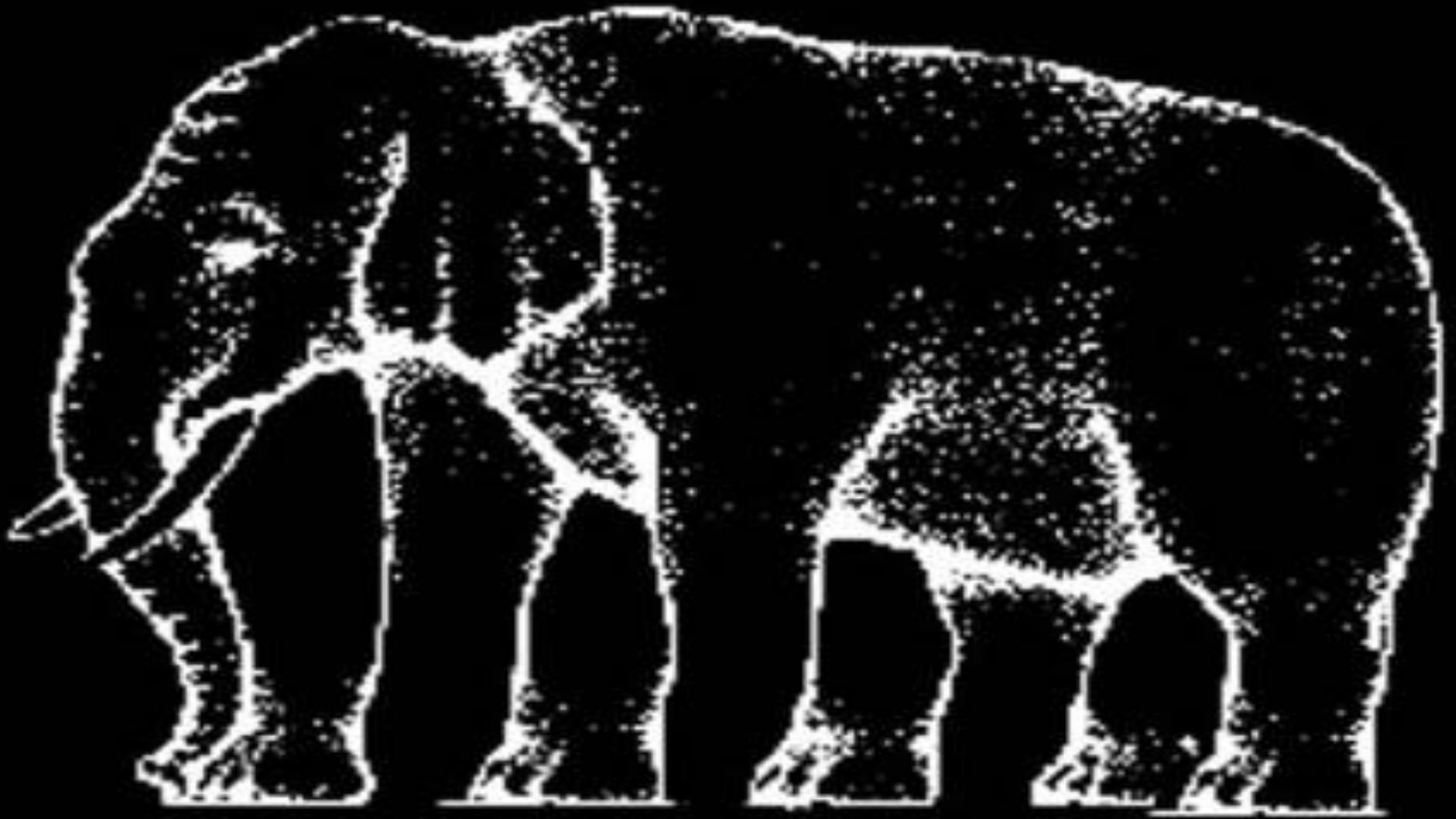
*cutting through complexity*

# Fraud & Computer Forensics

**Chris Budge, MPhil, CFE**  
**KPMG Forensic Services**

**15 November 2013**





How many legs does this elephant have?

The background consists of several overlapping, semi-transparent geometric shapes in various shades of blue (light, medium, and dark) and white. The shapes are primarily parallelograms and trapezoids, creating a dynamic, layered effect. The word "Fraud" is centered within a large, dark blue parallelogram on the right side of the image.

Fraud

# What is fraud?

## Definition

- Fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception or other unfair means.

## Types of fraud

- Misrepresentation or concealment of material facts
- Bribery
- Conflicts of interest
- Theft
- Breach of fiduciary duty

## Fraudulent financial reporting

- Improper revenue recognition
- Overstatement of assets
- Understatement of liabilities
- Omission of disclosures
- Deliberate misapplication of accounting standards
- Treasury and investment related fraud

## Asset misappropriation

- Theft of cash
- False payment requests
- Cheque fraud
- Billing schemes
- Theft of inventory/assets
- Procurement fraud
- Payroll fraud

## Corruption

- Kickbacks
- Personal interests
- Insider trading
- Bribery
- Extortion/blackmail
- Graft

# Drivers of Fraud – The Fraud Triangle

## Incentive/Pressure

- Credit crunch
- Debts
- Addictions
- Revenge



## Opportunity

- Poor controls
- Abuse of Authority
- Poor segregation of duties
- Exploiting errors

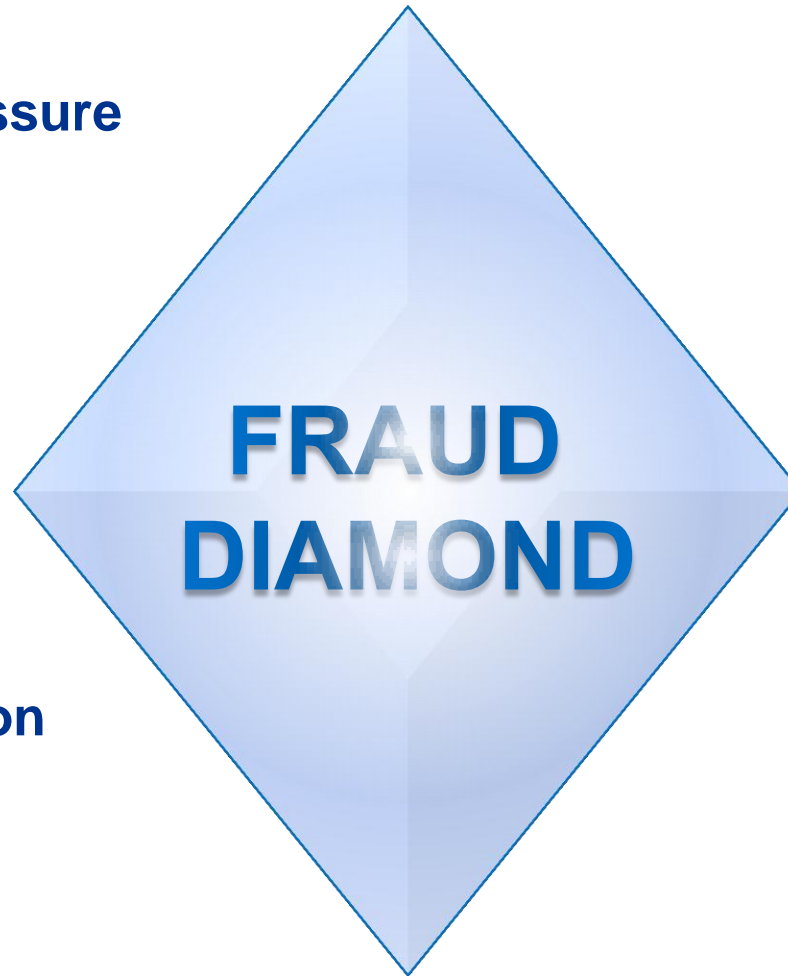
## Rationalisation

- “I need the money”
- “Who cares”
- “I’ll never get caught”

# Fraud Diamond – The Fourth Element

**Incentive/Pressure**

**Opportunity**



**Rationalisation**

**Capability**



- 10% Honest all of the time
- 80% Honesty varies depending upon opportunity and motivation
- 10% Dishonest whenever the opportunity presents itself

# KPMG analysis of global patterns of fraud

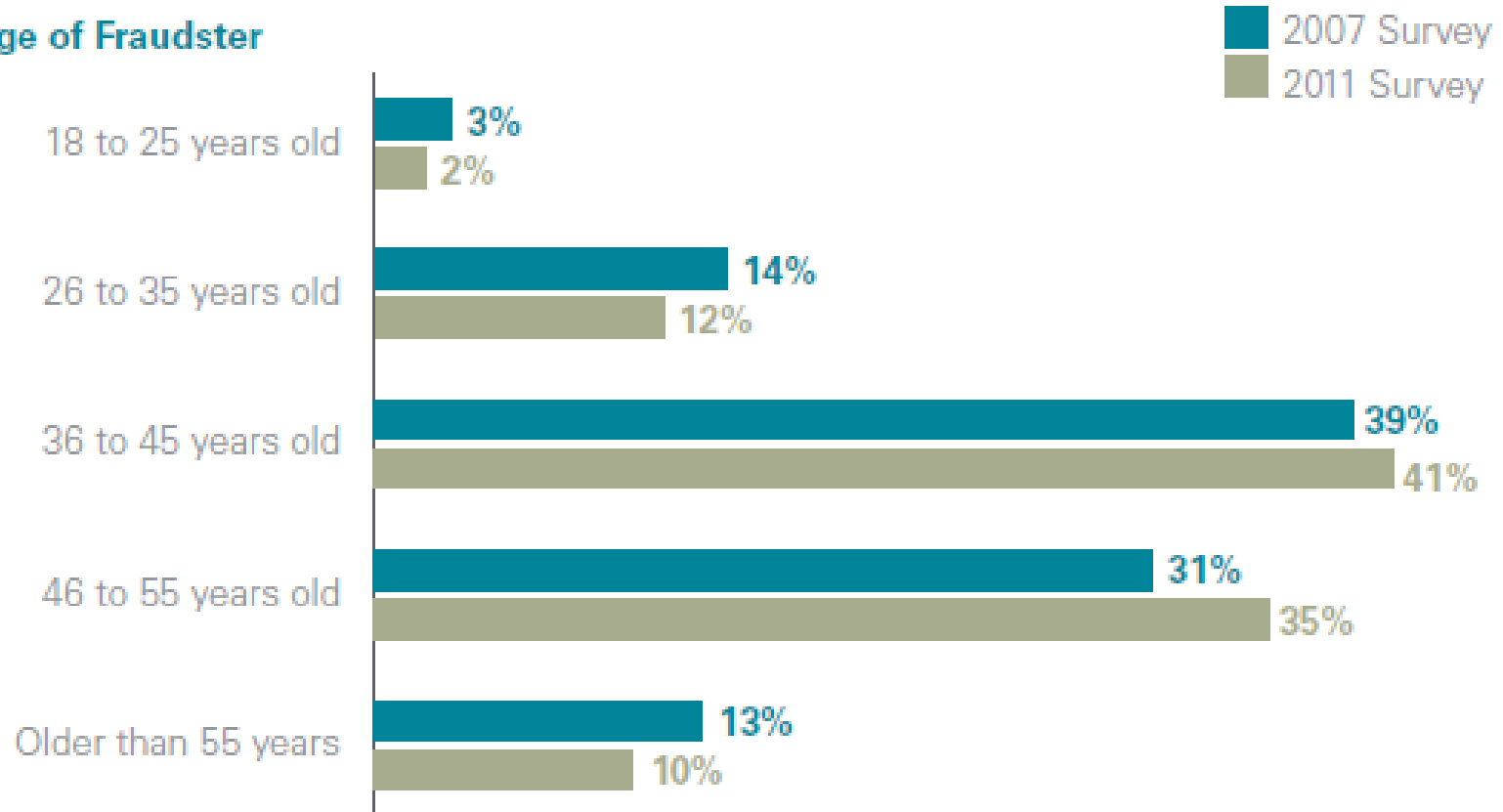
## Who is the Typical Fraudster?

- Male
- 36 to 45 years old
- Commits fraud against his own employer
- Works in the finance function or in a finance-related role
- Holds a senior management position
- Employed by the company for more than 10 years
- Works in collusion with another perpetrator



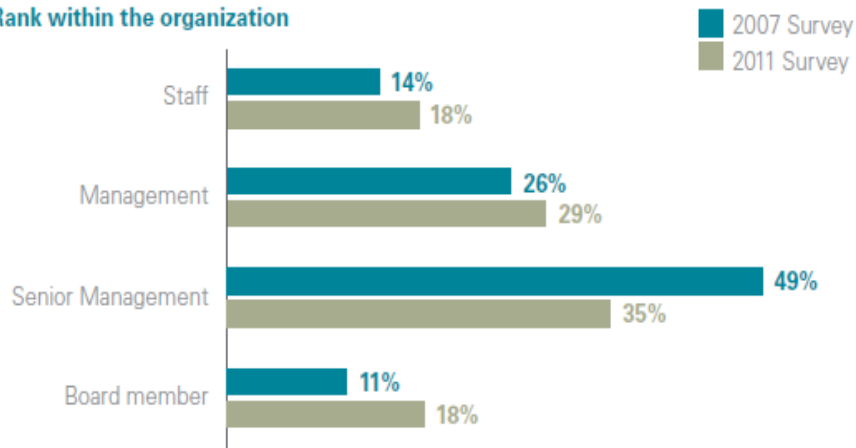
# Individual profile

## Age of Fraudster

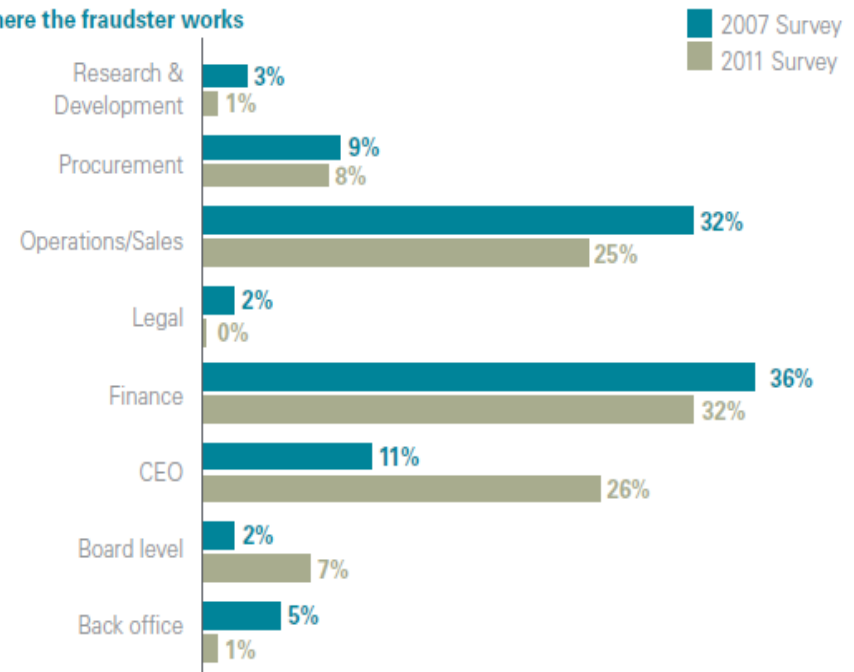


# Rank within the organisation/Where the fraudster works

## Rank within the organization

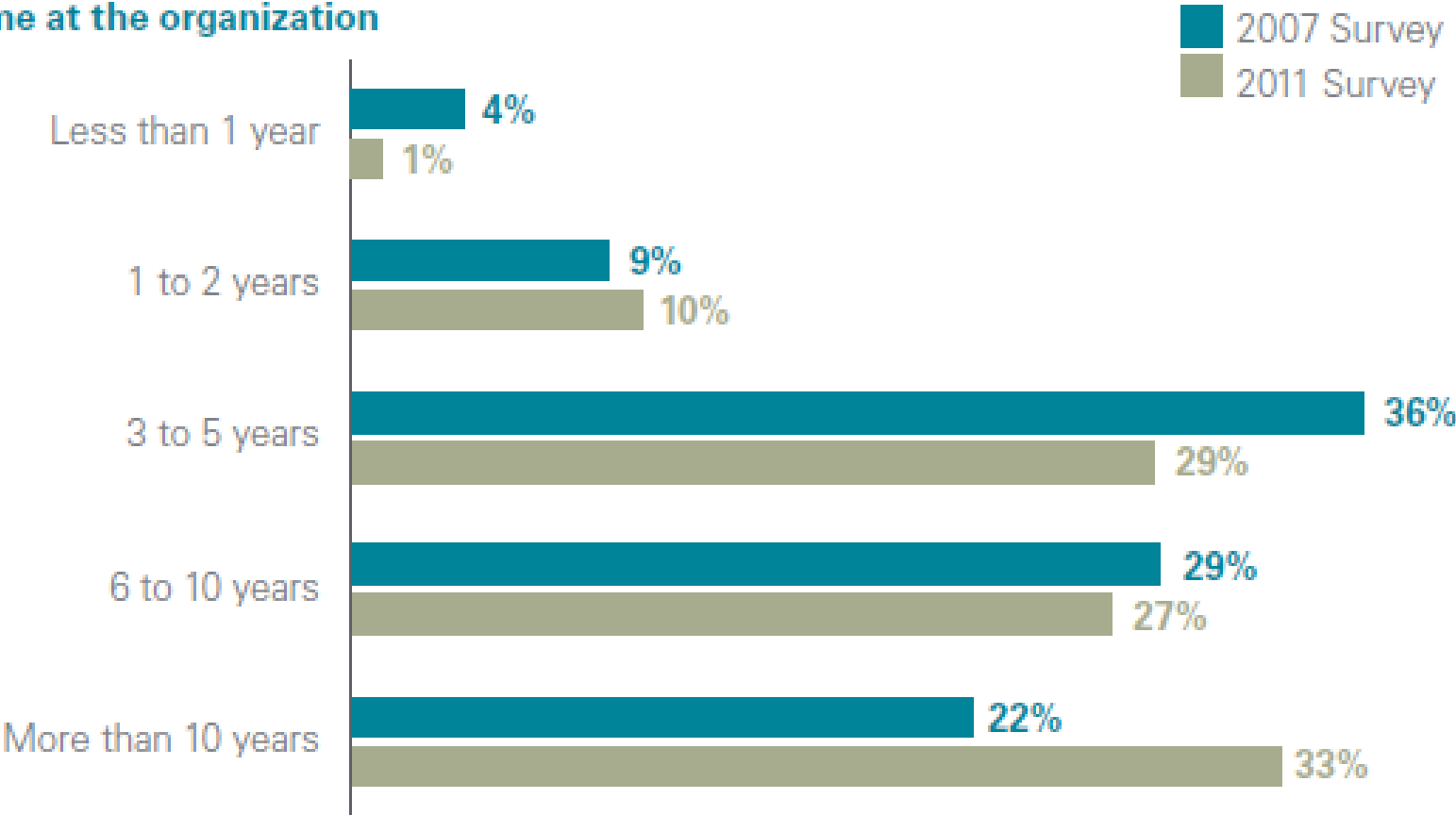


## Where the fraudster works



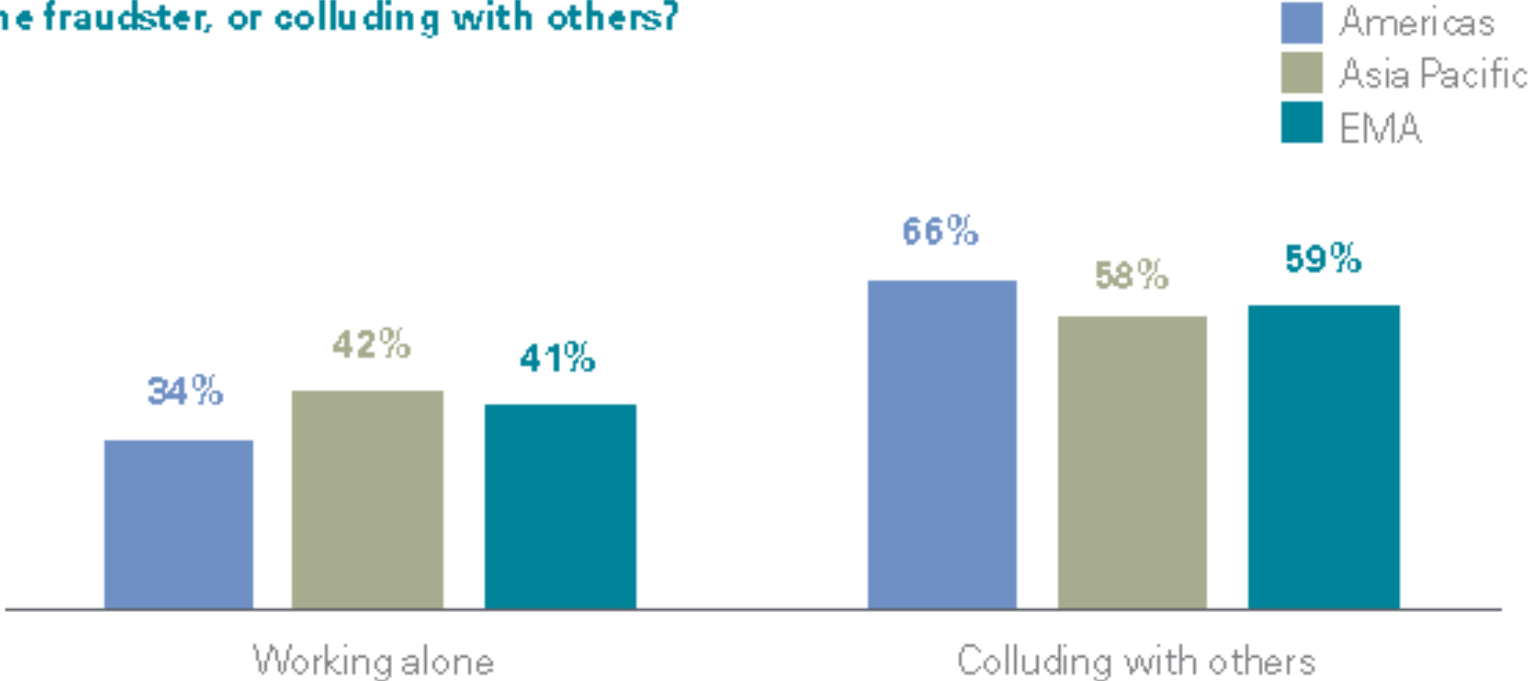
# Time at the organisation

Time at the organization



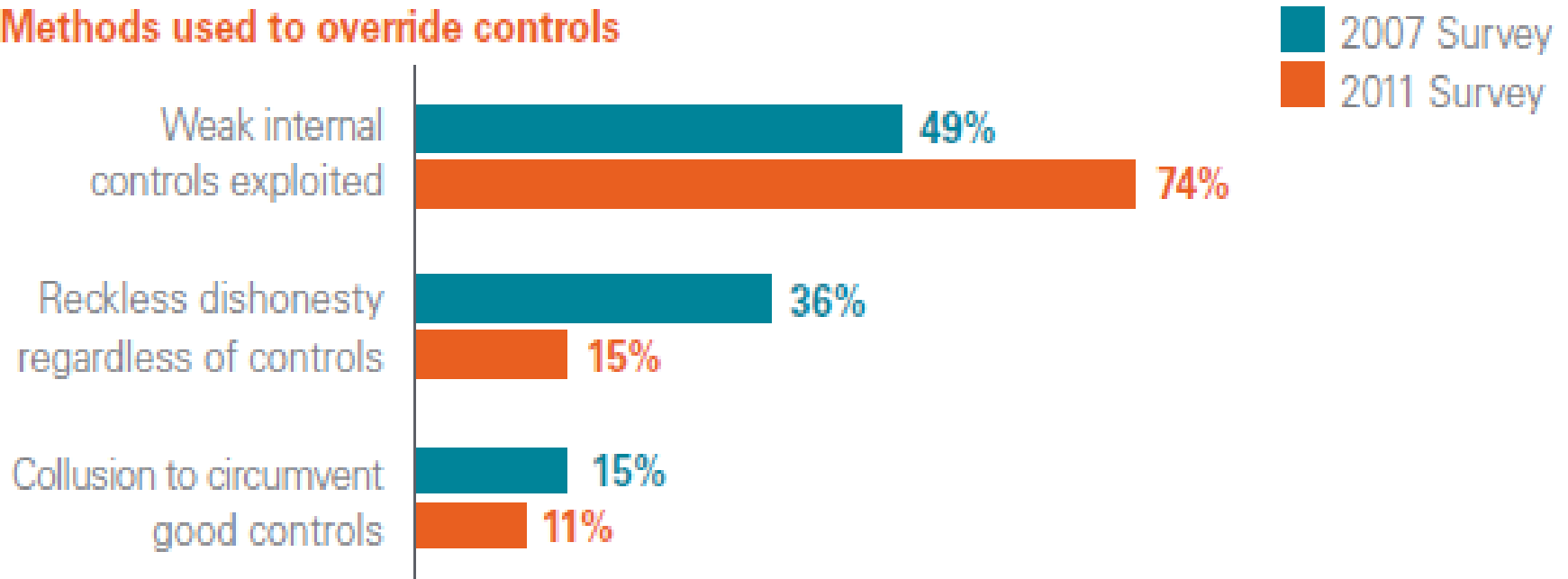
# Collusion

## Lone fraudster, or colluding with others?



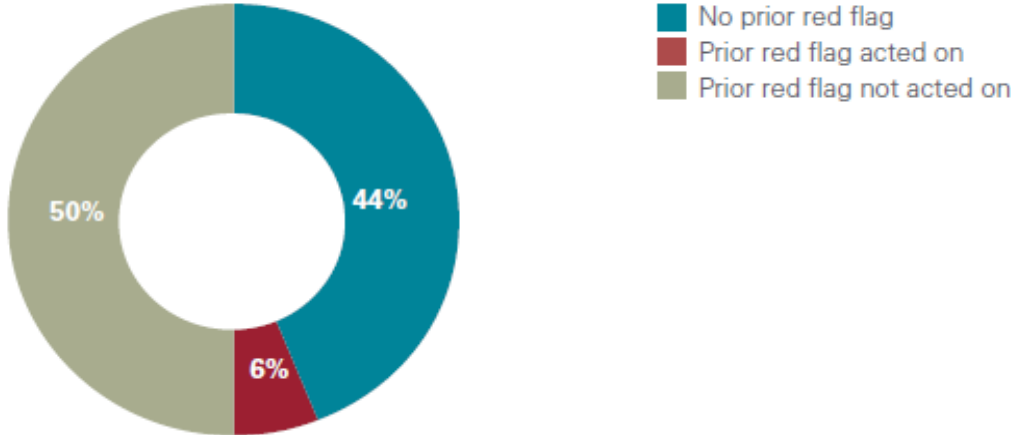
# Gaps in defenses

## Methods used to override controls

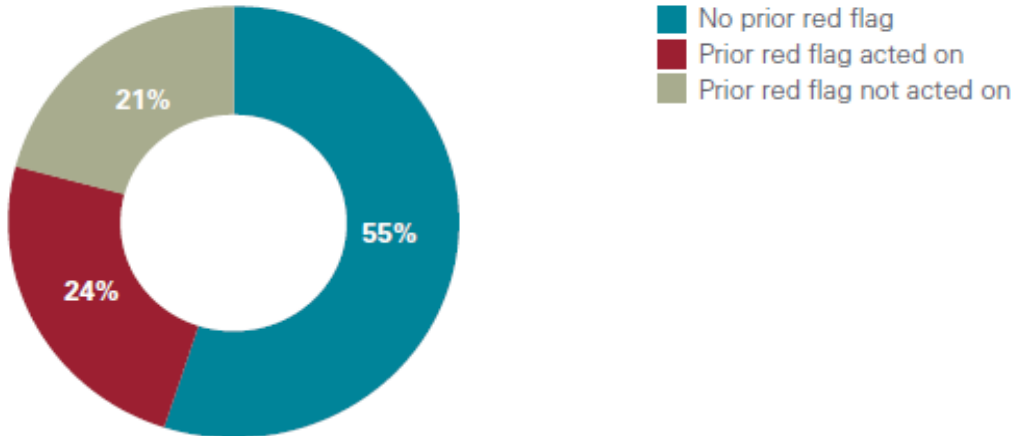


# Warning signs

Red flags identified and resulting actions taken (2011 Survey)



Red flags identified and resulting actions taken (2007 Survey)



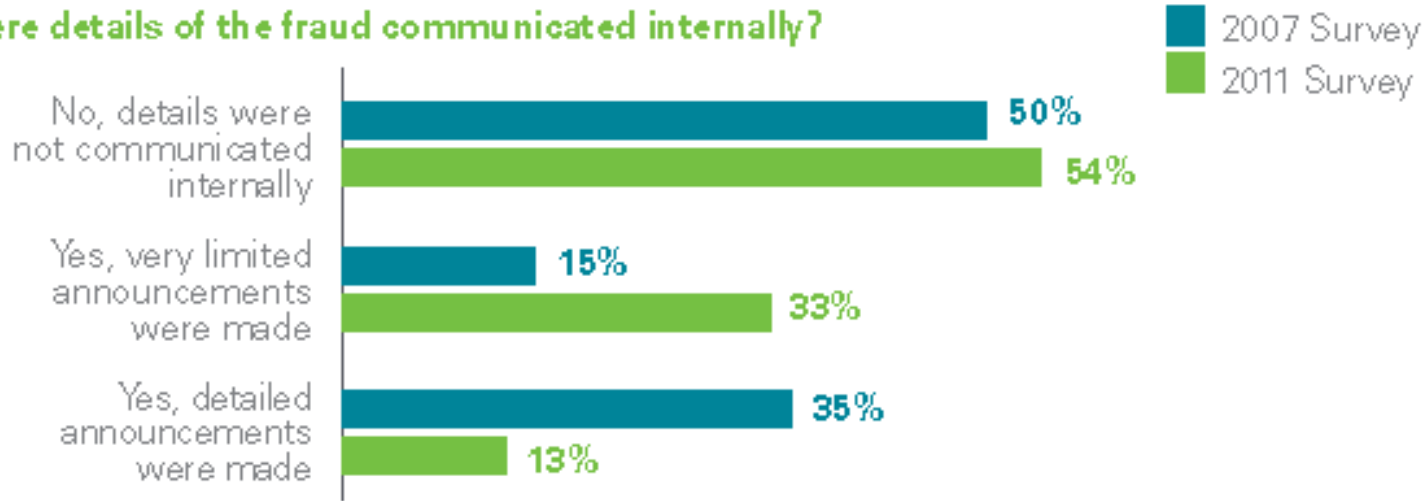


# Size and duration of the crime

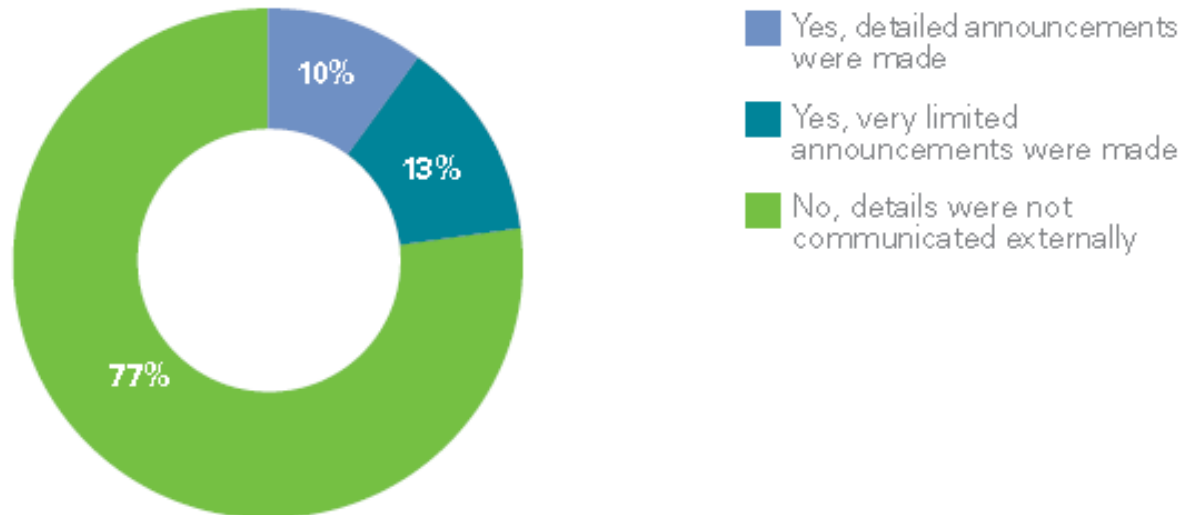
<b>Sub region</b>	<b>Average total losses per fraud (millions of U.S. dollars)</b>
Asia	1.5
Middle East	1.5
North America	1.2
Australia and New Zealand	1.1
Eastern Europe	1.0
Western Europe	0.9
Africa	0.9
South America	0.8
India	0.7

# Raising fraud awareness

## Were details of the fraud communicated internally?



## Were details of the fraud communicated externally?





**Introduction:**

**Effective Keys to  
Prevent & Detect Fraud**

# Approach to reducing fraud



Prevention	Detection	Response
<p style="text-align: center;">Board/audit committee oversight Executive and line management functions Internal audit, compliance, and monitoring functions</p>		
<ul style="list-style-type: none"> <li>• Fraud risk assessment</li> <li>• Code of conduct and related fraud policies and standards</li> <li>• Employee and third-party due diligence</li> <li>• Communication and training</li> <li>• Process-specific fraud risk controls</li> </ul>	<ul style="list-style-type: none"> <li>• Hotlines and whistleblower mechanisms</li> <li>• Auditing and monitoring</li> <li>• Proactive forensic data analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Internal investigation protocols</li> <li>• Enforcement and accountability protocols</li> <li>• Disclosure protocols</li> <li>• Remedial action protocols</li> </ul>



## Assessment of risks

Assessing the needs of the organisation based on the nature of fraud and misconduct that risk controls are intended to mitigate and the adequacy of existing controls.

## Design

Developing controls to prevent, detect, and respond to identified risks in a manner consistent with legal and regulatory criteria and other leading practices.

## Implementation

Deploying a process for implementing the new controls and assigning responsibility to individuals with the requisite level of authority, objectivity, and resources to support the process.

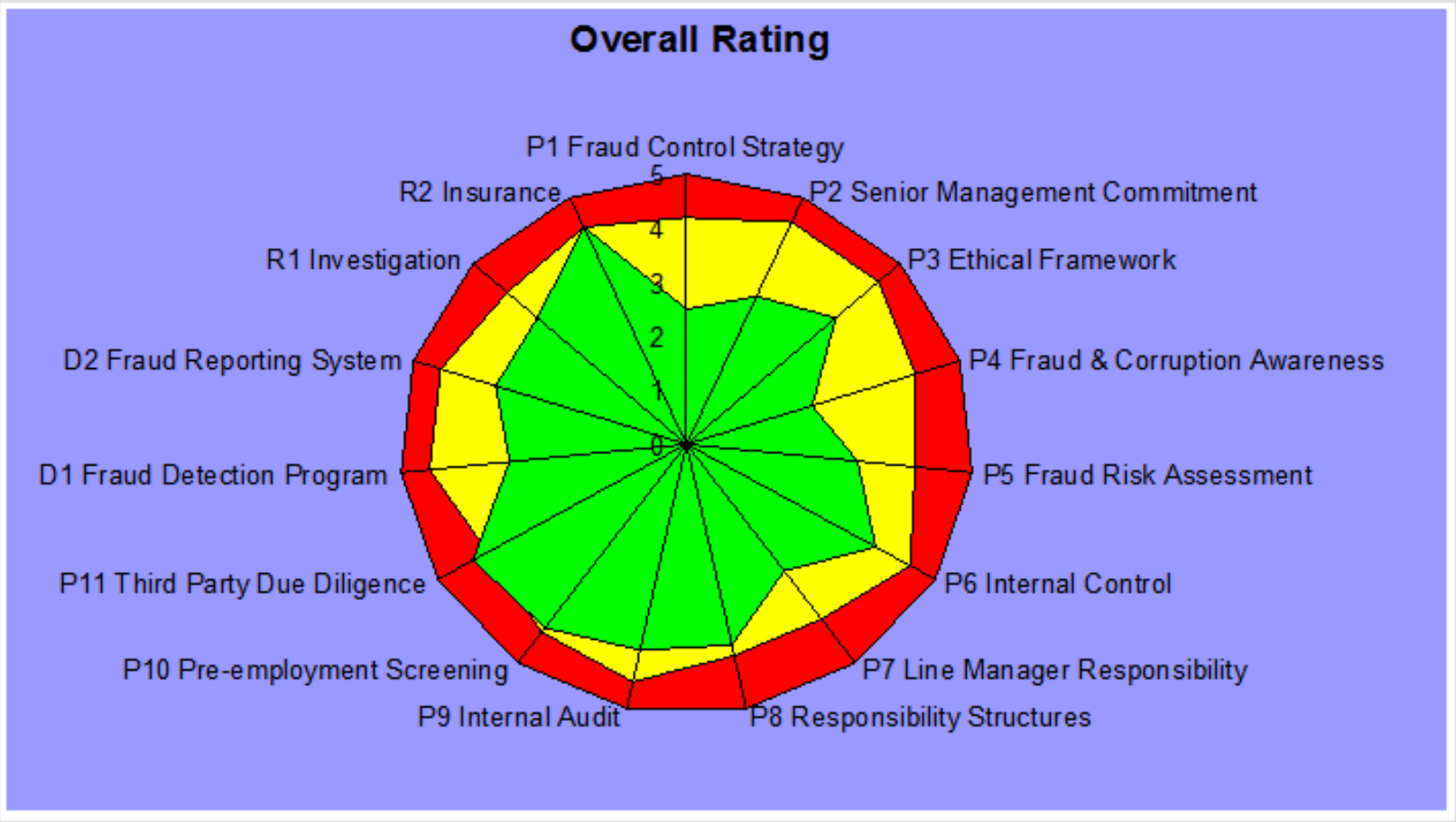
## Evaluation

Evaluating the design and operating effectiveness of controls through self-assessment, substantive testing, routine monitoring and separate evaluations.

# Fraud Gap Analysis

- Purpose is to review, at a high-level, fraud control policies and procedures.
- Assesses performance against 12 key attributes of a ‘better practice’ fraud control programme as follows:
  - Fraud control strategy
  - Senior management commitment
  - Ethical framework
  - Fraud awareness
  - Fraud risk assessment
  - Internal control
  - Line manager responsibility
  - Responsibility structures
  - Internal audit
  - Pre-employment screening & third party due diligence
  - Fraud detection programme
  - Fraud reporting systems

## Example reporting chart: Fraud Control Gap Analysis



# Fraud Risk Assessment

- A process aimed at proactively identifying and addressing an organisation's vulnerabilities to internal and external fraud in detail.
- Its objective is to help an organisation identify what makes it most vulnerable to fraud.
- Fundamental concepts are:
  - Probability – the chance an event will occur
  - Impact – the magnitude of the event if it occurs
- Process
- Frameworks



## Fraud Risk Assessment Framework

Ref	Risk	Inherent Risk			Employee and/or Location	Control Description	Effectiveness of Fraud Control	Control Type	Residual Risk			Control Improvements/ Fraud Risk Response
		L	S	R				P/D	L	S	R	

**Fraud Risk Matrix**

<b>Likelihood</b>	5	L	M	M	H	VH
	4	L	L	M	H	VH
	3	I	L	M	H	VH
	2	I	I	L	M	H
	1	I	I	L	M	H
		1	2	3	4	5
		<b>Significance</b>				



<b>Fraud Risk Matrix summary</b>		
<u>Likelihood (L)</u>		<u>Significance* (S)</u>
1 Rare	(<10% probability per year)	1 <\$100K
2 Unlikely	(<25% probability per year)	2 >\$100K-\$500K
3 Possible	(<50% probability per year)	3 >\$500K-\$1M
4 Likely	(<80% probability per year)	4 >\$1M-\$5M
5 Almost Certain	(>80% probability per year)	5 >\$5M

\*Also includes significance of **Reputation, Compliance and People**

<b>Risk Rating (R)</b>
VH- Very High; H – High; M- Medium; L- Low; I - Insignificant
<b>Control Type – P – Preventative; D - Detective</b>

# Other procedures to prevent fraud

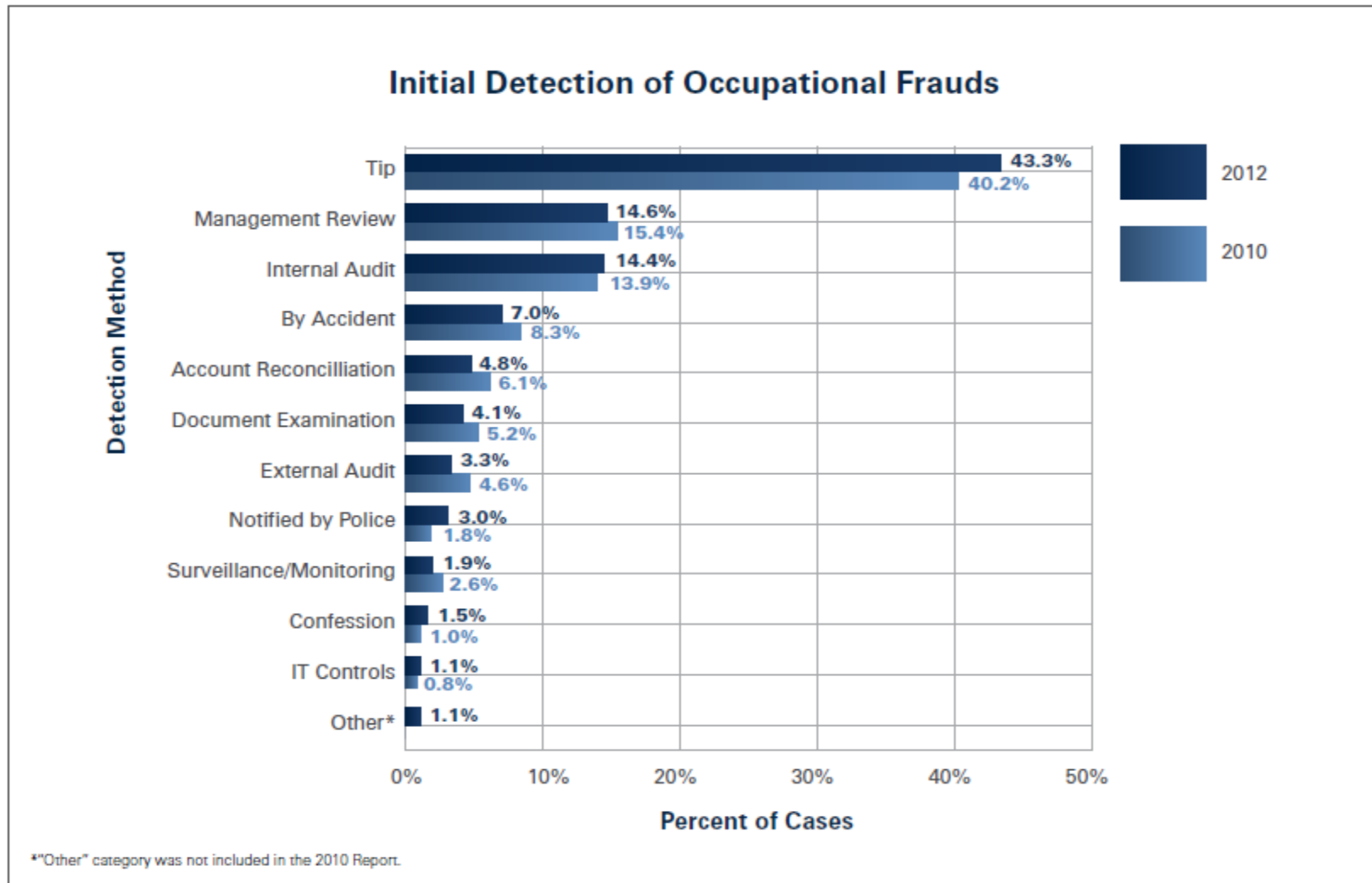
- Proactive fraud policy
- Management oversight
- Monitoring systems
- Fraud prevention policy and procedures
- Ethics programs
- Realistic financial goals
- Perception of detection

# Fraud detection

- Do not rely on external auditors!
- Anonymous hotlines
- Employee support programs
- Surprise audits
- Fraud training
- Job rotation/mandatory vacation
- Horizontal and vertical analysis of financial reports
- Ratio analysis
- Data analytics



# Initial detection of occupational frauds



Source: ACFE Report to the Nations on Occupation Fraud and Abuse – 2012 Global Fraud Survey

# Effectiveness of anti-fraud controls

## Median Loss Based on Presence of Anti-Fraud Controls

Control	Percent of Cases Implemented	Control in Place	Control Not in Place	Percent Reduction
Management Review	60.5%	\$100,000	\$185,000	45.9%
Employee Support Programs	57.5%	\$100,000	\$180,000	44.4%
Hotline	54.0%	\$100,000	\$180,000	44.4%
Fraud Training for Managers/Executives	47.4%	\$100,000	\$158,000	36.7%
External Audit of ICOFR	67.5%	\$120,000	\$187,000	35.8%
Fraud Training for Employees	46.8%	\$100,000	\$155,000	35.5%
Anti-Fraud Policy	46.6%	\$100,000	\$150,000	33.3%
Formal Fraud Risk Assessments	35.5%	\$100,000	\$150,000	33.3%
Internal Audit/FE Department	68.4%	\$120,000	\$180,000	33.3%
Job Rotation/Mandatory Vacation	16.7%	\$100,000	\$150,000	33.3%
Surprise Audits	32.2%	\$100,000	\$150,000	33.3%
Rewards for Whistleblowers	9.4%	\$100,000	\$145,000	31.0%
Code of Conduct	78.0%	\$120,000	\$164,000	26.8%
Independent Audit Committee	59.8%	\$125,000	\$150,000	16.7%
Management Certification of F/S	68.5%	\$138,000	\$164,000	15.9%
External Audit of F/S	80.1%	\$140,000	\$145,000	3.4%

Source: ACFE Report to the Nations on Occupation Fraud and Abuse – 2012 Global Fraud Survey

# Identifying common red flags

“A set of circumstances that are unusual in nature or vary from the normal activity. It is a signal that something is out of the ordinary and may need to be investigated further”.

**Do not ignore red flags!!!**

Types of red flags:

- Opportunity red flags
- Situational pressure red flags
- System red flags



# Examples of red flags

- **Opportunity red flags**

- Weak internal controls
- Inadequate screening of new employees
- Poor accounting records

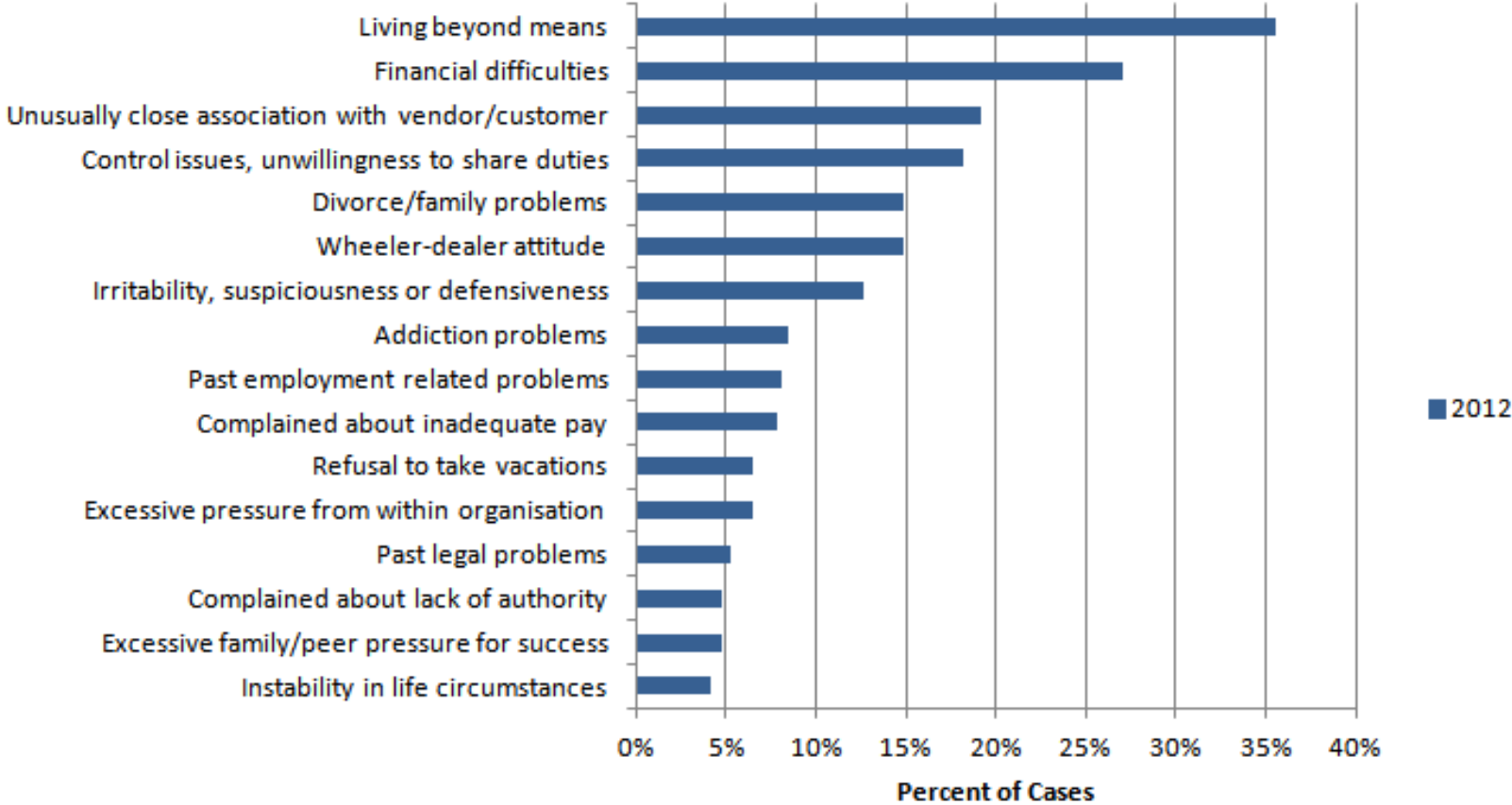
- **Situational pressure red flags**

- Resentment of superiors
- Inadequate income for lifestyle
- Emotional trauma in home or work life

- **System red flags**

- Accounts payable
  - Recurring identical amounts from the same supplier
  - Sequential invoice numbers from the same supplier
  - Payments increased to supplier for no apparent reason
- Payroll
  - Increase in overtime not justified by production or sales volume
  - Tax payments less than those required by current payroll expenses
  - High volume of manual transactions processed outside the payroll system

### Behavioural Red Flags of Perpetrators





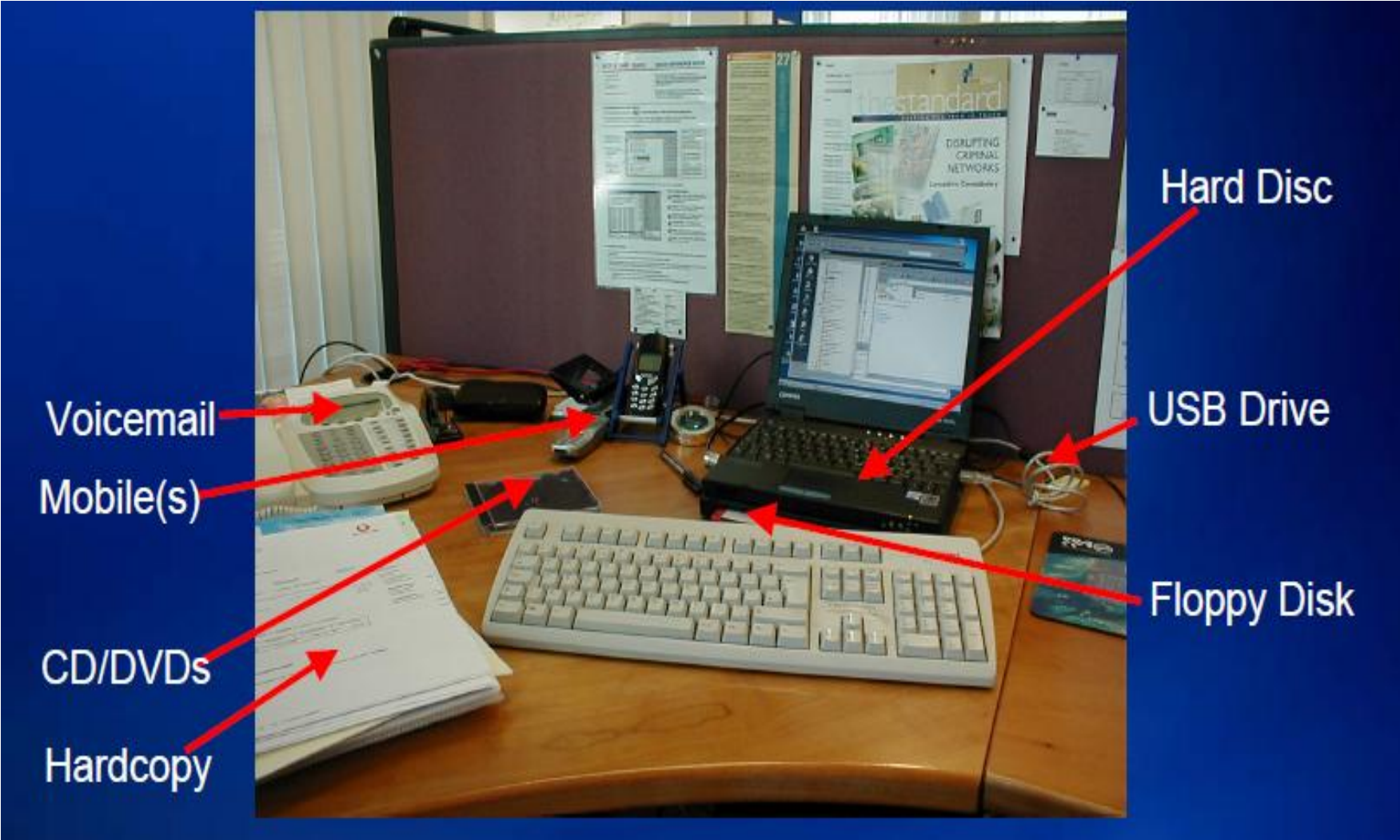
# What is forensic accounting?

- Forensic accounting is the application of investigative and analytical skills for the purpose of resolving financial issues in a manner that meets standards required by courts of law.
- Forensic accounting includes:
  - Fraud and misconduct investigations
  - Business valuations
  - Dispute resolution
  - Calculation of lost profits
  - Damages to business property
  - Valuation of divorce assets
- It is the use of accounting and information from other sources (e.g. interviews) to objectively determine facts in a manner that can support reasonable positions in court.

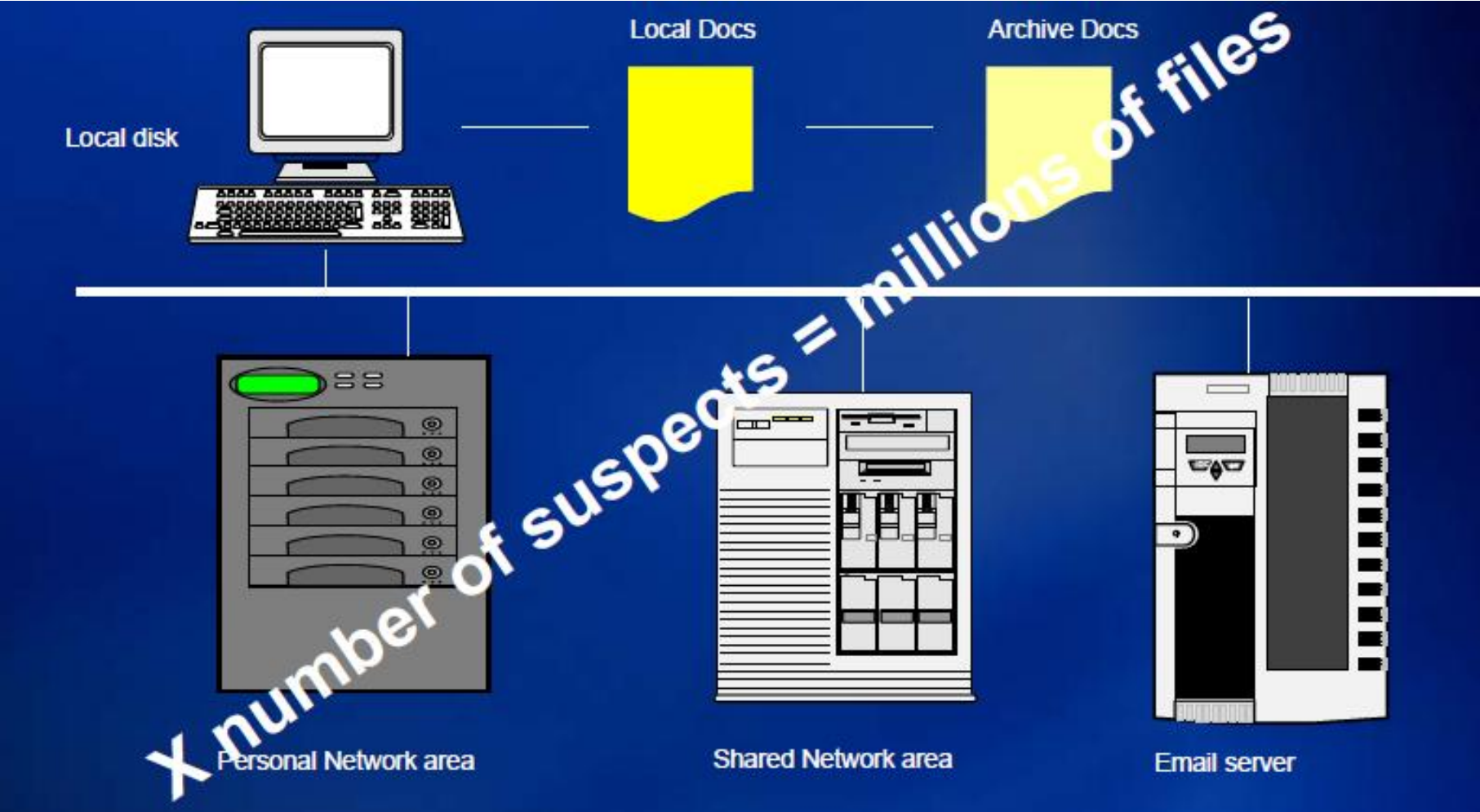


**The impact of  
IT on fraud**

# The old way



# The new way





# Data Volumes

**Kilobyte (KB)** 2 Kilobytes: A Typewritten page

100 Kilobytes: A low-resolution photograph

**Megabyte (MB)** 1 Megabyte: A small novel OR a 3.5 inch floppy disk

5 Megabytes: The complete works of Shakespeare

**Gigabyte (GB)** Gigabyte: a pickup truck filled with books

100 Gigabytes: A library floor of academic journals

**Terabyte (TB)** 1 Terabyte: 50,000 trees made into paper and printed

2 Terabytes: An academic research library

**Petabyte (PB)** 2 Petabytes: U.S. academic research libraries

200 Petabytes: All printed material

**Exabyte (EB)** 2 Exabytes: Total volume of information generated in 1999

5 Exabytes: words ever spoken by human beings

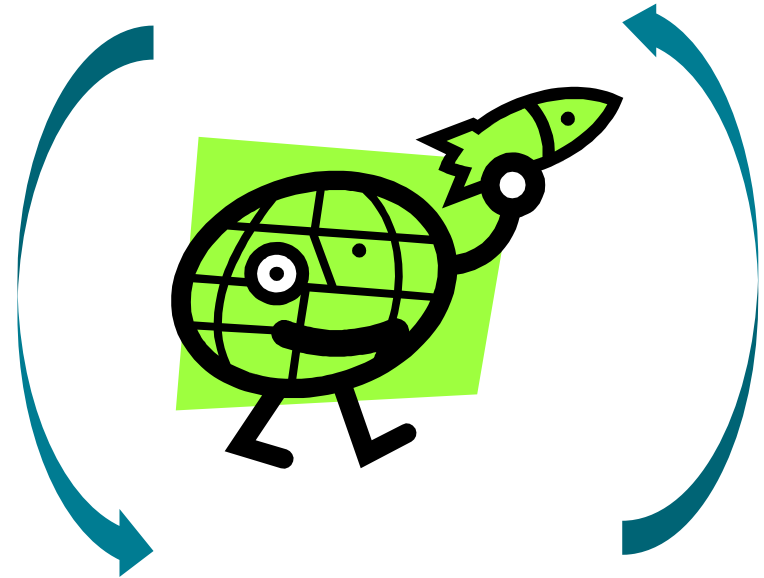
# Quantity of data



297 mm long

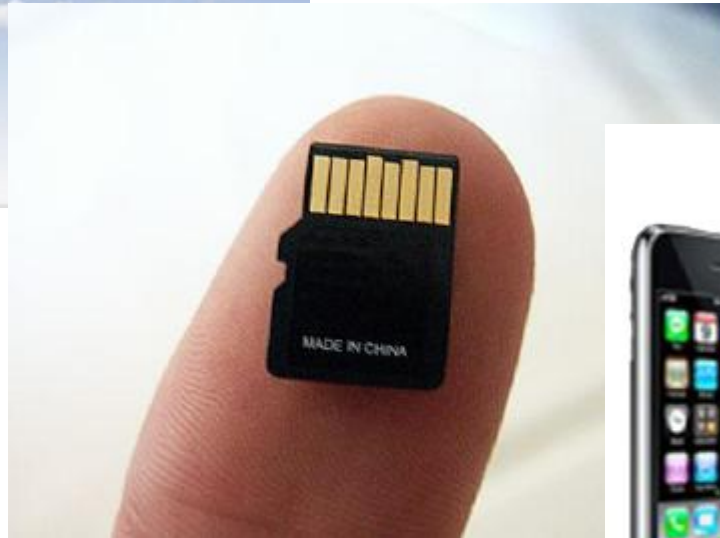


1 TB



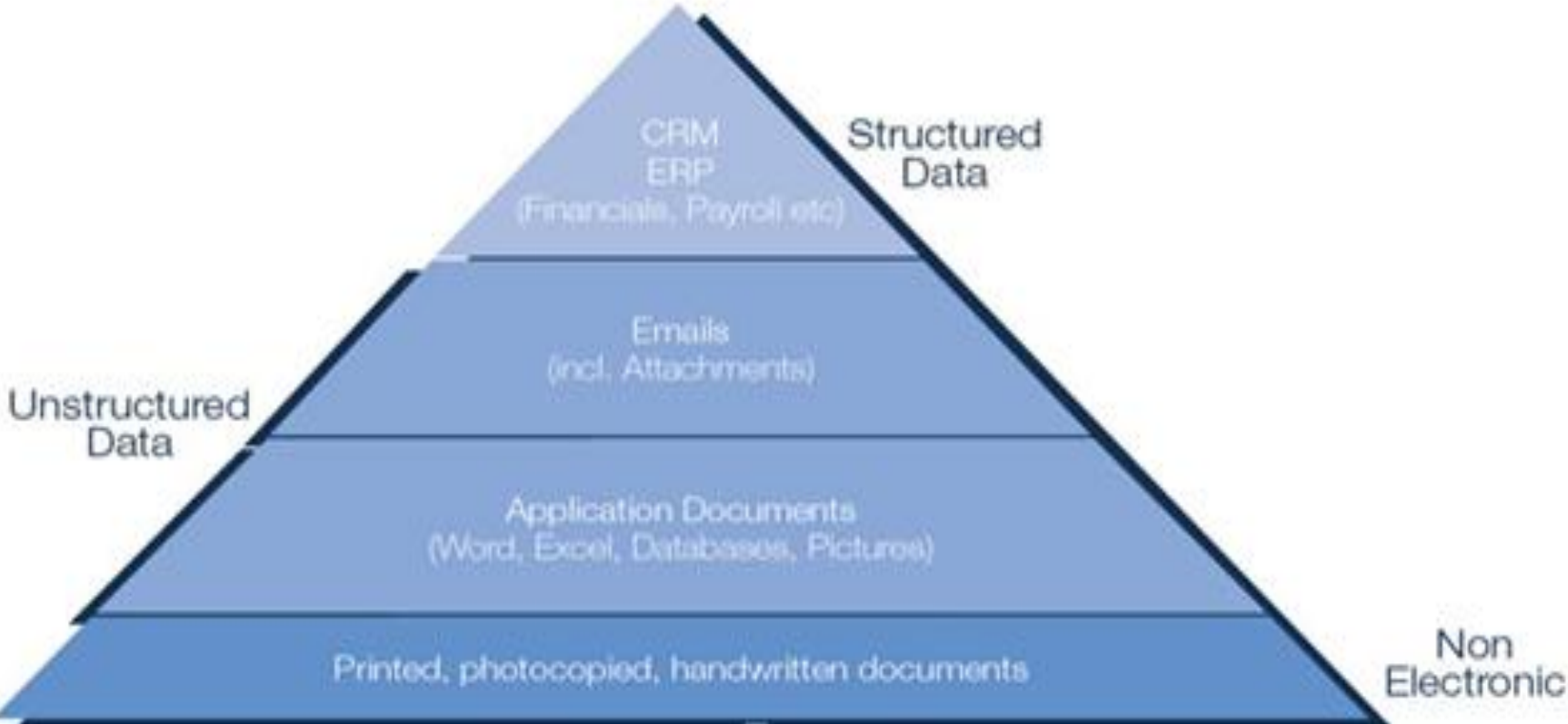
98,999 km end to end

# Other considerations – who ‘owns’ the information & compulsion to produce





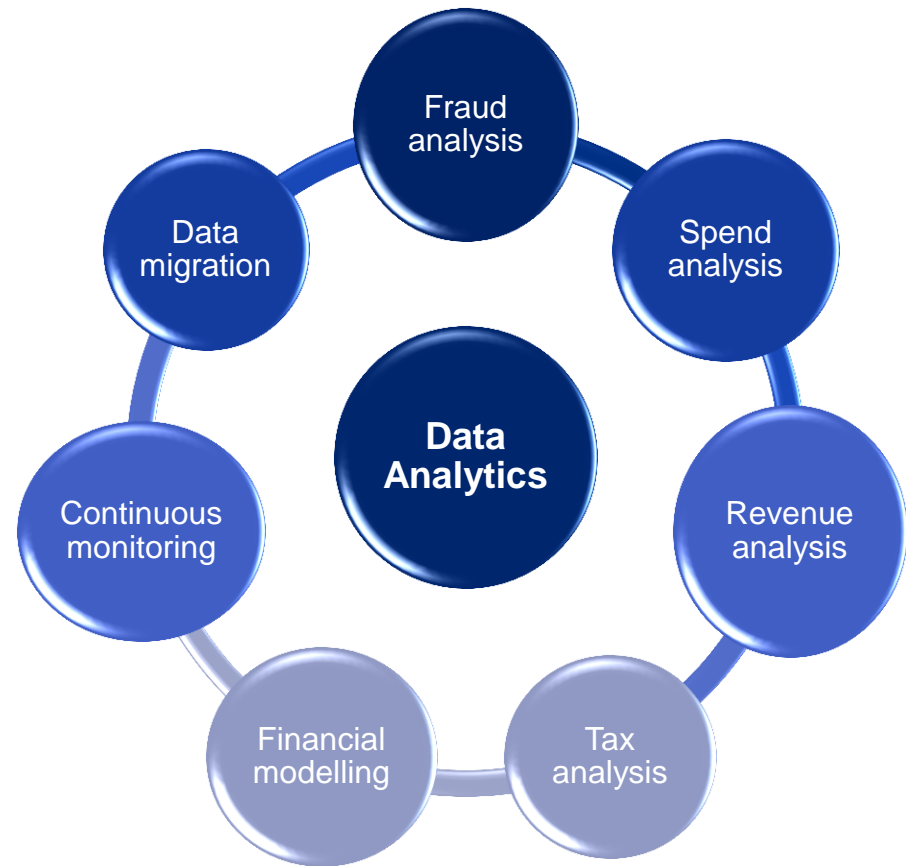
# Structured and unstructured data – Data Analysis



# What is Data Analytics?

Data analytics is characterised by:

- Analysing large data sets to obtain full coverage
- Automated procedures and approaches
- Use of software
- Performing tests not feasible to do manually
- Re-calculation of manually calculated values
- Repeatable
- Quantifying issues
- Finding that needle in the haystack



The background consists of several overlapping, semi-transparent geometric shapes in various shades of blue (light, medium, and dark) and white. The shapes are primarily parallelograms and trapezoids, creating a dynamic, layered effect. The text 'Forensic Computing' is centered in the white space of the right side of the image.

# Forensic Computing

*“For any two points of contact there is always a cross-transference of material from one to the other.”*

Edmond Locard 1877–1966

**Every contact leaves a trace.**

# What is forensic computing?

## Goal

The goal of computer forensics is to examine digital media in a manner with the aim of preserving, recovering, analysing and

facts and opinions about the information.

forensically sound



## Evidence

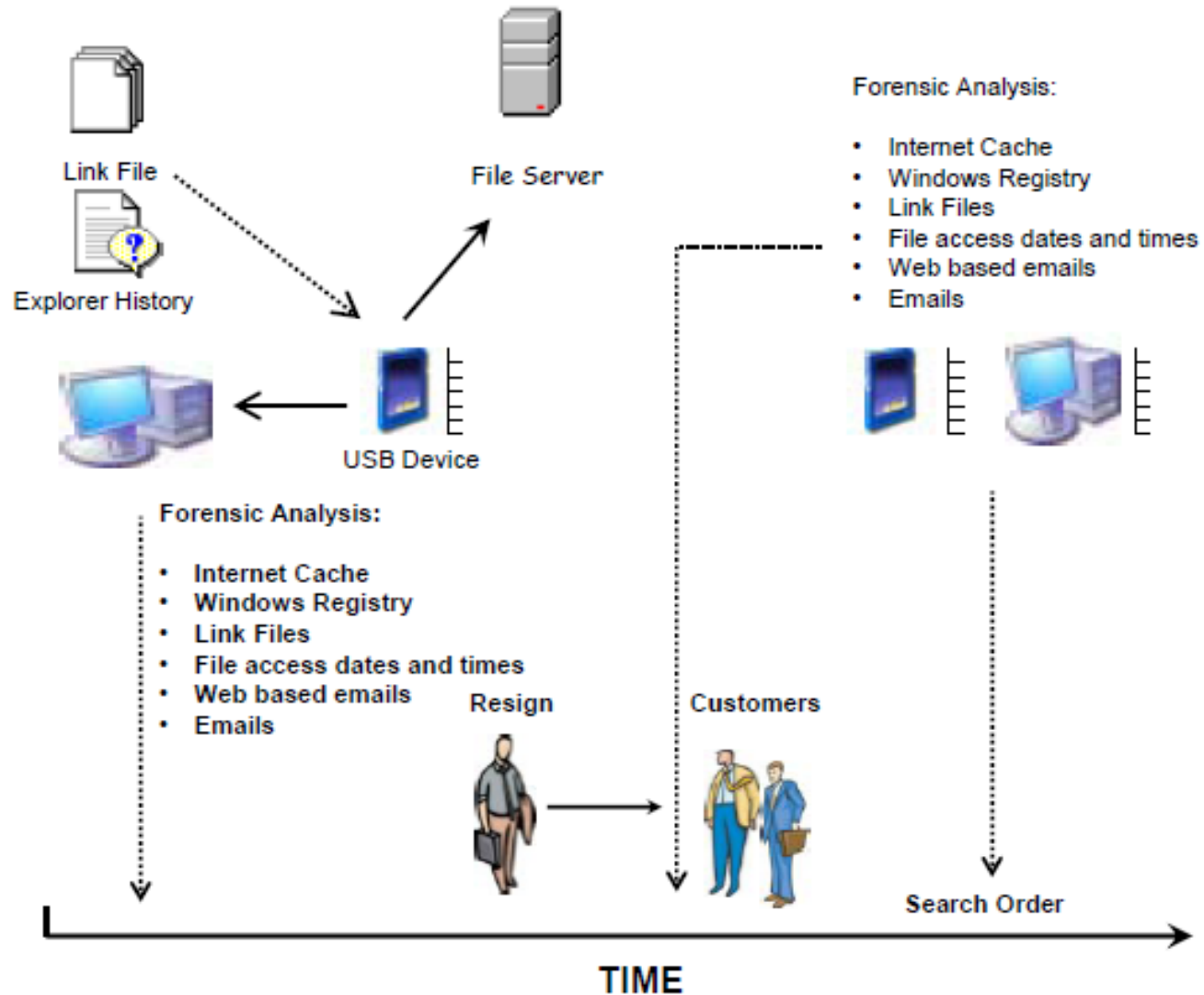
- All evidence must pass at least three "hurdles" before it will be admitted:
  - Relevancy
  - Competency; and
  - Materiality

## Best Evidence

- The Best Evidence Rule:

requires that anything of a documentary or "content" nature must have the **originality of it authenticated by a witness** competent enough to vouch for the factual basis of it upon **recognition of the original** even though that original may have changed hands.

# Reconstructing the past



# What to consider?

- What types of electronic evidence can be retrieved from a Personal Computer?
- What are the various sources of electronic evidence to be found in a home?
- Can personal or home based evidence be obtained?
- What types of electronic evidence can be retrieved from a corporate network?
- What are the sources of electronic evidence in a corporate environment?
- What are the key steps or considerations when identifying and collecting electronic evidence?



# Evidence locations

## ● Corporate:

- File, E-Mail, Proxy, Fax servers
- Firewall, E-mail, System logs
- Laptops, Computer, Tablets
- Removable media (Thumb drives, CD/DVD)
- Backup media (HDD, Tapes)
- Multi-function devices (Photocopier/Printers)
- Voice mail systems
- Smart devices (Memory cards inside)
- Alarm and access control systems
- Vehicle GPS/Computers
- Laptops, Computer, Tablets
- Home networks logs
- Removable media (Thumb drives, CD/DVD)
- Backup media (HDD, Tapes)
- Multi-function devices (Photocopier/Printers)
- ISP Records
- Smart devices (Memory cards inside)
- Gaming machines

## ● Home:

# Best practice guides

- Good practice guide for Computer-Based Electronic Evidence – Association of Chief Police Officers UK
- Forensics Plan Guide SANS Institute 2006
- Electronic Crime Scene Investigation, A Guide for First Responders – US DoJ NIST
- HB 171-2003 Guidelines for the management of IT evidence – Standards Australia
- RFC 3227 Guidelines for Evidence Collection and Archiving
- Emerging Standards:
  - [ISO/IEC WD 27037.3 Information Technology: Security Techniques – Guidelines for the identification, collection and/or acquisition and preservation of digital evidence](#)

# Locard's Exchange Principle

Every contact, no matter how slight, will leave a trace.



---

wiping hard drive	
wiping hard drive	910,000 results
wiping a hard drive	602,000 results
wiping a blackberry	111,000 results
wiping blackberry	232,000 results
wiping a computer	2,290,000 results
wiping iphone	383,000 results
wiping hard drives	669,000 results
wiping rags	119,000 results
wiping computer	2,280,000 results
wiping a hard drive clean	137,000 results

[close](#)

# Internet Artifacts


Last Visited [UTC]	Host	Search Engine Criteria
12/07/2007 23:45:56 Thu	www.google.co.nz	hiding money obtained through fraud
12/07/2007 23:45:56 Thu	www.google.co.nz	
12/07/2007 23:45:44 Thu	www.antimoneylaundering.ukf.net	
12/07/2007 23:45:06 Thu	www.google.co.nz	how to steal money from employer
12/07/2007 23:45:05 Thu	www.google.co.nz	buy usb key with encryption
12/07/2007 23:43:56 Thu	stats.datahjaelp.net	
12/07/2007 23:43:56 Thu	gfx.download-by.net	
12/07/2007 23:43:49 Thu	pagead2.googlesyndication.com	
12/07/2007 23:43:49 Thu	www.zip-backup.com	
12/07/2007 23:43:48 Thu	www.download-by.net	
12/07/2007 23:43:48 Thu	www.download-by.net	
12/07/2007 23:43:48 Thu	pagead2.googlesyndication.com	
12/07/2007 23:43:24 Thu	www.lestwarog.com	
12/07/2007 23:43:24 Thu	pagead2.googlesyndication.com	
12/07/2007 23:43:24 Thu	pagead2.googlesyndication.com	

# Challenges

- Most IT Departments will not use forensically sound software to copy data.
- The IT Department may be staffed by contractors who may leave the business at the first opportunity.
- Most IT Departments recycle back up ‘tapes’ therefore to ensure a full back up exists of the systems at the date of appointment you will need to back up the systems and take the back up tapes out of circulation.
- Possibility of incorrect procedures
  - Knowledge of potential infringements
  - Investigation clarity
  - Accurate and factual information to be considered presented non-specialist
  - All factors to be considered
  - Unfair presentation (judgemental verses independent)
  - Consider legally privilege material
  - Provision of information to all parties

# Be wary

- The truth is the position of the teller
- Burden of proof requirements
- Correct process by all from first notice
- Not to use ‘this matter’ for other issues
- Independent experts can tell the story to their ‘clients’ advantage
- A user logon does not mean ‘they did it’
- Look for supporting evidence: alarms, email traffic, access other files etc



**eDiscovery & Technology  
Assisted Reviews  
(Tomorrows world)**

# Client Review - Intella

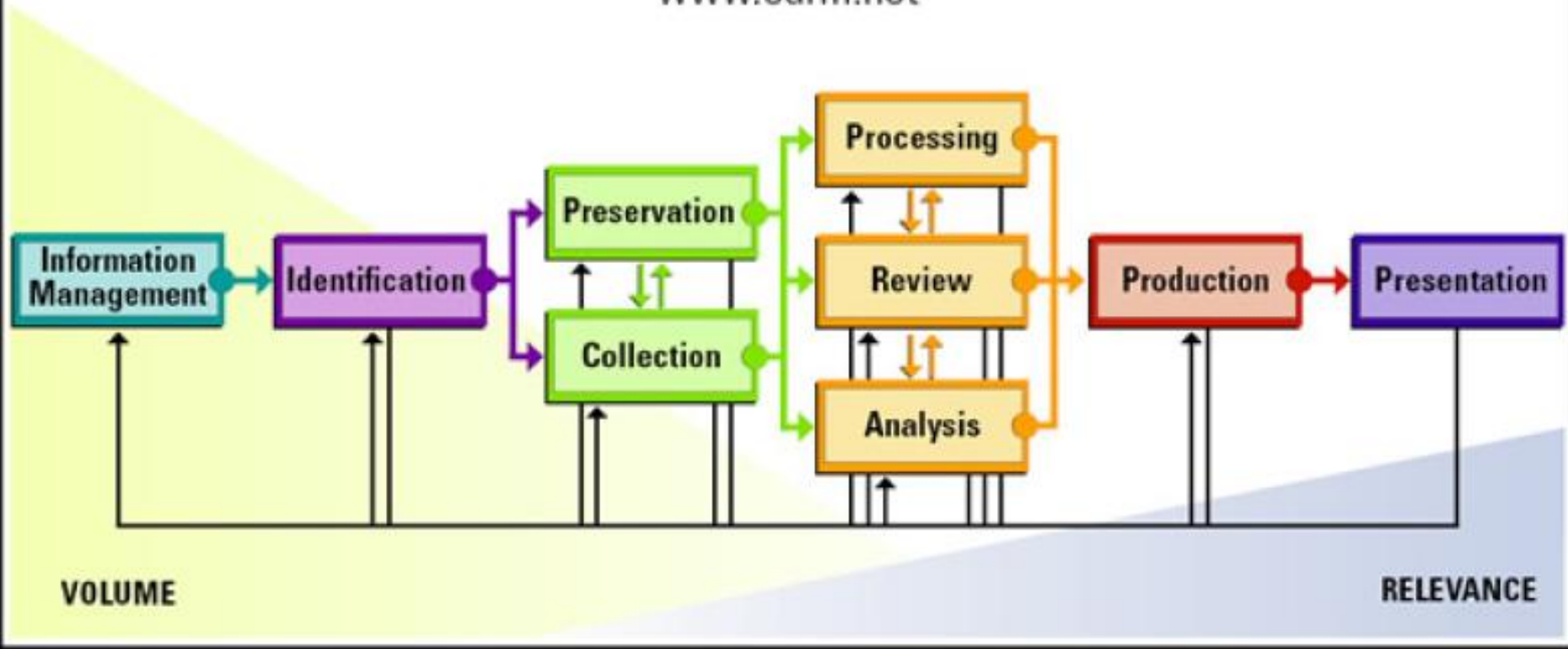




# Electronic discovery reference model

## Electronic Discovery Reference Model

[www.edrm.net](http://www.edrm.net)





Questions ?

Chris Budge

[cbudge@kpmg.co.nz](mailto:cbudge@kpmg.co.nz)

+64 4 8164832