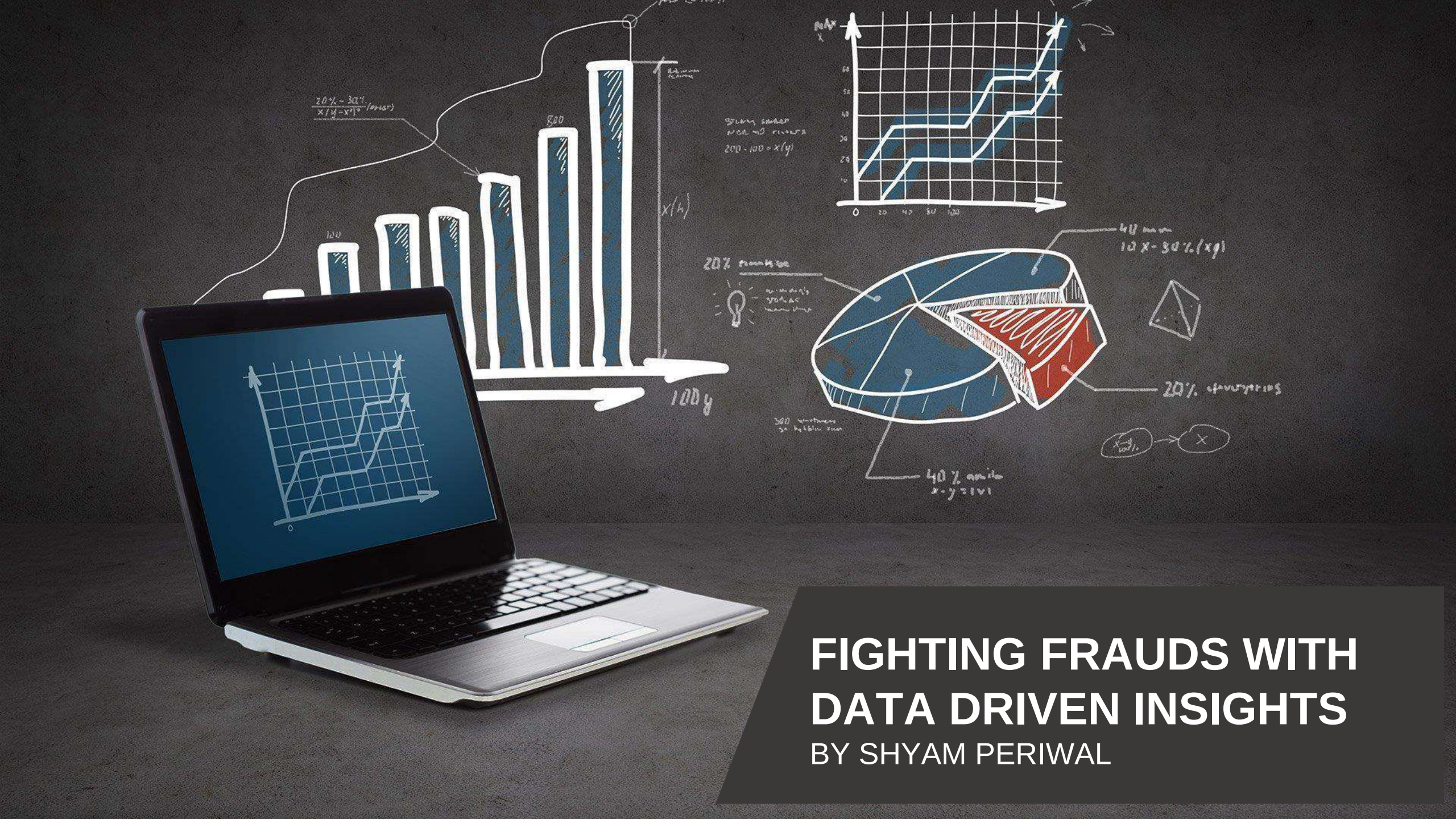


FIGHTING FRAUDS WITH DATA DRIVEN INSIGHTS

BY SHYAM PERIWAL

Table of Content

Fraud

What is Fraud?

Companies Act 2013

*As per the explanation to Sec 447 of Chapter XXIX, "**fraud**" in relation to affairs of a company or any body corporate, includes any **act, omission, concealment of any fact or abuse of position** committed by any person or any other person with the connivance in any manner, **with intent to** deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, **whether or not there is any wrongful gain or wrongful loss.***

The Institute of Chartered Accountants of India

*SA240 – The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements, issued by the ICAI defines fraud as an **intentional act** by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.*

Institute of Internal Auditors

*'Any illegal act characterized by **deceit**, **concealment**, or **violation of trust**. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain **money**, **property**, or **services**; to **avoid payment** or **loss of services,** or to secure **personal** or **business advantage**'.*

What is Common Among Them?

ENRON

Satyam

ARTHUR ANDERSEN

xerox

LEHMAN BROTHERS

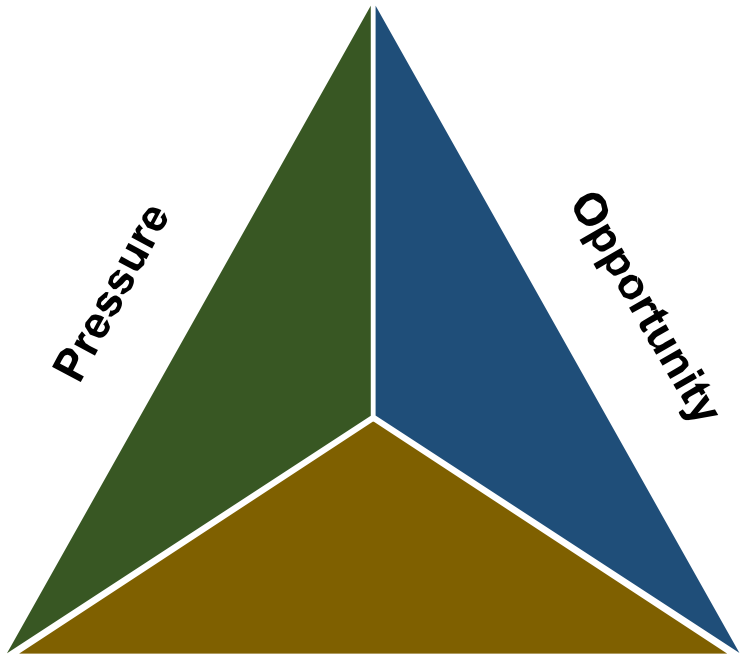
parmalat

What Happened Because of Fraud?

Why Frauds Happen?

Pressure (motive)

- Addiction – drink, drugs, gambling
- Coercion or blackmail
- Credit crunch
- Debts
- Family pressure
- Illness
- Results, results, results!
- Revenge



Opportunity (ability to carry out fraud)

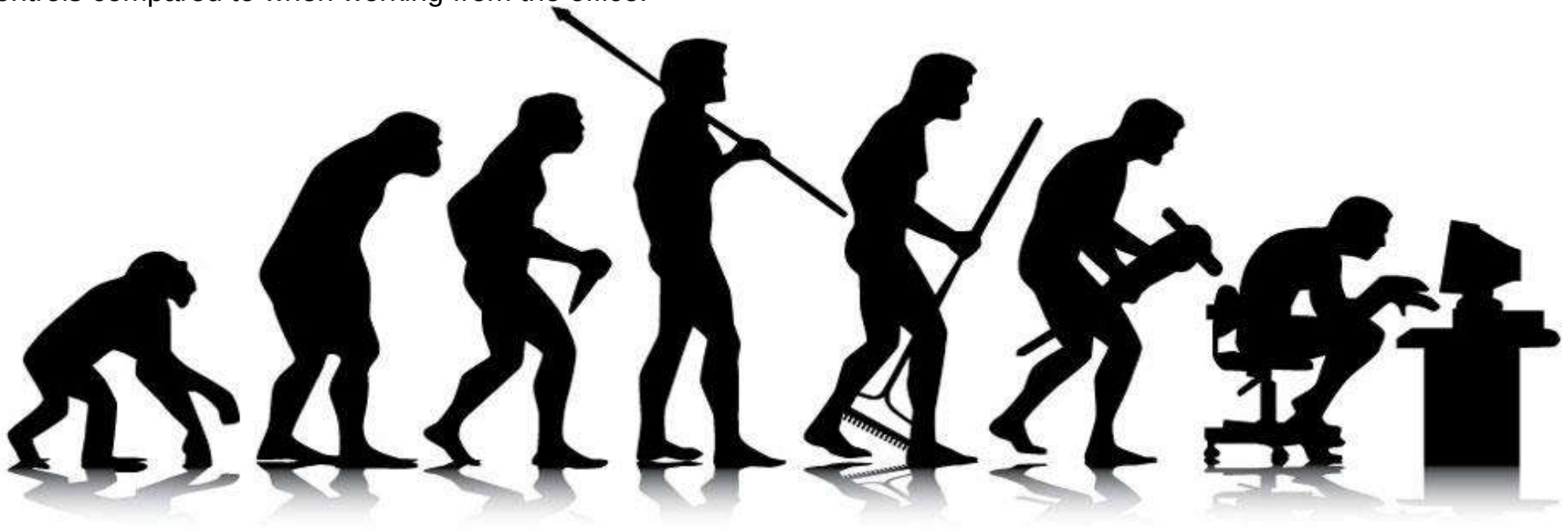
- Abuse of authority
- Complex transactions
- Exploiting errors
- Inadequate & ineffective internal audit
- Inadequate & ineffective internal controls
- Inadequate segregation of duties
- Lack of effective oversight
- Poor governance

Rationalization (justification of dishonest intention)

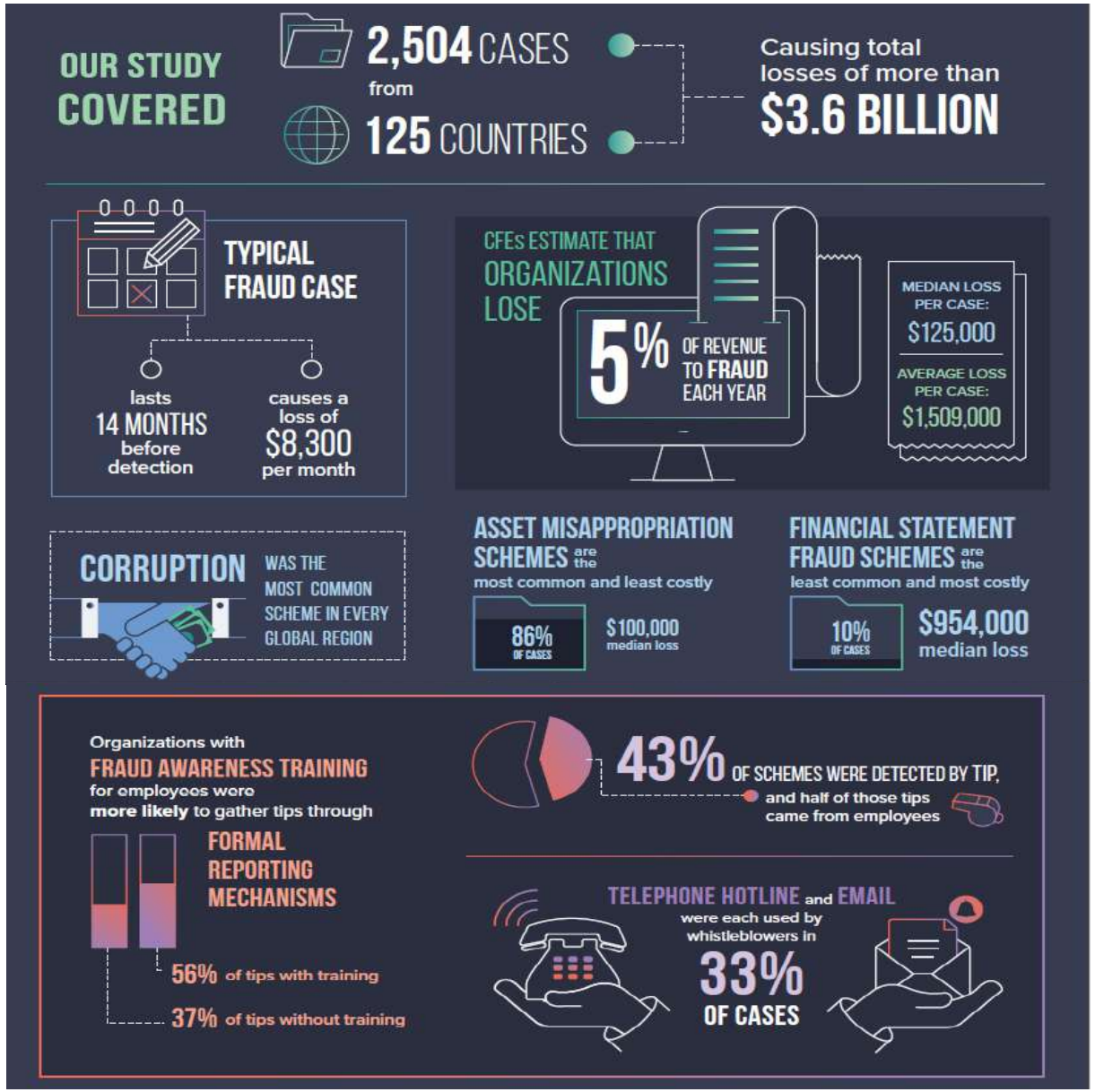
- Everyone else does it
- I am in charge
- It is a cost of doing business
- It is a victimless crime
- It is only a small amount
- I'll never get caught
- Rules are meant to be broken
- They can afford it
- They do not pay me enough
- Who cares?

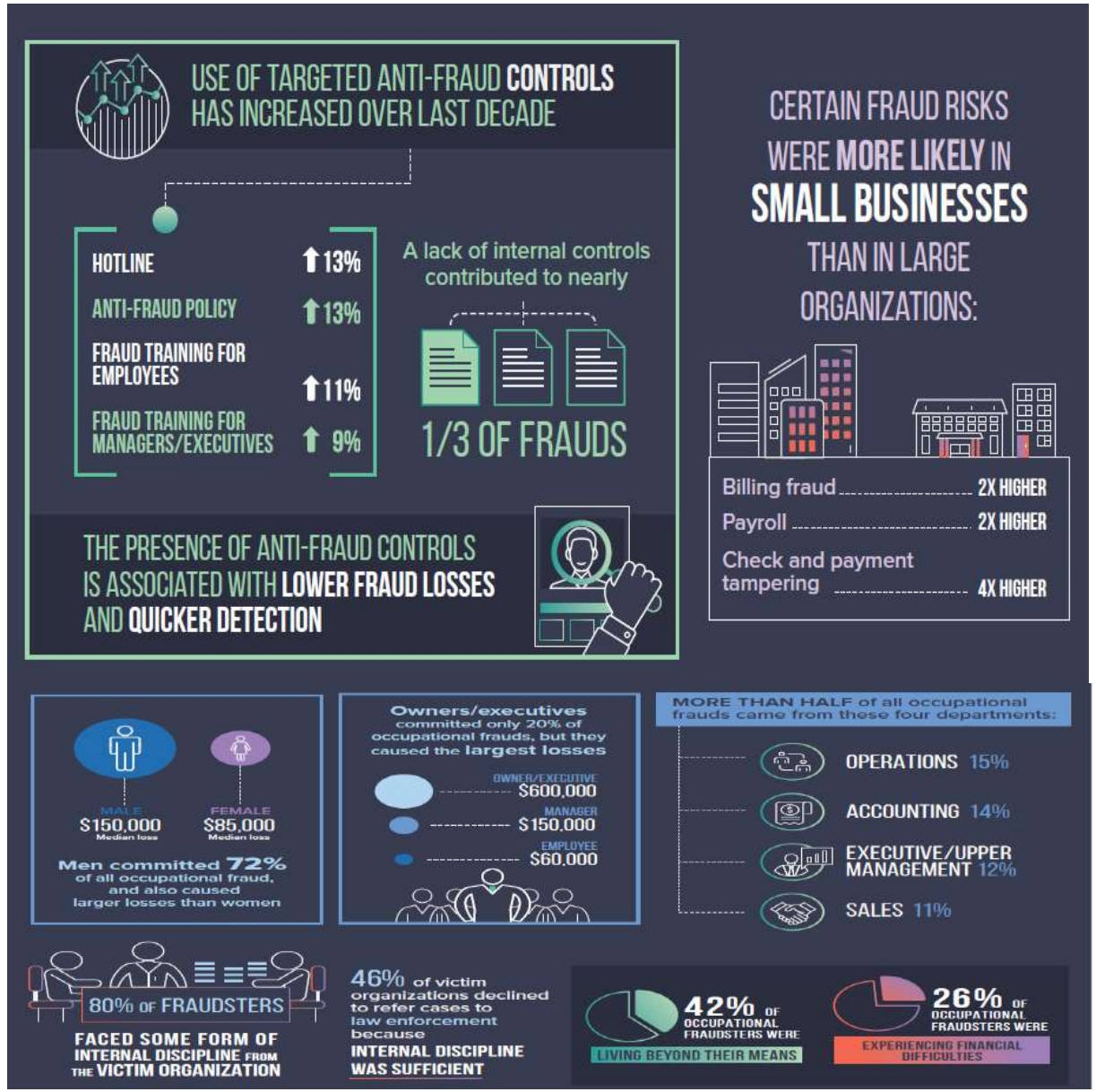
Frauds Is Evolving

- For today's business organizations, fraud is inevitable. It's no longer a matter of "if" you will be affected — it's a matter of "when" you will be affected.
- Many businesses are vulnerable to fraud, particularly those with sales channels exposed to electronic payment portals and systems, complex global supply chains, a significant presence in emerging markets, and so on.
- Business reengineering, reorganization, or downsizing may weaken or eliminate control, while new information systems may present additional opportunities to commit fraud.
- In recent years, the development of new technologies has also provided further ways in which criminals may commit fraud. With the advancement of technologies, fraud has evolved and become increasingly difficult to discover. In other words, the fraudster is getting smarter.
- The global pandemic- COVID-19 has also led to a higher number of frauds and malpractices since people are working from home, having poor IT controls compared to when working from the office.



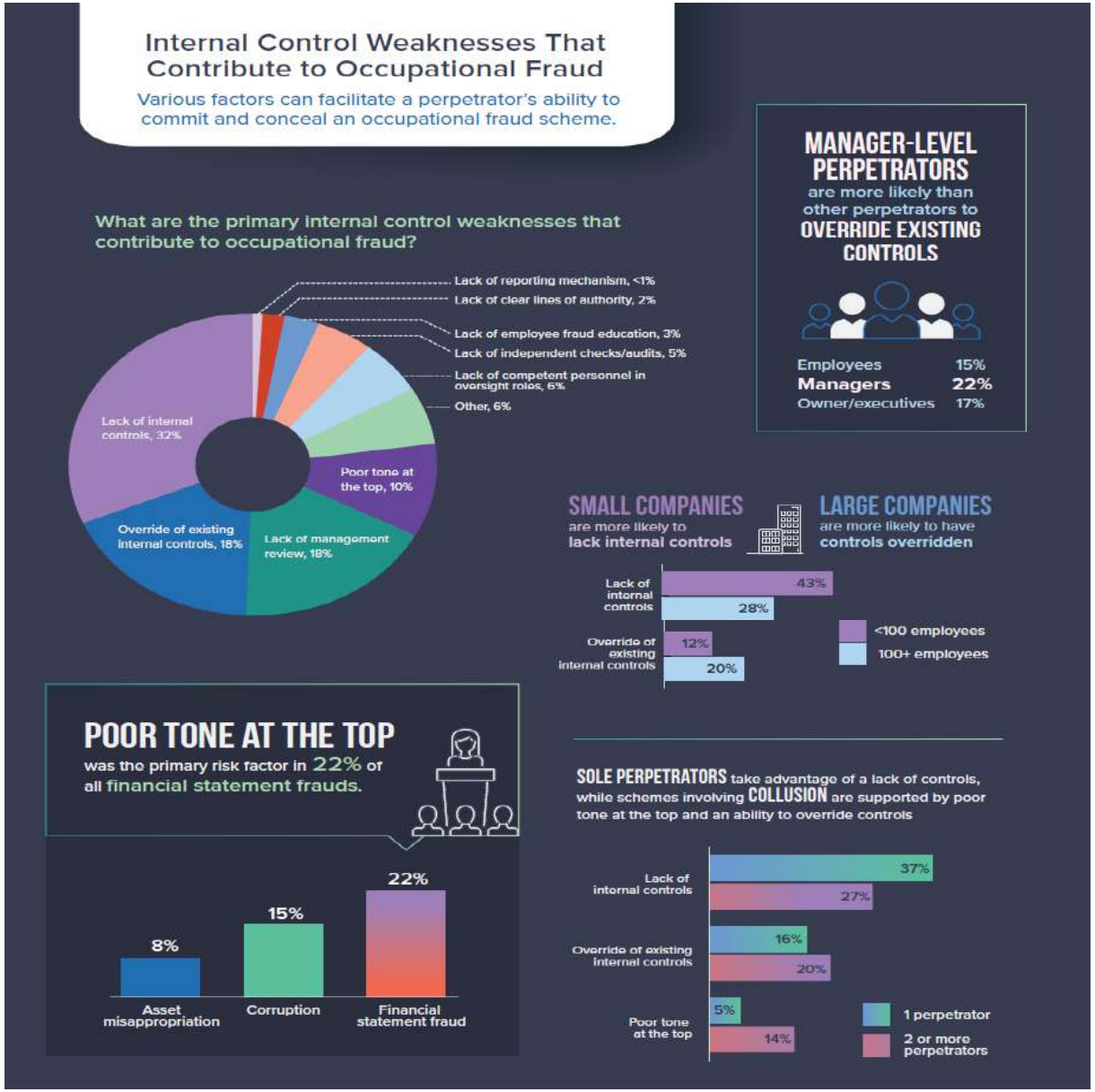
Fraud Statistics

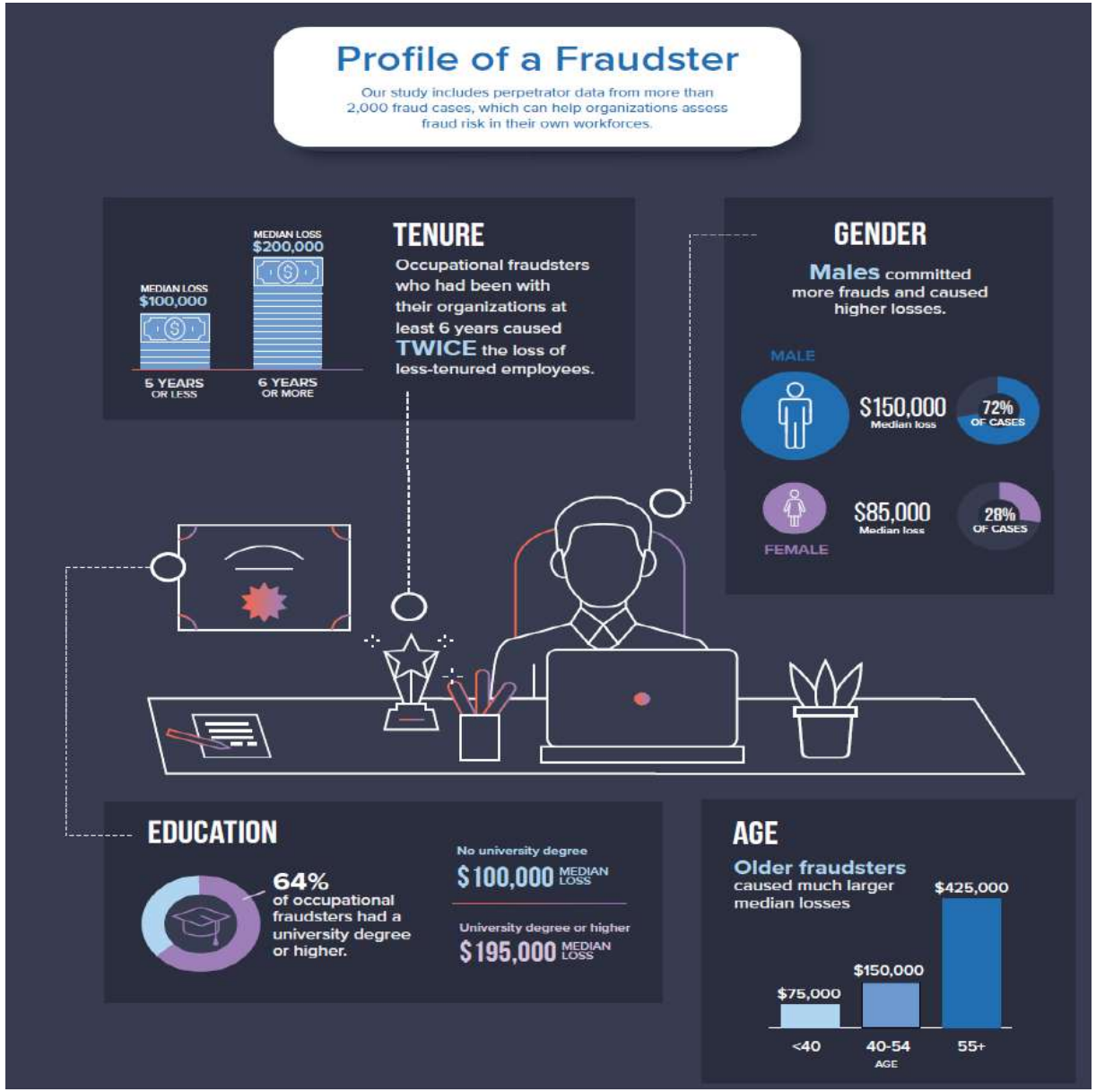




Source: 2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.

Fraud Statistics





Source: 2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.

Fraud Statistics

Behavioral Red Flags of Fraud

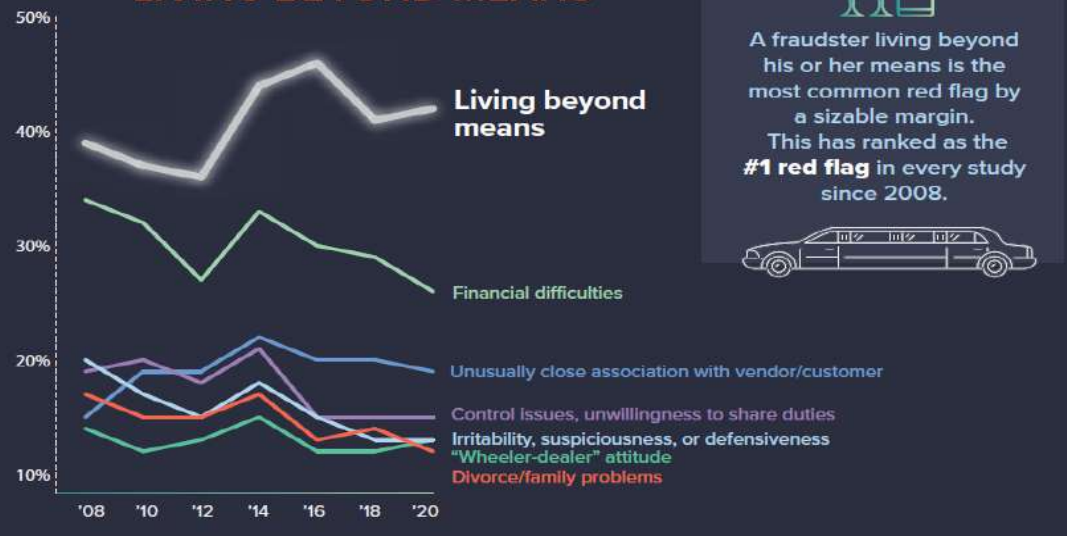
Recognizing the behavioral clues displayed by fraudsters can help organizations more effectively detect fraud and minimize their losses.

85% OF ALL FRAUDSTERS displayed at least one **BEHAVIORAL RED FLAG** while committing their crimes.

7 KEY WARNING SIGNS

42%	26%	19%	15%	13%	13%	12%
Living beyond means	Financial difficulties	Unusually close association with vendor/customer	Control issues, unwillingness to share duties	Irritability, suspiciousness, or defensiveness	"Wheeler-dealer" attitude	Divorce/family problems

LIVING BEYOND MEANS

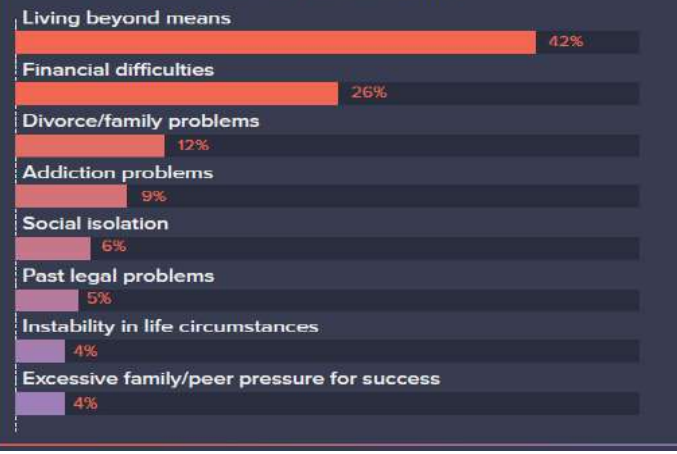


A fraudster living beyond his or her means is the most common red flag by a sizable margin. This has ranked as the **#1 red flag** in every study since 2008.

CLASSIFYING RED FLAG BEHAVIORS

In **52%** of cases, the fraudster exhibited red flags connected to their **work duties**.

In **63%** of cases, the fraudster exhibited red flag behavior associated with his or her **personal life**.



JOB PERFORMANCE AS A WARNING SIGN

A fraud perpetrator's job performance will often suffer while the scheme is taking place. Each of these performance-related issues were cited in at least 10% of cases.

- **13%** POOR PERFORMANCE EVALUATIONS
- **13%** EXCESSIVE ABSENTEEISM
- **12%** FEAR OF JOB LOSS
- **12%** EXCESSIVE TARDINESS
- **10%** DENIED RAISE OR PROMOTION

Source: 2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.

Fraud Statistics

What are the most common occupational fraud schemes in various industries?

Identifying the most common fraud schemes within industries can help organizations design controls to guard against their most significant threats. In Figure, we show the most common occupational fraud schemes in industries with at least 50 reported cases. The risks are shaded from yellow to red, with darker variants representing higher-risk areas. For example, in the health care industry, corruption represents the highest risk (40% of cases), followed by billing schemes (33% of cases).

INDUSTRY	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Banking and financial services	364	8%	10%	18%	9%	40%	8%	10%	10%	2%	2%	10%
Government and public administration	189	18%	5%	9%	4%	48%	17%	4%	17%	17%	0%	7%
Manufacturing	177	23%	5%	6%	8%	50%	20%	18%	23%	10%	2%	8%
Health care	145	33%	10%	10%	14%	40%	22%	14%	24%	15%	6%	10%
Energy	89	24%	6%	7%	6%	66%	11%	9%	25%	6%	1%	9%
Retail	89	22%	15%	15%	11%	37%	17%	6%	20%	11%	7%	15%
Insurance	82	24%	2%	5%	9%	43%	16%	11%	9%	5%	2%	6%
Education	82	30%	9%	13%	18%	30%	22%	7%	17%	13%	1%	22%
Construction	77	22%	13%	12%	17%	47%	9%	25%	13%	13%	4%	13%
Transportation and warehousing	64	13%	5%	9%	5%	52%	9%	3%	23%	6%	0%	19%
Technology	63	24%	0%	5%	6%	46%	13%	13%	22%	11%	0%	0%
Telecommunications	62	5%	2%	3%	2%	56%	5%	6%	31%	2%	0%	5%
Food service and hospitality	59	22%	20%	10%	12%	39%	8%	8%	25%	12%	10%	14%
Services (professional)	54	37%	0%	9%	20%	26%	24%	15%	11%	22%	2%	11%
Real estate	52	25%	13%	12%	21%	48%	17%	15%	12%	8%	4%	27%

Source: 2020 Report to the Nations.

Fraud Statistics

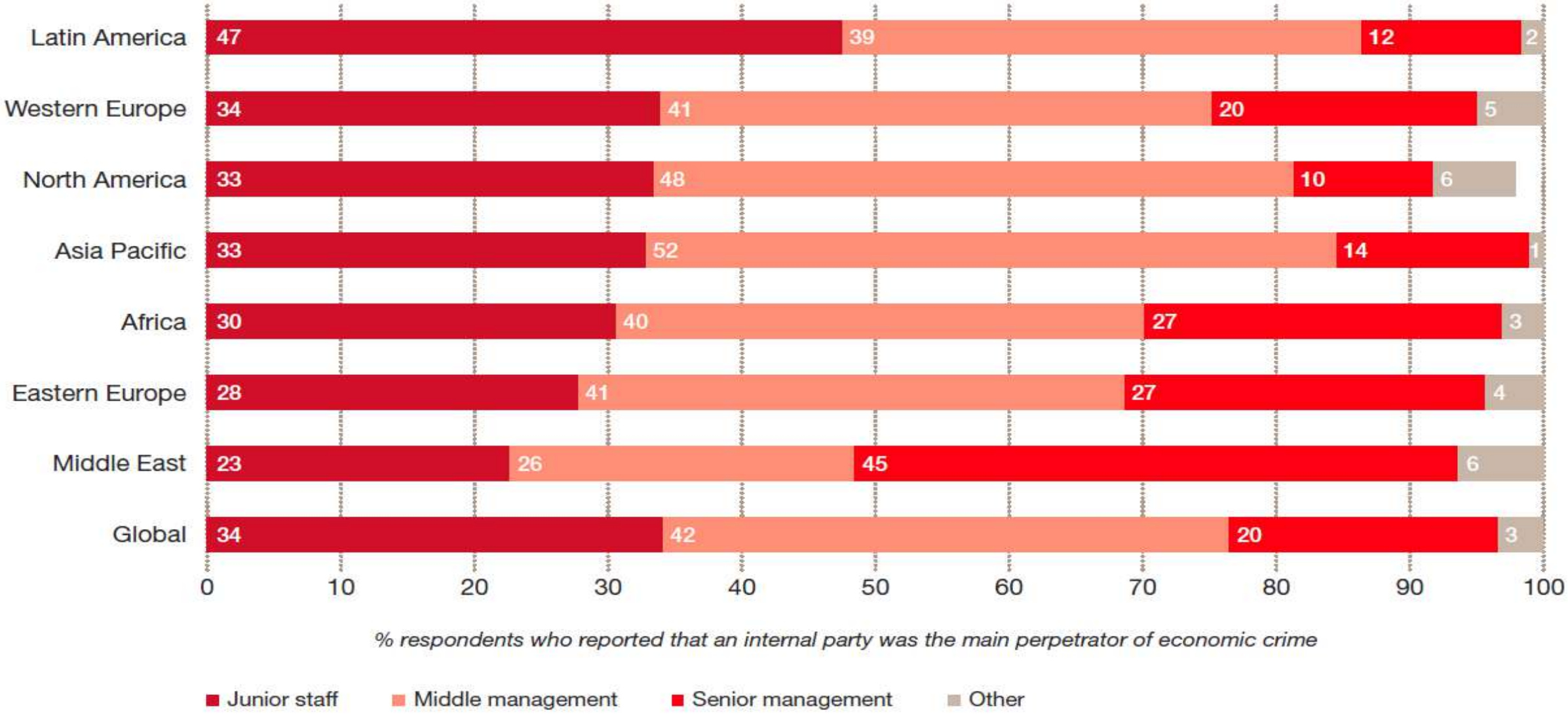
What are the most common occupational fraud schemes in high-risk departments?

The eight departments accounted for 76% of all occupational frauds in the study. The specific fraud schemes used by perpetrators in these departments are presented to help organizations assess risk and develop effective anti-fraud controls within these high-risk areas. Boxes are shaded from yellow to red, with darker boxes indicating higher-frequency schemes for each department.

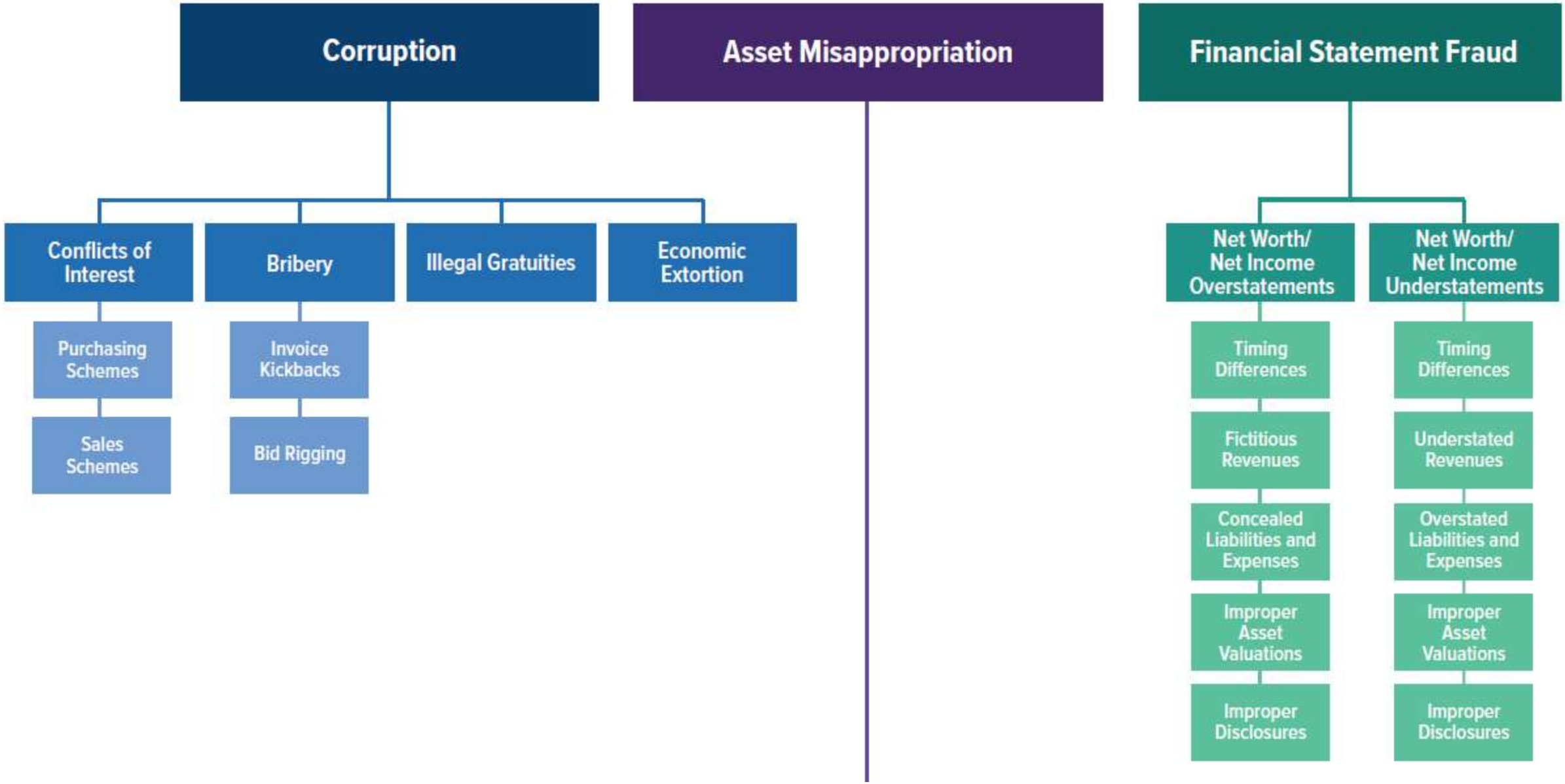
DEPARTMENT	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Operations	288	15%	5%	10%	5%	44%	12%	7%	15%	8%	3%	9%
Accounting	277	32%	14%	12%	27%	24%	18%	15%	11%	21%	5%	19%
Executive/upper management	234	26%	11%	12%	11%	62%	26%	30%	18%	12%	3%	10%
Sales	225	10%	6%	10%	5%	39%	14%	8%	21%	2%	4%	10%
Customer service	175	5%	8%	11%	8%	33%	6%	1%	9%	2%	2%	17%
Administrative support	116	31%	8%	18%	12%	29%	14%	8%	12%	9%	3%	12%
Finance	101	20%	10%	12%	9%	35%	14%	14%	12%	9%	3%	8%
Purchasing	96	22%	4%	4%	2%	81%	7%	7%	18%	2%	0%	4%

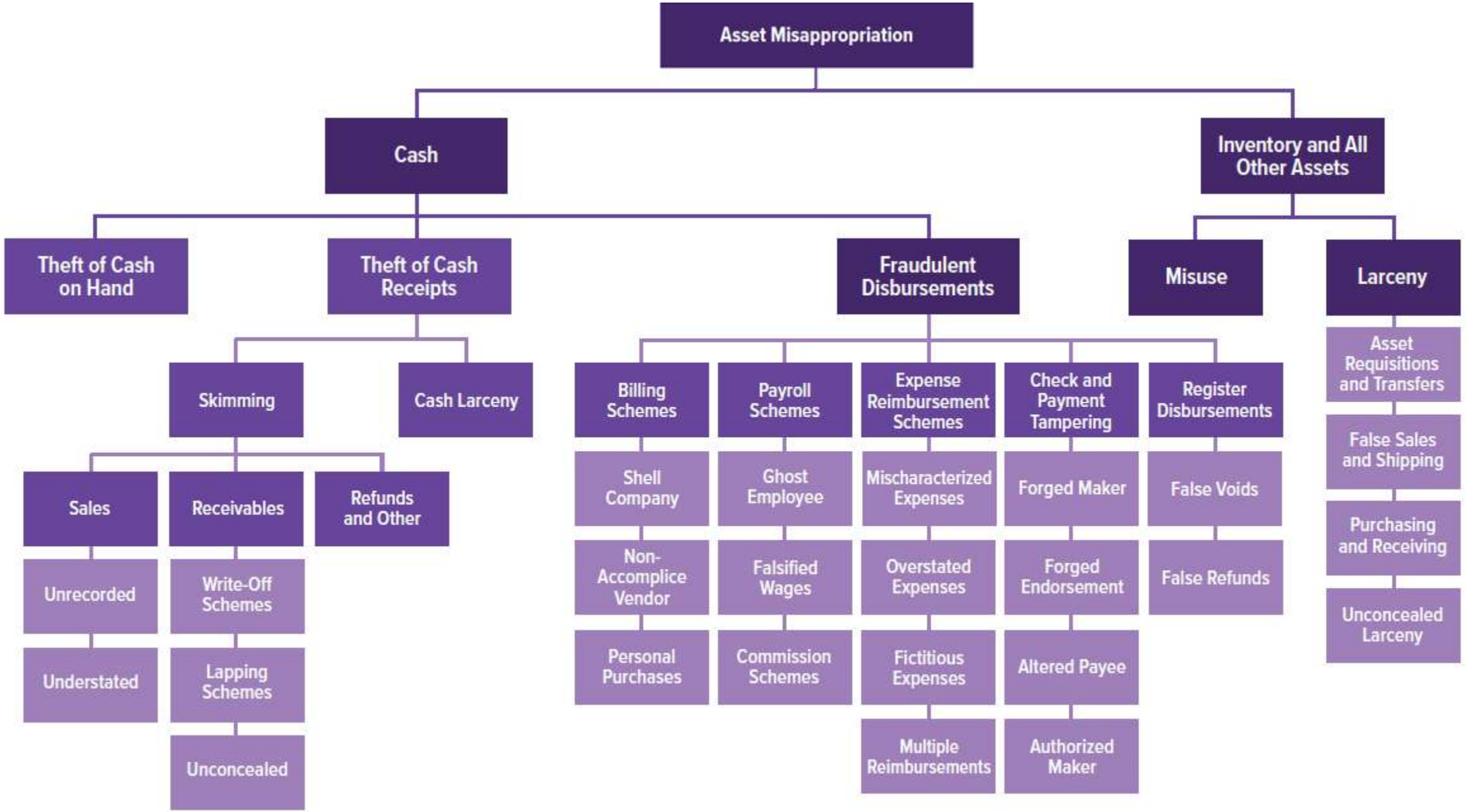
Source: 2020 Report to the Nations.

Profile of Internal Fraudsters By Region



Occupational Fraud & Abuse Classification System (The Fraud Tree)





Source: 2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.

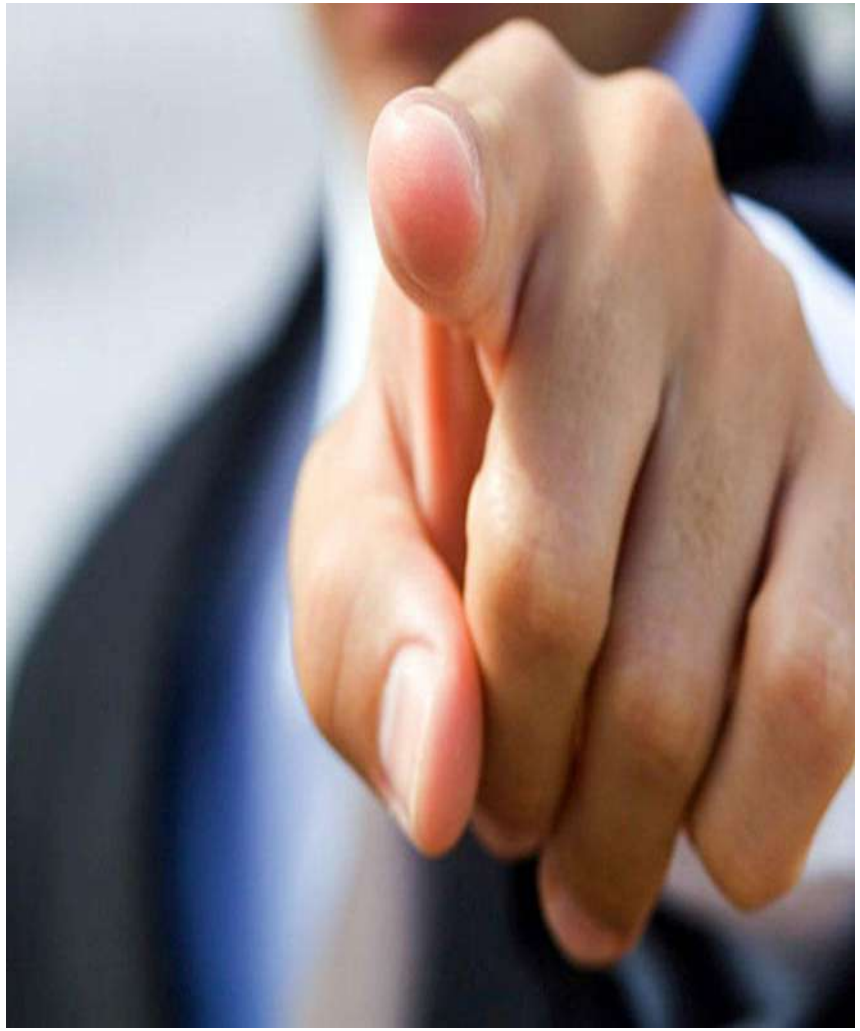
Why Focus on Fraud?

Damage inflicted by corporate fraud goes far beyond direct monetary loss. Intangible loss include;

- Poor brand reputation and public image
- Lack of business credibility
- Low employee morale and performance
- Inability to retain and attract qualified staff
- Damage to regulator relations
- Poor dividend returns/effect on share price
- An inability to meet short term commitments

Who Is Responsible To Detect Fraud?

- With increased regulatory focus and widespread negative impact of frauds, organizations are increasingly concerned about the vulnerability and exposure, and whether they are adequately protected.
- Management is responsible to implement controls and to develop a healthy tone at the top that deters fraud.
- Internal auditors are nowadays expected to have sufficient knowledge to evaluate the risk of fraud in their organizations and are required to report to the Board on any fraud risks found during their investigations. The internal auditors should have sufficient knowledge to identify the indicators of fraud.
- Internal auditors should provide objective assurance to the Board that fraud controls are sufficient for identified fraud risks and ensure that the controls are functioning effectively.



Data Analytics

You can have data without information, but you cannot have information without data.

- Daniel Keys Moran

American Computer Programmer and Science Fiction Writer

The goal is to turn data into information, and information into insight.

- Carly Fiorina
ex CEO of Hewlett-Packard

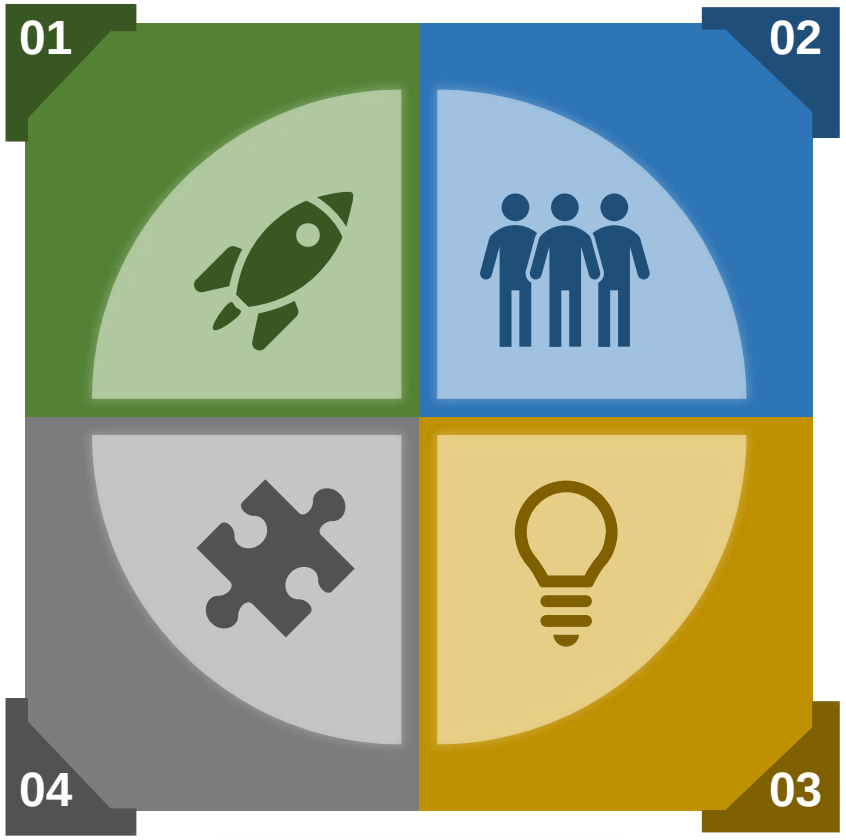
Data Analytics – How It Works?

Data Sourcing

Data sourcing starts with answering the key questions: What data to source, How and where of data quality checks, and rules and controls around how to manage and maintain the supply of data.

Data Narration & Story Telling

Creating dashboards providing exception-based reporting and alerts which helps the management in monitoring the internal process controls.



Data Analysis & Mining

Using an extract of data to search for and identify trends, exceptions, errors, or indications of potential fraud by comparing and analyzing files according to the criteria established by the auditor.

Rule Engine

identify errors, fraud, and inefficiencies by independently checking and validating transactions against specified control parameters and business rules.

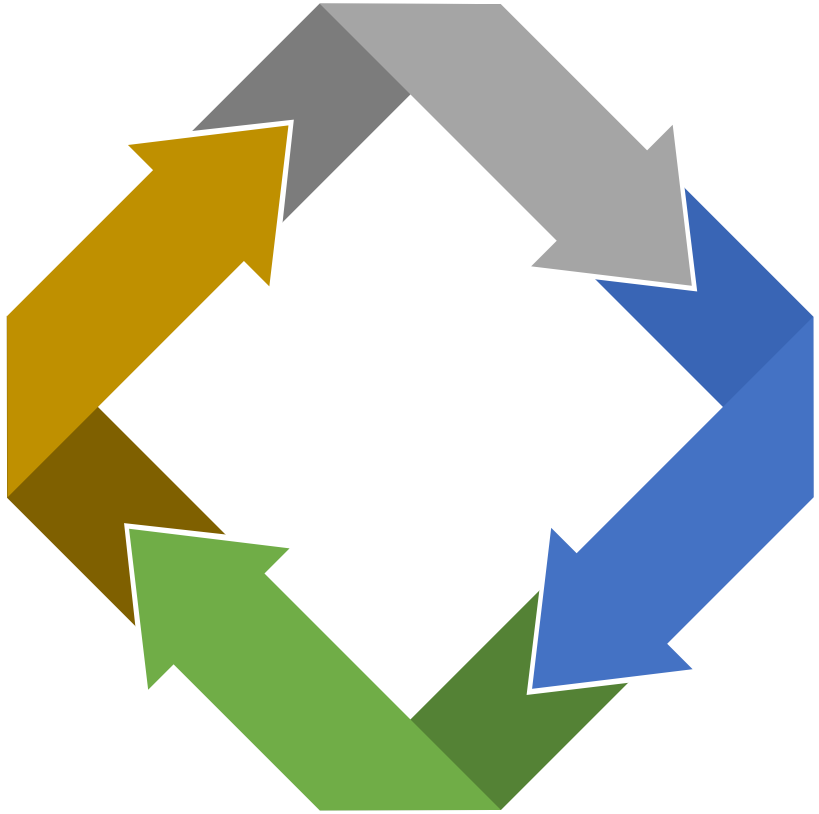
Need For Data Analytics In Fighting Frauds?

Use Advanced Technologies

- Automating Audit tests can bring down the review time.
- Less time is spent on performing analysis, more time is spent on understanding the analysis.

Perform Deeper Analysis

- Data analytics methods can be helpful in audit planning.
- Analytics helps to identify risks by analyzing data and to identify patterns, correlations, and fluctuations.



Build New Methods

- Organizations moving to agile methodologies for audit.
- More frequent cycles help audit functions contribute more flexibly and in real-time.

More Transparency

- Advanced analytics can help better understand the internal control environment.
- Use exception reporting to improve audit efficiency and detect fraud.

Types of Data Analytics

01

Descriptive

Hindsight

What happened?

02

Diagnostic

Oversight

Why did it happen?

03

Predictive

Foresight

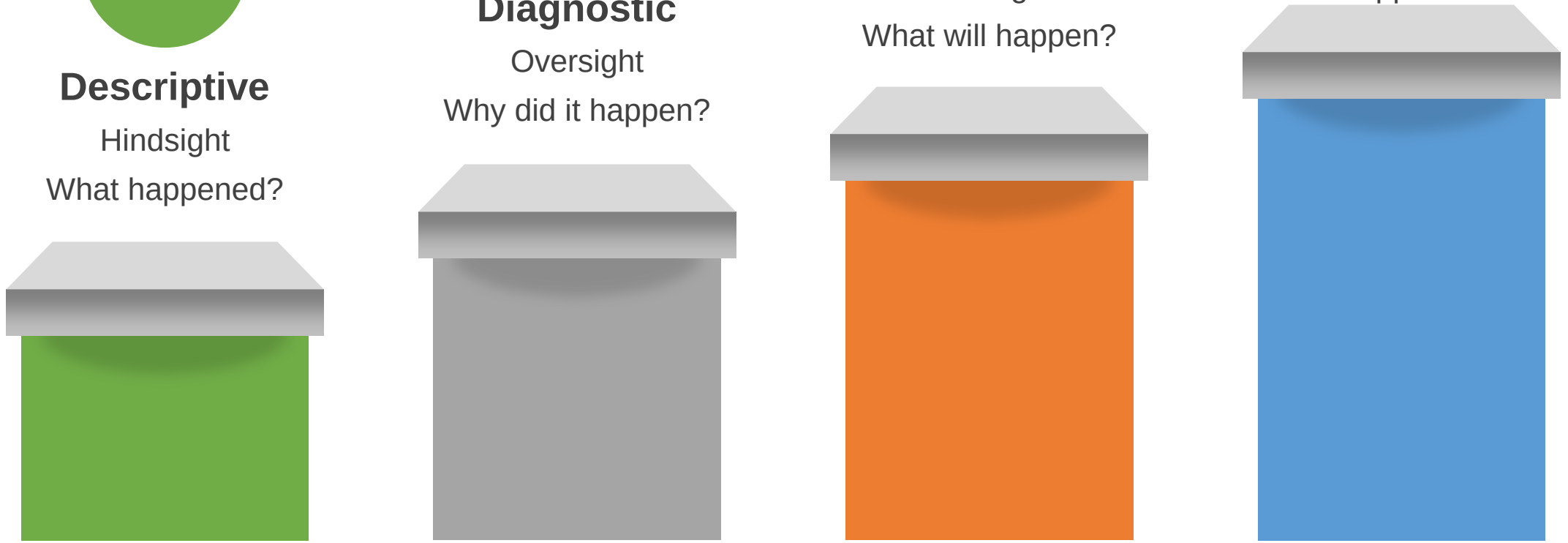
What will happen?

04

Prescriptive

Insight

How can we make it happen?



Why Sampling Is No Longer Good Enough But Using Data Analysis Is Effective For Fraud Detection

Sampling

- There are serious shortcomings with many controls testing methods like sampling.
  - You can't fully measure the impact of control failures.
  - You can miss smaller anomalies—which can result in very large frauds over time.
  - Sample testing doesn't show warning patterns.
- Although testing a sample of data is a valid audit approach but it's not very effective for fraud detection purposes. This is because fraudulent transactions don't generally occur randomly.
- To effectively test and monitor internal controls, enterprises need to analyze all relevant transactions—something that's almost impossible to do without data analytics and automation.

Data Analytics

- Test 100% transactions.
- Automate testing to ensure:
  - Continuous assessment of pain areas and scheduled repetitive monitoring of other risk areas.
  - Increased efficiencies in identifying indicators of fraud.
- Access and relate data from virtually any source.
  - Internal or external to organization & without moving sensitive data outside of the secure data center.
- Identify where automated system-based controls
  - Are not functioning effectively.
  - Do not apply to the business process (manual control).

Why Data Analytics Is Important?
Because We Are Worried About These……..

Is everything Right ?

Duplicate Payment Unusual Returns Invalid or Duplicate Supplier Master Delayed Collections Statutory Audit Findings Unauthorized Credit Duplicate Invoices Unused Credit Memos Unauthorized Journal Entries Split Purchase Orders Over-payments to vendors

Unauthorized credit Billing Errors

Inaccurate Financial Reports Supplier Fraud

Delayed Supplier Payments Incorrect Payment Terms

Unapproved or Illegal Suppliers

Unauthorized Access

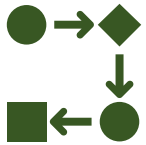
Challenges In Data Analytics

1

People

- Limited Resources
- Investment in Time & Training
- Proficiency in Using Analytics Software
- Proficiency in Performing Analysis

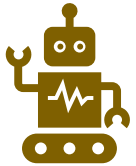
2



Process

- Objectives
- Strategy & Governance
- Measuring Success
- Pilot First

3



Technology

- Tool Selection
- Available Support
- Initial & Ongoing Cost
- Integration with Systems
- Data Consideration
- Training

4

Data

- Availability
- Accessibility
- Quality
- Format
- Centralized
- Storage
- Security

Questions We Should Ask Our Self About Data Analysis And Fraud

- Where is my highest risk of fraud?
- What indicators – if any – would I expect to see in the data?
- What systems do I need to access to highlight suspected fraud?
- Can I get access to this data?
- What techniques (matching, grouping, filtering) should I apply?
- Can I automate these analytics to drive efficiency and immediate results?

Audit Analytics Journey

Understand Data	Develop Procedures	Select Tools	Use Technology	Ideal Approach
• Understand specific data elements that are needed to support the internal audit team and its needs. • Ensure access to an accurate source of data. • Establish an audit data repository. This will help when dealing with lots of data in a complex ERP environment.	• Keep a track of the data imported and processed. This shall help in logging data flow at various stages. • Procedures should be maintained in central audit servers. • Keep a backup of the source data so that in case the base data is corrupted you have a backup available.	• The commonly known tool includes ACL, IDEA, etc. • It is important to use a tool that allows logging and scripting capability for continuous auditing. • The audit tool used should be capable of importing data from various external sources. This needs to be evaluated early to avoid any roadblocks during the later stage of the audit.	• The auditor should be aware of the limitations of tools in terms of querying, data conversion, etc. • An auditor should be able to move from working papers to an audit analytics process environment. • The results of the analysis are then linked directly back to the supporting's or working papers.	• Automation is the key value driver when utilizing audit analytics for various internal audit assignments. • Standardized and repeat audit tests, improve the efficiency, consistency, and quality of audits. • Continuous auditing and monitoring allow management to identify audit issues almost on a real-time basis.

Illustrative List of Data Analytics

Purchase	Sales	Inventory	Finance & Accounts
Purchase price variance (same material, same vendor, same week / month)	Inconsistent sales price (same material, same customer, same month, different price)	Procurement of non-moving inventory	Identify duplicate vendor bill booking / bill payment
Purchase order created with higher price while existing old purchase order is open at less price	Variation in price (sales price master vs order price vs price invoiced)	Issue / consumption of expired inventory	Suspicious journal entries by keywords
Changes to purchase order terms post release,	Incomplete / incorrect customer master data	Inventory write offs and inventory write backs	Expenses booked with backdated effect
Purchase order rate amendment post receipt of material	Sales invoicing during month end and subsequent cancellation	Analysis of negative inventory	Excessive group meal expenses
Split purchase orders	Unusual / high discount given to the customer	Non adherence to FIFO norms for inventory consumption / issue	ABC pareto analysis for expenses (period basis, vendor basis)
Single vendor dependency for high value items	Cases where 100% material returned and delay in physical receipt of material	Trend comparison of receipt quantities and issue quantities inventory item-wise	Suspicious reimbursement claims (creating duplicate claims by submitting the same expense under a corporate card transaction and an out-of-pocket transaction)
Frequent changes in vendor master data	Contribution as a percent of sales from new customers /or customers who have left	Variances in standard cost vs actual cost	Interest recovery not made for delayed payments
Identification of employee as vendor (employee-vendor match)	Identification of employee as customer	Analysis for inventory items with zero price value	ABC pareto analysis for journal vouchers, Transactions with no maker checker

What Is Red Flag?

A red flag is an indicator of a potential problem

Some Red Flags And Warning Bells

- Behavioral red flags (living the high life inconsistent with remuneration)
- Employees with unusual work habits - not taking leave
- Close ties and nexus with vendors, third-parties etc
- The unidirectional trend in errors
- Non-rotation of duties
- Concentration of power in one or group
- Missing documents, alteration, destruction & overwriting
- Unreconciled accounts

Sample Red Flags

Area	Red Flags
Procurement	• Long term vendors are suddenly no longer used. • Unusually high volumes of business with a particular vendor – especially a new vendor. • The sudden jump in complaints by vendors of exclusion from the bidding process. • Circumvention of bidding rules & procedures. • Prices for goods or services see a sudden jump. • Contract change orders lack sufficient information. • Purchasing exceeds the budget, significant increases in expenses and accounts payables. • Sham corporations.
Vendor's Entity Verification	• Supplier and employee with matched names, addresses, telephone numbers, email addresses, fax numbers, etc. • Suppliers based in potentially unusual locations. • Unusual or unexplained changes in vendor master file. • Trading pattern shows renewed activity after a dormant period.
Vendor's Unusual Invoices	• Low and / or sequential invoice numbers of supplier's invoice numbers indicating supplier is overly dependent on our company. • Invoices, which are "round sum" values such as Rs.50,000, Rs.500,000, etc. By looking at the supplier and the type of service they provide, ask yourself the question "is this reasonable?" • Invoices that are not matched to purchase orders. • Vendor invoices that have no telephone or company registration number; have unusual looking address (residential address); are sent from different companies but look suspiciously similar in format and layout; contain vague or incomprehensible descriptions of the goods or services provided; have been manually altered.

Sample Red Flags

Area	Red Flags
Financial Statements	• Delay in finalization of accounts. • Frequent changes in accounting policies. • Continuing losses. • An overdraw of loans and advances. • Higher cost per unit of production. • The high number of losses or wastage shown in books vs. norms. • High investment in group companies. • Profit not supported by increased cash availability.
Banking Transactions	• Funds transferred from the company's bank account to the employee's personal bank account (exception is reimbursements). • Manipulation of the accounting entries showing payments made to employee's own entities posted as bank charges / commission / LC charges etc. Sometimes even posted as payment to company's other vendor etc.
Others	• Accounts receivable balances overstate the amounts that can be realistically collected from customers. • Significant unreconciled variances in the bank reconciliation and/or accounts receivable reconciliation. • Significant increase in fixed asset adjustments or inventory adjustments. • Significant or unusual fluctuations in depreciation expense. • Unusual amounts in estimates of accruals. • Significant variations in liability and purchase amounts against previous periods and budget. • Significantly underspent at the halfway point but fully or overspent at the end of the year.

Data Analysis Techniques


“DATA WILL TALK TO YOU IF YOU’RE WILLING TO LISTEN TO IT.”
- JIM BERGESON

Benford's Law

- Benford's Law states that if we randomly select a number from a table of physical constants or statistical data, the number 1 as a first digit of a number will appear 30.1% of the time while the number 9 as a first digit will appear only 4.6% of the time. Benford also developed a distribution of frequencies for second, third, and fourth digits.
- Using data analysis, you can see artificial highs or lows within your data that could be indicators of fraud, and then you can drill down and investigate further. The idea is to test certain points and numbers and identify those that appear more frequently than they're supposed to.
- Benford's Law is particularly useful for detecting purchasing and accounts payable fraud. Other suitable areas include:
  - Journal entries
  - Accounts payable transactions
  - Customer/client refunds
  - Purchase orders
  - Loan data

Position of Digit in Number				
Digit	**First**	**Second**	**Third**	**Fourth**
0		0.11968	0.10178	0.10018
1	0.30103	0.11389	0.10138	0.10014
2	0.17609	0.10882	0.10097	0.10010
3	0.12494	0.10433	0.10057	0.10006
4	0.09691	0.10031	0.10018	0.10002
5	0.07918	0.09668	0.09979	0.09998
6	0.06695	0.09337	0.09940	0.09994
7	0.05799	0.09035	0.09902	0.09990
8	0.05115	0.08757	0.09864	0.09986
9	0.04576	0.08500	0.09827	0.09982

Trend Analysis

- Trend analysis is the idea that what has happened in the past will give insight into what will happen in the future.
- Using trend analysis, you can examine the general ledger balance over time. Once you expect what will happen, compare the trend to the expectation. If the trend doesn't meet the expectation, you can determine why.
- The period-to-period change method is the simplest type of trend analysis. For example, you project data into the future (e.g., month or year) based on data from two or more prior periods, and then you measure the outcome in values or percentage change.
- Predictive analysis from both trend analysis and time series can be used in a continuous monitoring environment.
- The analysis can help provide a forecast, and that data can then be compared to the actual data immediately after the event. Any difference between the two indicates that the data has diverged from its past trend, meaning a change of some kind must have occurred. Further investigation may reveal that this change was intentional/malicious.

Ratio Analysis

- Another useful fraud detection technique is the calculation of ratios for key numeric fields.
- Like financial ratios that give indications of the relative health of a company, data analysis ratios point to possible symptoms of fraud. Three commonly employed ratios are:
  - Highest value to the next highest (Relative size factor)
  - Highest value to the lowest value (maximum / minimum)
  - Current year to the previous year.
- In many cases, high ratios or abnormal values that deviate from industry standards and/or current business scenarios, have often unearthed potential frauds that need to be investigated.

Relative Size Factor Test

- In the relative-size factor test, a ratio is computed. The largest number in the data set is divided by the second-largest number. This test is often used in the accounts payable area.
- Suppose the highest accounts payable amount paid to vendor X for January is INR 50 lakhs and the second highest payment is INR 40 lakhs. This would result in a relative-size-factor ratio of 1.25 for January. In February, however, this same relative-size-factor test yields a ratio of 12.5 (INR 500 lakhs highest payment divided by INR 40 lakhs second highest payment). Obviously, this large change in the ratio needs to be investigated. You may discover that a decimal point was inadvertently moved one place to the right, resulting in INR 500 lakhs rather than INR 50 lakhs payment.

Ratio Analysis (Case Study)

- ABC Fashions Inc. owns and operates retail clothing stores for women nationwide. The company builds and maintains all its retail stores. Each store manager is authorised to spend up to Rs. 50,000 per quarter on store maintenance. These expenditures include things such as repairing broken store windows, and fixing air conditioning and heating problems, roofing problems, plumbing problems, etc. The maintenance expenditures are captured store by store.
- In 2019, to establish a benchmark or baseline data, the internal auditors of ABC Fashions Inc. decided to analyse the maintenance expenditures using digital analysis. During their analysis they had determined the pattern of the typical distribution for maintenance expenditures per quarter per store:
  - 30% of the expenditures ranges from Rs 1 to Rs 1,250;
  - 50% of the expenditures ranges from Rs 1,251 to Rs 2,500;
  - 15% of the expenditures ranges from Rs 2,501 to Rs 3,750; and
  - 5% of the expenditures ranges from Rs 3,751 to Rs 5,000.
- In 2020, a further analysis of maintenance expenditures across all stores revealed that one store had 47 percent of its maintenance expenditures in the Rs 1 to Rs 1,250 range.
- This store was scheduled for an internal audit visit. Suspecting fraud, the internal auditors included a Chief finance executive on their audit team. The Chief finance executive's investigation revealed that the store manager was participating in a kickback scheme with her brother-in-law who owns a heating and air conditioning company.
- Without the digital analysis of the maintenance expenditures account, this fraud possibly would have never come to light.

Duplicate Transactions

- Duplicate testing is one of the more common fraud tests because it can indicate fraud as well as inefficiency and inaccuracies in transactions.
- Running tests for duplicate transactions can determine if for example, you're getting duplicate invoices from somebody—and whether it's deliberate or accidental.
- Ordinarily, invoice-number/vendor-number combinations are unique. So, transactions with the same invoice-number / vendor-number combinations would be an unexpected data pattern. Duplicate transactions could be a possible symptom of fraud that should be examined. But a word of caution: you should properly investigate the transactions before jumping to conclusions. Transactions that look like duplicates may simply be progress payments or equal billing of monthly charges.
- Duplicate payments in most cases may not be fraud-related but continue to be a significant accounts payable weakness that is both preventable and recoverable.
- Duplicate invoice numbers could indicate that invoices have been paid twice, either accidentally, or intentionally. A fraudster could be processing these invoices and paying the money to themselves or working with somebody at the vendor company to share the proceeds from the duplicate payments.

Even Amounts

- People who commit fraud often create invoices with rounded amounts, which are invoices without pennies. Even (rounded-Rupee) amounts does not happen that often. So, numbers that are rounded to tens, hundreds, and thousands might be considered anomalies and should be looked at more closely.
- Don’t just focus on the large Rupee amounts. Even small amounts should be reviewed because these are generally easier for fraudsters to get away with. For example, consider reimbursement of travel expenses. Your organization will have maximum daily amounts for travel, meals, gas, etc. It’s most likely that these amounts are set in rupee amounts (e.g., Rs1000 for dinner, Rs 6000 per night for accommodation). To ensure that these maximums aren’t abused, the claims should be checked against receipts. It’s very uncommon, for example, for a hotel room to come to a rounded figure with taxes included. But if you’ve got hundreds of employees and they’re all making expenses claims, that’s thousands of expenses to analyze and confirm that the amounts are legitimate, which can’t be done manually.
- Try to rank your vendors by those with a high percentage of rounded amount invoices. To do this, just calculate each vendor’s number of rounded amount invoices and divide it by the total number of invoices for that vendor, obtaining the percentage. Then rank by descending percentage to review the most suspicious vendors first.
- Data analysis software allows users to identify rounded-rupee instances in the data, so you can investigate these further and ensure that claims match the data.

Last-Two Digit Test

- The last two digits test is another example of how digital analysis can be used.
- According to Benford's Law, as one investigates the far-right digits of a number (that is, the third and fourth digits) there's an approximately equal probability of each far-right digit occurring.
- For instance, the last two-digit combinations of 00, 01, 02 through 99 have approximately a 1 percent chance of occurring. If the data set shows a last two-digit distribution different from this expected 1 percent pattern, then you may need to do a follow-up analysis.
- For example, assume the last two digits, 00, occur 4 percent of the time in the data set. This could indicate that there's excessive rounding taking place.
- If the last two digits, 99, appear more than expected in the data set, employees may be trying to avoid a pre-set Rupee limit.

Other Analysis

Ducking Authorization Levels

- Sometimes managers concentrate their purchases just below their authorisation levels, so their choices won't be scrutinized.
- Managers with Rs 10,00,000 purchasing levels authority might have a lot of invoices for Rs 9,00,000 to Rs 9,99,999, which would show up in data analysis by spikes for first three digits at 900 and 999.

Biases in Corporate Data

- In one company's accounts payable data, there was a large first two-digit spike (excess of actual over expected) at 24.
- An analysis showed that the amount $24.50 occurred abnormally often. The audit revealed that these were claims for travel expenses and that the company had a $25 voucher requirement.
- Employees were apparently biased toward claiming $24.50.

If you torture the data long enough, it will confess to anything.

RONALD COASE

Case Studies

Corporate Scandals – Satyam Computers

- Chairman Ramalinga Raju admitted falsifying accounts.
- Of the stated, 755 million euros in Satyam’s cash and bank balance 710 million euros were non-existent.
- There were multiple red flags that the auditors could have caught upon. A simple check with the banks would have revealed that the cash and bank balances were overstated.
- Statutory auditors was accused of negligence in auditing Satyam in the 8 years previously, as the company grew from a handful of people to 53,000 workers in 66 countries.
- Mahindra Group's IT arm, Tech Mahindra, purchased a major stake in the company and in June 2009 the company renamed itself Mahindra Satyam. Later it was merged into Tech Mahindra.

Corporate Scandals – Siemens AG

- Siemens paid penalties of US$ 1.6 billion for paying bribes of US$ 805 million to foreign officials to obtain large telecommunications and infrastructure contracts in Iraq, Argentina, Nigeria, Iran, Tunisia, Vietnam & Bangladesh.
- The investigation found questionable payments of roughly US$ 1.9 billion from 2002 to 2006 that have triggered a broad range of inquiries in Germany, the United States, and many other countries.
- Once inquiries commenced, Siemens replaced all top leadership positions.
- Siemens has tightened its internal controls and implemented strict compliance and anti-corruption measures throughout the company.

Corporate Scandals – Wake County Transportation

- In 2006, employees of the Wake County School Board in Raleigh, North Carolina, conspired with suppliers to divert over US$ 4.8 million using fraudulent invoices to receive various kickbacks.
- The scheme succeeded despite apparently strong internal controls, such as a bid limit of US$2,500.
- The School Board employed only one internal auditor. Although the auditor had audit software that should have easily detected these unusual patterns, it was either not used or misapplied.
- There were numerous red flags that were not noticed.

Corporate Scandals – Walmart

- Modus Operandi was Walmart paid bribes to several third-party intermediaries (TPIs) to get necessary approvals.
- Walmart failed to implement sufficient internal accounting controls related to anti-corruption. Through these operations, Walmart was able to retain third-party intermediaries (TPIs) that made improper payments to government officials to obtain store operating permits and licenses. e.g.: Walmart was funneling of US$ 500,000 in a Brazilian company, to get construction-related approvals.
- Accounting lapses were Walmart falsely recorded improper payments in joint venture books. They used vague descriptions like "misc. fee”, "miscellaneous“, "professional fee“, "incidental" and "government fee“.
- The company repeatedly failed to take red flags seriously and delayed the implementation of appropriate internal accounting controls.
- Legal repercussions was US$ 282 million (approx. Rs 1,962 crore) as a fine for violating the Foreign Corrupt Practices Act (FCPA) in India, China, Mexico, and Brazil.

Strengthening Internal Controls And Processes To Prevent Fraud

Abraham Lincoln said:

"If I had six hours to chop down a tree, I'd spend the first four hours sharpening the axe".

Review Points

Companies should adopt technology that helps them in making their counter-fraud response comprehensive and effective. With fraudsters becoming more sophisticated, and global data increasing at exponential rates, data analytics, machine learning, artificial intelligence is now more than ever, a critical tool to deal with increasing levels of global fraud.

By embedding technology tools in every stage of the audit process and mining the vast repositories of data available (both internal and external), auditors can deliver unprecedented real-time insight, as well as enhanced levels of assurance to management and audit committees. Data analytics can be used on structured and unstructured data across multiple processes. There is an increasing number of analytics tools built for fraud management. Further, They should base their choice on the six fundamental pillars of organizational change:

- Culture – creating a culture that beats fraud and corruption.
- Capability – Study history of fraud – Around since the beginning of time. Study the types of fraud happened – More ways than we can imagine. List down risks. Identify what internal controls we have against risks. Define risk mitigation plan to strengthen controls to ensure that the range of counter-fraud measures or benchmarks is appropriate to the range of fraud risks.
- Capacity – deploying the right level of resources to deal with the level of fraud risk.
- Competence – making sure that the team has the right skills and standards.
- Communication – raising awareness, deterring fraudsters, sharing information and celebrating successes.
- Collaboration – working together across internal and external boundaries and leveraging the knowledge of colleagues, other local authorities to speed up the investigation.

THANK YOU

DHANYAWAD

धन्यवाद