Duarte Trigueiros

Fraud Prevention and Detection: Methods, Technologies and Vendors

An introductory manual

Master in European Studies Association, Macau

Duarte Trigueiros

Fraud Prevention and Detection: Methods, Technologies and Vendors

An introductory manual

Master in European Studies Association, Macau

2016

Book Sheet / Ficha Técnica

Booktitle / Título: Fraud Prevention and Detection: Methods, Technologies and Vendors - An Introductory Manual

Author / Autor: Duarte Trigueiros

Editor / Editado por: Master in European Studies Association, Calçada do Gaio n. 6, Macau

Illustrations / Ilustrações: Soluções Criativas, Lda.

Book Cover / Capa: Soluções Criativas, Lda.

Book Drawing / Tiragem: 500 copies

Printing and Finishings / Impressão e Acabamentos: Welfare Printing Company, Lda.

Printing Date / Data da Impressão: November 2016

Legal Deposit / Depósito Legal: Central Library of Macau, 2016

ISBN 978-99965-689-0-9

FRAUD PREVENTION AND DETECTION: METHODS, TECHNOLOGIES AND VENDORS

The introductory manual on "fraud prevention and detection: methods, technologies and vendors" offers an opportunity to:

1. increase awareness of the different types of strategies and procedures followed by organizations to prevent and detect fraud;
2. acquire a better understanding of analytical and technological procedures used to the same end;
3. critically evaluate claims made by vendors of Information Technology (IT) solutions and the relationship between costs and benefits for the organization when such solutions are implemented.

The initial chapters of the manual contain a comprehensive view of the different types of fraud and how fraud is prevented and detected in organizations. Then, the manual focuses on the existing IT solutions for fraud detection, discussing their pros and cons.

Complementary readings are suggested, commented and referenced.

Acknowledgement: the publication of this manual was made possible with the generous support of the Macau Foundation.

Macau, 29 of October 2016

Contents

Chapter 1: Introductory notions

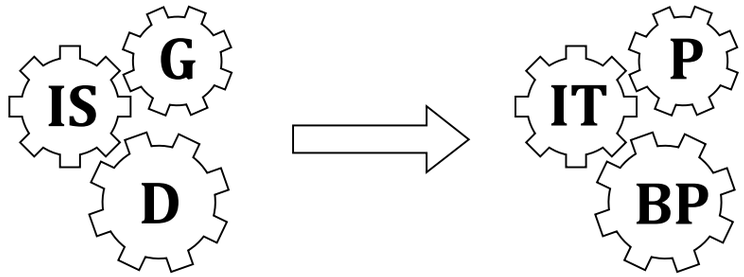
According to the “Better Practice Guide” of the Australian National Audit Office (2010), fraud may be defined as “dishonestly obtaining a benefit by deception or similar means”. The use of deception or trickery and the attempt to hide the dishonesty for as long as possible are the two major characteristics of fraud. The benefit obtained using fraud is not restricted to monetary or material benefits, and may be tangible or intangible. The benefit may be obtained by a third party rather than, or in addition to, the perpetrator of the fraud.

The initial chapter of this manual is dedicated to describing management procedures aimed at preventing fraud within an organization. The first and most basic principle to be understood is that successful fraud control is never the result of isolated actions. Fraud control cannot be confined to a specific activity. It requires the involvement of the whole organization.

More than in other areas of concern, fraud prevention and detection illustrate the unavoidable interactions which exist, in organizations, between the following three factors: management strategy and practice, governance structure and rules, and the use that is made of Information Technology (IT)-based solutions. This manual highlights such close connections, shows the strong points of IT, explaining why some of the claims made by IT vendors may be misleading, and stresses the integrated nature of success against fraud.

Fraud control management

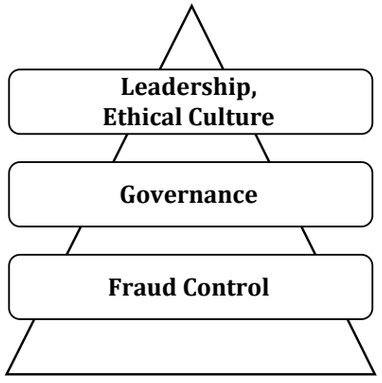
We call “fraud control” to the business process (BP) leading to a reduced, acceptable level of fraud across all activities of an organization; and to the continuation of such acceptable level. Business processes rely on people (P) and on IT for the pursuing of their goals. In the case of fraud control, however, the decisive factors leading to successful IT-based fraud control are shown in this manual to be Governance (G), the availability of historical data (D) and the appropriate use of Intelligent Systems (IS) in tasks such as the mining of transaction files or as complex models capable of detecting suspect patterns.



Any business process aiming at an effective fraud control within the organization must encompass three requirements:

1. Leadership and ethical culture
2. Governance
3. Fraud control strategies and procedures.

Fraud control procedures are just the operational level of a hierarchy where leadership is committed to an ethical culture in the organization. At the middle level of this hierarchy, stands the set of good-quality, clearly stated, well-known governance rules and principles. These are the indispensable upper levels of any effective fraud control.



In other words, effective fraud control requires a decided commitment from the top, together with an ethical culture which must become pervasive inside the organization. Prevention and detection procedures (that is, the fraud control operations) are of little use when there is no strategic commitment to fraud control and no governance structure to support it.

Leadership and ethical culture

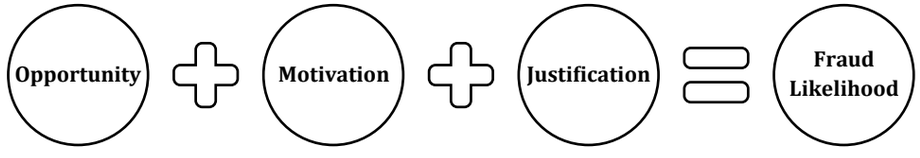
The key leadership and ethical culture points to consider are:

1. Strong executive leadership in support of fraud control policies and management
2. If staff perceive that controls to respond to fraud are not robust or supported by management, they are much less inclined to report their observations or suspicions.
3. The establishment of an ethical culture is a key element of sound governance and plays an important role in preventing fraud and helping to detect it once it occurs.

Governance rules and structure

Effective fraud management requires, as mentioned, an overall governance structure that reflects the operating environment of an organization. When developing or maintaining a fraud control governance structure, organizations need to ensure that they have considered, and made to be reflected in specific governance rules, the three conditions for fraud to occur. Such conditions are widely accepted as being:

1. an opportunity (that is, poor internal and external controls)
2. a motivated individual, namely a person with serious money problems;
3. a justification in the part of an individual for the fraudulent activity



Here are a few typical examples:

- Opportunity - poorly secured supplies or equipment, access to corporate checkbook, unchecked petty-cash register.
- Motivation – acutely needs cash for some reason.
- Justification - passed over in a promotion, having been put aside, quarrels.

Opportunity is the first, indispensable condition for fraud to occur. Fraudsters are, in the majority of cases, normal, honest persons who discovered an opportunity and took advantage of it. It should be made clear from the onset that normal people are not born criminals yet they will commit fraud if they can do it and are hard pressed by difficulties. Or, in other words, all persons are potential criminals given an opportunity, coupled with dire need of money.

What leads someone to attempt a crime is the existence of an obvious, easy and apparently innocuous way of committing such crime. In the first place, therefore, fraud control measures need to focus on restricting the level of opportunity available to commit fraud, through the development and implementation of pervasive and efficient fraud control procedures.

Motivation consists, in most cases, of an acute lack of resources, an approaching catastrophe caused, for instance, by gambling and other debts, by health problems of a close relative together with the lack of means to access medical aid, by unemployment and other causes. Persons with a comfortable prospect regarding money do not, in general, commit petty fraud.

Finally, justification is a kind of moral support to take revenge or to get what a person considers his or her right. Past actions such as being passed over in promotions, being placed in a "shelf" or being the target of unkind, offensive actions in the part of superiors.

An individual's propensity to commit crime is, in general, not related to personality and other characteristics. Fraud is the result of the situation, social bonds within an organization and pressing, external factors.

Also, criminality is not connected to any specific class in society. Well-off persons may not commit petty fraud yet they will succumb to the allure of corruption and its connections to power, or to ego-gratifying tax-evasion schemes.

In what concerns crime, there are two types of perpetrators:

- calculating or predatory and
- situation-dependent

Calculating perpetrators want to compete and assert themselves, are inclined to taking risks, lack feelings of anxiety or empathy. A culture based on competition promotes and justifies the pursuit of material self-interest, often at the expense of others and even in violation of law. Thus competition is in the origin of cheating among children (in school activities and in sports) and, for the same basic reasons, it may promote fraud among the modest and the prominent, among the rich and the poor.

Situation-dependent criminals, on the contrary, are ordinary people with no intent to harm others. Most of the frauds are perpetrated by this second group.

Governance rules and structures are critical to the operation of fraud control, to support the role of the board of directors (BOD) and that of the executive management (CEO) and to ensure compliance with the guidelines enacted within the organization regarding fraud. Governance structures in particular, must be well understood and accepted by all.

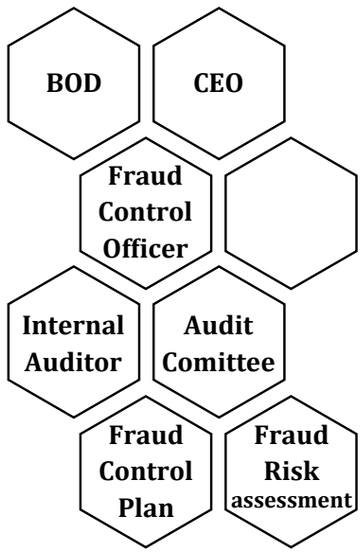
According to the "Better Practice Guide" of the Australian National Audit Office (2010), governance may comprise, in the case of large entities,

1. Fraud Control Officer,
2. Internal Auditor,
3. Audit Committee

And there should be in place a Fraud Control Plan together with a Risk assessment study.

An audit committee plays a key role in securing and enhancing awareness of fraud control, including reviewing management's approach to new and emerging risks during periods of significant change, such as the implementation of new policies and programs.

A typical governance structure should include the following elements closely linked:



The internal auditor has the responsibility for managing the risk of fraud. The responsibility for managing all types of risks rests with management as part of its ongoing responsibilities. However, internal audit can assist an entity to manage fraud control by advising on the risk of fraud and the design or adequacy on internal controls. It can also assist in detecting fraud by considering fraud risks as part of its audit planning and being alert to indicators that fraud may have occurred.

Internal audit provides an independent and objective review and advisory service to:

a. provide assurance to the CEO / BOD that the financial and operational controls designed to manage risks and achieve the entity's objectives are operating in an efficient, effective and ethical manner
b. assist management in improving the entity's business performance

Internal audit can also assist in managing fraud control by providing advice on the risk of fraud, advising on the design or adequacy of internal controls to minimize the risk of fraud, and by assisting management to develop fraud prevention and monitoring strategies.

An effective internal audit plan should include a review of those fraud controls designed to address the significant fraud risks faced by an entity. The audit committee provides independent assurance and advice to the CEO / BOD on operations, their control and observance of statutory or legal requirements.

Audit committee: key responsibilities of an audit committee include:

1. risk management
2. the internal control framework
3. external accountability (including financial statements)
4. legislative compliance
5. internal audit
6. external audit

In relation to fraud control, audit committee's responsibilities include:

1. reviewing risk management procedures for the identification and management of financial and business risks, including fraud risks
2. overseeing the process of developing and implementing the fraud control plan, to provide assurance that appropriate processes and systems are in place to prevent, detect and respond to fraud-related information

Fraud control lifecycle

Fraud control requires the implementation of a number of key control strategies which contribute to effective fraud control. The strategies are grouped in four key phases forming the Fraud Control Lifecycle:

a. Fraud prevention involves those strategies designed to prevent fraud from occurring in the first instance;
b. Fraud detection includes strategies to discover fraud as soon as possible after it has occurred;
c. Fraud response covers the systems and processes that assist an entity to respond appropriately to an alleged fraud when it is detected; and

d. Fraud monitoring, reporting and evaluation provide assurance that responsibilities are being met and promote accountability by demonstrating compliance with fraud control strategies.

Prevention **Detection** **Response** **Monitoring**

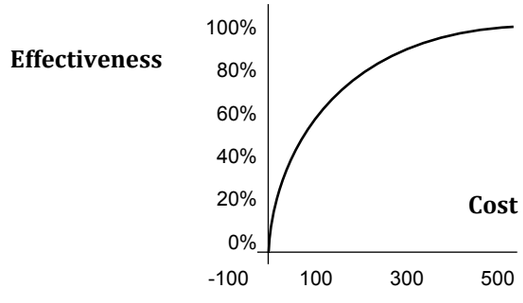
These strategies are interdependent and subject to a cyclic process of review and enhancement. Each strategy must be subject to active management within an organization. Senior executive oversight -- through sound governance -- will ensure that each strategy does not operate in isolation, and that interdependencies are effectively identified and managed.

Control effectiveness versus control cost

Fraud control inevitably increases non-productive costs in three ways:

1. Directly by requiring the extra use of technology and employees in order to perform the mentioned four control strategies
2. Indirectly by reducing operational performance
3. Costs arising from the negative effect of control on customer satisfaction

Strategic decisions must be taken in order to find an appropriate balance able to avoid excessive, costly control, without increasing fraud exposure significantly. While defining such balance it is worth bearing in mind the Pareto Principle, according to which the relationship between the effectiveness of fraud control and associated costs is nonlinear: the initial 50% of fraud cases are easy to prevent; the next 25% will take the same effort; the next 12.5% will take the same effort and so on. Thus fraud prevention will never be 100% effective.



Moreover, resources available for fraud control are limited. Organizations need to plan at both strategic and operational levels to best meet its responsibilities within its allocated resources and budget. This means planning the implementation of fraud control activities based on priority areas in terms of success or otherwise, in meeting its primary objectives.

The type and quantity of fraud controls that can be established depend on the objective of the fraud control program and the mechanisms it uses to achieve its aim. The table below, taken from the "Better Practice Guide" of the Australian National Audit Office (2010), provides some examples of fraud controls that could be used in each phase of a fraud control program.

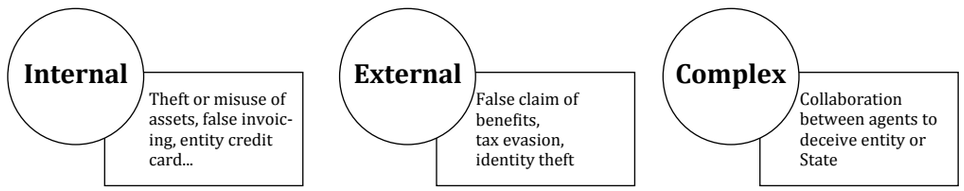
Phase of a fraud control program	Examples of fraud controls to implement
Policy development, program design and business case	• Fraud risk assessment • Fraud control plan • Employment screening • Communication and awareness
Procurement strategy	• Rigorous and transparent tender processes • Screening of potential suppliers and customers • Segregation of duties on selection and approval of procurements
Delivery / implementation / management	• Regular supplier reviews (includes surprise audits) • Data mining / analysis • Internal and external reporting mechanisms (hotlines, website, internal reporting channels) • Response to identified / reported frauds • Management / internal audit review of internal controls
Closure	• Management / internal audit review of program closure and expenditure of final monies

Fraud classification

There are several possible ways of classifying fraud but just a few are of any practical interest. The most common are classification by origin, by magnitude / frequency and by target.

By origin frauds are usefully classified as

1. internal to the entity, when they are committed by an entity's staff
2. external to the entity, when fraud is committed by persons external to the entity
3. collaboration between internal and external parties



By magnitude / frequency, frauds are classified as

1. Occupational: relatively small, frequent, internal frauds, committed by staff
2. Large, non-frequent, internal frauds, committed by management
3. Endemic: relatively small, frequent, external frauds

The most general and indeed useful fraud classification is by origin. For example, occupational fraud can further be classified as:

Asset misappropriation	Corruption	Financial Misstatement
• Cash • False Invoicing • Payroll ...	• Accepting bribes • Exchanging favors • Nepotism	• Earnings manipulation • Liabilities hiding

The above are indeed the most common types of occupational fraud.

Each of them has its own, characteristic risk pattern: asset misappropriation is widespread, depending on opportunity mostly. This type of fraud is frequent in lower and middle ranks of organizations and also in outsiders. It may be more frequent in accountants and other employees directly dealing with money, inventories, customers and suppliers. By contrast, corruption is highly cultural, its pattern varying from country to country. In some countries corruption is endemic, closely relating to organized groups, often but not always of a criminal type. Corruption is much less dependent on opportunity and much more difficult to eradicate than asset misappropriation. Finally, the misstatement of financial statements, although widespread and extremely damaging, is a type of fraud restricted to accountants and executives of companies. External auditors are often unable to detect it and much effort has been spent in detecting the misstatement of accounting reports automatically. Regulatory authorities such as the Securities and Exchange Commission (SEC) in the US are known to have been effective in detecting this type of fraud in a number of cases.

By target, frauds can be

- non-financial or
- financial.

Non-financial fraud aims at dilapidating resources or gaining notoriety, not at monetary advantage. The most common types are:

a) Telecom fraud
   a. aimed at the service provider
   b. allowed by the service provider
   c. Hacking and Internet vandalism

b) Scientific fraud
   a. fabrication of results,
   b. Plagiarism

...and other types

Financial fraud types are innumerable; they may be, for instance,

a) Identity appropriation in the use of credit card and others
b) Concealing the source of funds ("money laundering") although nowadays this type of crime is generally regarded as a concern independent from fraud.
c) Tax evasion
d) Medical: false prescription and others
e) Retail: theft committed by store managers and employees
f) False claims in insurance, State benefits and others
g) False information in insurance, bank credit loan application and others
h) Stock exchange – insider trading, dumping and others
i) Financial reports – false Accounts

… and many other types. Appendix C is devoted to an exhaustive presentation of the major varieties of fraud types.

Chapter 2: Prevention

Prevention is, in the majority of cases, the most effective and the cheapest path towards fraud control. In the form of deterrence measures, the prevention of fraud is in fact the only procedure guaranteed to bear results.

The rules of thumb or general guidelines for fraud prevention are well-known:

1. Accept the fact that fraud can occur and that nobody is immune. A healthy amount of moral skepticism is indispensable in the part of the entity's management. Most likeable persons who never committed fraud before will do it given opportunity, motivation and justification.

2. Always perform employee screening on hiring. While you may consider yourself a good judge of character, most fraudsters are likeable persons.

3. Let employees know that management is actively looking for fraud. Do not accuse employees of being dishonest but do ask questions when facing unusual situations. Employees should know that great attention is given to the possibility of fraud and nobody is exempt from scrutiny.

4. Set up general business controls:

a. Control the mail by having it picked up by an employee with no financial responsibilities. Scan all financial mail for anything that looks uncommon.
b. Control and receive the bank statements. Review their contents before reconciling. Look for missing checks, out of sequence checks, unknown payees, checks that appear altered, or checks not signed by an authorized signer
c. Control receivables by limiting access to customers' records
d. Maintain access control over inventory and monitor material costs closely
e. Establish an annual operating budget and compare to actual results

f. Rotate employees, require them to take vacations and cross- train employees over multiple functions
g. Hold regular meetings with department managers
h. Visit job sites and/or vendors

5. Establish and communicate formal fraud policies for the organization

6. Take action when fraud occurs. Action and publicity are against the feeling of managers that were victims of fraud; but it is all important that fraud be publicized and acted upon rather than hidden away.

7. Scenario thinking: imagine that you were going to perpetrate a number of frauds against specific entity functions and how they would be accomplished. Take action to remedy these opportunities regardless of how unlikely they may seem.

Key policies supporting fraud prevention include:

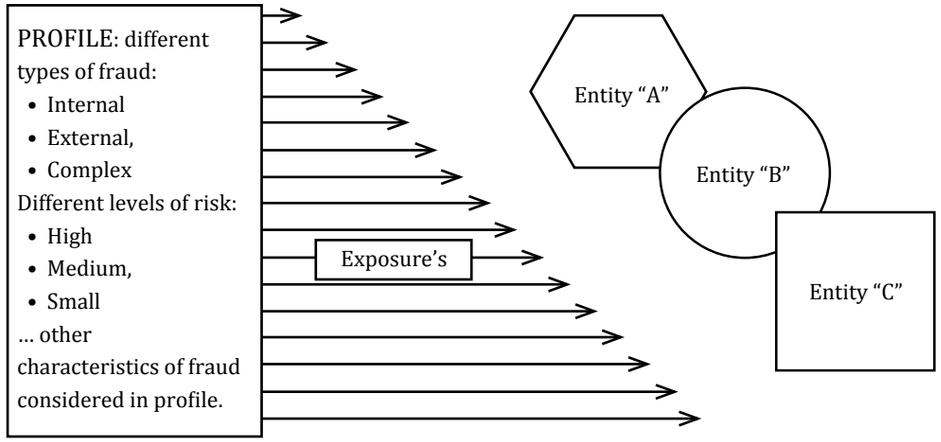
a. enact a Code of Conduct for the organization
b. put in place fraud risk management processes
c. draw a fraud control plan
d. perform regular fraud awareness training
e. put in place fraud-related controls for activities with a high fraud risk exposure
f. keep accurate and up-to-date data on fraud
g. communicate investigation outcomes so as to demonstrate that allegations and incidences of fraud are serious and robustly dealt with

Risk profile, exposures and risk levels

Not all organizations are similar regarding the risk of fraud. Some are not exposed to external fraud; some are especially exposed to corruption. In order to prevent fraud effectively, it is worth viewing the risk of fraud as the interaction between a

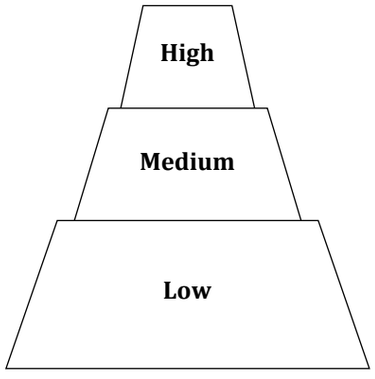
1. "risk profile" of the organization or their comprising entities, and the
2. "exposures" of such entities to different types of fraud.

The relationship between fraud risk profile and exposures may be described as follows:



As with other fraud control strategies, an organization should align the resources it commits to preventative strategies according to its fraud risk profile and exposures. The fraud risk profile of specific entities within an organization may lead to low, medium or high risk levels; and within each entity, exposures to a given type of fraud may also lead to low, medium or high risk levels. A range of preventative strategies and measures that should be considered when managing fraud risks is illustrated thus:

Fraud risk level:



Preventive strategies:

- Rotation of personnel
- Security clearances for staff
- Regular Supplier reviews
- Independent confirmation of service delivery
- Supplier and customer screening
- Regular and random audit checks
- Experienced personnel placed in high risk roles
- Code of conduct
- Fraud policy
- Fraud awareness training
- Employment screening

Preventive measures at the bottom of the triangle represent those measures that would need to be implemented by any entity to have an effective fraud control. Strategies at the top of the triangle are appropriate if an entity has a significant exposure to specific types of fraud.

Resources devoted to preventative strategies and controls should be proportionate to the fraud risk profile and exposure of each entity as indicated by, for example,

1. significance, dimension of losses caused by fraud
2. scope of risks of fraud
3. complexity of risks of fraud
4. sensitivity of possible fraudulent activities

The controls identified and their associated costs should be considered with respect to the nature and scale of the fraud risks they are designed to address.

Internal (occupational), external and complex fraud

For prevention and detection purposes, fraud is classified by origin, that is, as

1. internal (perpetrated by an employee, manager or contractor of an entity). The most usual or common types of internal fraud is known as “occupational”.
2. external (perpetrated by a customer or an external service provider or third party)
3. complex (collaboration between employees, contractors and/or external service providers)

Common types of internal fraud include:

a. theft or misuse of tangible assets (cash, inventory, plant and equipment) by employees;
b. theft or misuse of intellectual property or other confidential information (including health, tax and personal records);
c. financial statement reporting fraud;
d. release or use of misleading information for the purposes of deceiving, misleading or to hide wrongdoing;

e. false invoicing;
f. credit card and other payments fraud;
g. receiving bribes or improper payments (corruption);
h. misuse of position by employees in order to gain some form of financial or non-financial benefit (corruption)

The principal opportunities for internal fraud to occur arise from poor internal controls.

Rule of thumb: the three most common types of internal / occupational fraud are:

1. Asset misappropriation: schemes in which the perpetrator steals or misuses an entity’s resources such as: false invoicing, payroll, check tampering, billing, expense reimbursements and skimming (cash is stolen before it is recorded).
2. Corruption: schemes in which fraudsters use their influence in business transactions in a way that violates their duty to their employers in order to obtain a benefit for themselves or for someone else, for example: the employees might receive or offer bribes, extort funds from third parties or engage in transactions that present conflicts of interest.
3. Financial misstatement: perpetrator intentionally misstates or omits material information from the entity’s financial reports, for example: reporting of fictitious revenues or expenses, or the concealment of revenues or expenses in order to make an entity appear more profitable or conversely, less profitable to evade taxes.

Fraud is most likely to occur in the accounting department. Accounting staff generally have the greatest access to resources and have the opportunity and knowledge to hide the fraud.

Examples of external fraud include:

a. customers deliberately claiming benefits from government programs that they are knowingly not eligible for
b. fraudulent claims made to Insurance companies

c. false information to obtain a credit loan from a bank
d. external service providers making claims for services that were not provided
e. individuals or businesses intentionally evading payment of taxes to government
f. identity theft for credit card fraudulent use, for Internet fraudulent purchases, for bank account access and many others

Cases of complex fraud involve collaboration between agency employees and external parties.

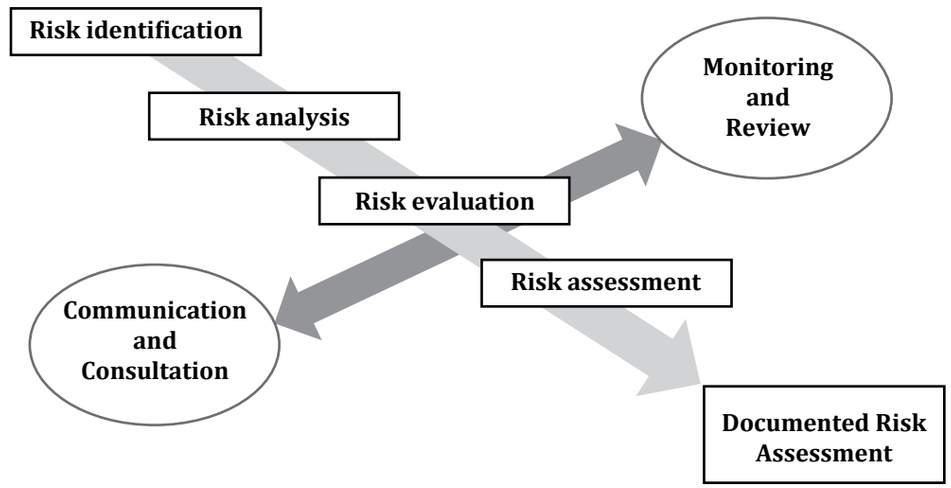
Each entity has its own role which brings about a profile of fraud exposures. The table below, taken from the "Better Practice Guide" of the Australian National Audit Office (2010), shows examples taken from the Public Sector of fraud exposure by entities or functions.

Entity or Function	Examples of fraud exposure
Policy development and review	An example of inappropriate behavior in an organization with a policy focus is where a civil servant makes improper use of inside information, or uses their status, power or authority in order to gain or seek to gain a commercial benefit or other advantage
Procurement including tendering and managing supplier interfaces	Government purchases include the acquisition of goods, services, and property, including intellectual property. Public officials should not benefit personally from procurement decisions involving expenditure of public money. The community and suppliers have a right to expect government to perform their duties in a fair and unbiased way and that the decisions they make will not be affected by self-interest or personal gain.
Revenue collection and administering payments to the general public	Tax evasion and benefit fraud (including fraud associated with social, health, and welfare payments) is generally characterized by the deliberate provision of incorrect information in order to secure payments or payment amounts for which the recipient is not entitled.

Service delivery to the general public including program and contract management	Contracting (or outsourcing) is now an integral part of doing business in the public. An example of external fraud includes the fraudulent conduct of service providers who charge the State for goods or services that are not delivered, or delivered in an incomplete way.
Exercising regulatory authority	An example of corrupt and inappropriate behavior that may occur in a regulatory authority is abuse of power, that is, when an official uses their authority as a regulator to approve compliance with regulatory requirements in exchange for a benefit or advantage.

The fraud control process

Fraud control should not be an isolated procedure; rather, it should be linked to other risk management procedures of the organization,. The figure below illustrates the basic components of a risk management procedure.



It is worth commenting on the major features of the risk management procedure:

1. A fraud risk assessment procedure involves communication and consultation with relevant employees at all levels during all stages of procedure. This communication should address issues relating to the risk itself, its causes, its impact (if known) and the measures taken to tackle it. This approach ensures that those accountable for implementing the risk management procedure understand the decision-making procedure and the reasons why certain actions are required.
2. In the first place, an organization's objectives should be set to work together (aligned) with external and internal constraints or advantages to be taken into account when managing risk. This sets the risk criteria for the remaining of the process.
3. Identifying fraud risks requires entities to consider both internal and external fraud risks. Organizations should also consider fraud risks that may emerge in the future, for example, those created by a change to an IT system or other significant changes in business processes.
4. It is also important that fraud risks are taken into account in the design of a new system or program. Identifying fraud risks at the system and program levels will assist entities to assess overall risk and to reflect these risks in their strategic planning objectives.
5. As fraud entails dishonesty and deception, the identification of fraud risks importantly requires a skeptical mindset and involves asking probing questions such as:

    a. How might a fraudster exploit weaknesses in the systems of controls?
    b. How could a perpetrator override or circumvent controls?
    c. What could a perpetrator do to conceal fraud?

6. Documenting and assigning ownership of the risks and controls is important. The business area responsible for managing a particular fraud risk should be identified and the timeframe for implementing any remedial action should also be clearly documented in risk management plans.

7. It is also important to monitor and review the fraud risk assessment regularly. Where an entity undergoes a substantial change in structure or function, or where there is a significant transfer in function (for example, as a result of outsourcing), the entity must undertake another fraud risk assessment in relation to the changed functions.

An entity should also actively monitor and review its identified fraud controls. Changes in the effectiveness or applicability of such controls can impact on the entity's fraud risk assessment to either increase or decrease fraud risk. An entity's internal audit area would generally be expected to assess periodically whether the entity's fraud control framework is appropriate and is operating.

Assessing the entity's profile of fraud risk exposure

The audit committee oversights the building and updating of an entity's fraud risk exposures' profile. As mentioned, each entity has its own profile of fraud risk exposures. Industry, location, and cultural factors that can influence fraudulent behavior are to be considered in drawing the profile.

The listing of the different types of frauds known to have been committed against entities of a similar type is an appropriate first step in drawing the profile of fraud risk of an entity. To each item of such list it would then be added the corresponding expected likelihood of occurrence (incidence is high, medium, low or naught) together with preventive, detective and response measures. Occurrences of different types of fraud by industry and location can be found in publicly available reports, for instance, in fraud surveys.

The following is an example of internal fraud schemes: name, definition and cases:

1. Schemes involving theft of cash receipts

skimming	Any scheme in which cash is stolen from an organization *before* it is recorded on the organization's books and records	• Employee accepts payment from a customer but does not record the sale and instead pockets the money
cash larceny	Any scheme in which cash is stolen from an organization *after* it has been recorded on the organization's books and records	• Employee steals cash and checks from daily receipts before they can be deposited in the bank

2. Schemes involving fraudulent disbursements of cash

billing	Any scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for personal purchases	• Employee creates a shell company and bills employer for services not actually rendered • Employee purchases personal items and submits an invoice to employer for payment
expense Reimbursements	Any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses	• Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc.
check tampering	Any scheme in which a person steals his or her employer's funds by intercepting, forging or altering a check drawn on one of the organization's bank accounts	• Employee steals blank company checks and makes them out to himself or an accomplice • Employee steals an outgoing check to a vendor and deposits it into his or her own bank account
payroll	Any scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation	• Employee claims overtime for hours not worked • Employee adds ghost employees to the payroll
cash Register disbursements	Any scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash	• Employee fraudulently voids a sale on his or her cash register and steals the cash

3. Other assets' misappropriation schemes

Misappropriation of cash on Hand	Any scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises	• Employee steals cash from a company vault
non-cash Misappropriation	Any scheme in which an employee steals or misuses non-cash assets of the victim organization	• Employee steals inventory from a warehouse or storeroom • Employee steals or misuses confidential customer financial information

… and so on

After major fraud risk exposures are identified, each of such potential threats should be the object of specific preventive and detective actions.

The appendix shows an extensive list of frauds made available by the Association of Certified Fraud Examiners, ACFE, a US body. Most of the frauds an entity may face are listed there.

Preventive measures detailed

The following 7 measures are generally viewed as the basic preventive actions which any organization should put in place:

1. The existence of a clear, well-known Code of Conduct of the organization: this is the first building block in establishing a strong ethical culture.

2. The identification of all possible Conflicts of Interest and their removal: the management of conflicts of interest is an integral part of establishing an ethical culture. Of primary concern within a government entity is the conflict between private and public interests, and the effective management of this issue. The most basic guidelines on how to actively manage conflicts of interest are as follows:

a. register or declare in writing a possible or potential conflict of interest to a manager
b. restrict involvement of employees in matters in which they have (or are perceived to have) a conflict of interest
c. recruit third parties who do not have an interest (such as probity advisers) to advise on or participate in the matter
d. remove employees from involvement in matters in which they have real or perceived conflicts of interest
e. an employee may have to relinquish assets or other private interests or resign

3. The Screening of New Staff Members is also mandatory: practical steps to be taken are:

a. verification of identity
b. police criminal history search in all countries where the individual has resided
c. reference checks with the two most recent employers and any public sector employer
d. check with any relevant professional licensing or registration board to determine whether an inquiry by a professional licensing or registration body is pending. Examples include the Institute of Chartered Accountants or the Bar Association

e. consideration through interview and any necessary follow-up of any employment history gaps and reasons for those gaps
f. verification of qualifications through an independent source, for example, by calling the relevant institutions rather than relying on information or documentation provided by the individual

4. Regular Fraud Awareness Training: all staff members should have a general awareness of fraud, how they should respond to fraud and the organization's processes if fraud is detected or suspected within their workplace. Fraud awareness training is an effective method of ensuring that all employees are aware of their responsibilities for fraud control and of expectations pertaining to ethical behavior in the workplace.

Ensuring that employees understand what constitutes fraud and the cost of fraud is another key objective of fraud awareness training. The training of managers and staff can assist them to recognize the common behavioral signs that fraud is occurring, and encourage them not to ignore these "red flags".

A good fraud awareness training regime includes information on:

a. the principles of privacy and confidentiality legislation and awareness, Public Service legislation and underpinning expectations such as statements of Values and Code of Conduct and ethical standards (including how to report fraud and unethical behavior) and conflicts of interest policy
b. what constitutes fraudulent conduct, including practical examples of fraud and the potential benefits fraudsters seek to obtain (intangible and tangible)
c. how and where to communicate concerns about known or potential wrongdoing
d. responsibilities for the prevention, detection, investigation and reporting of unethical behavior including the roles of the individual, the Fraud Manager and the Chief Executive
e. the organizational and personal benefits of effective fraud control
f. the signs or "red flags" associated with potentially fraudulent activity
g. whistleblowing mechanisms, protections and consequences for inappropriate disclosures

h. the potential disciplinary consequences for those who engage in unethical behavior
i. the role of (internal) conduct investigations
j. the role of the Police and the Public Prosecutions where serious criminal behavior is alleged

Consideration should also be given to the design of specific and ongoing refresher fraud training for employees who work in areas in which there is a higher risk of fraud.

5. Not just new staff, all new suppliers and service providers should also be screened: confirming identity, solvency and reputation is important in managing fraud control within an organization. The screening of service providers should be tailored to the size and relative risk which such individual or organization represents.

Entities should take steps to ensure the good intentions (bona fides) of new suppliers and customers and periodically confirm the bona fides of continuing suppliers and customers.

Depending upon the relative importance and risk presented by the service provider, practical steps an entity can take to verify their bona fides on both an initial and periodic basis include:

a. checking that the organization's trading address and telephone listing matches its contact details
b. searching the company register
c. confirming that the organization's identifier corresponds to its company register
d. verifying the personal details of directors, including a bankruptcy and criminal search
e. confirming current legal proceedings pending and judgments entered
f. confirming the entity's registration with the appropriate chamber of commerce or industry association if applicable

6. Fraud controls for high exposure processes and activities: some examples of preventative fraud controls that can be applied to activities highly exposed to fraud:

a. segregation of duties. This means that two persons are involved in authorizing a transaction: the person who makes the choice and the person who verifies its conformity with plan or budget
b. hard coded IT system controls, that is, access restrictions or / and money value limits for processing transactions
c. effective procedural controls and management oversight where appropriate
d. physical security measures including the use of safes and access restrictions
e. the deterrent effect of regular and random quality assurance checks by management to determine the existence of a service or goods procured
f. regular supplier reviews and the maintenance of a register of non-compliance / breaches of contractual conditions and reporting requirements
g. rotation of personnel in risk positions, requiring staff to take regular annual leave and also requiring that balances never accrue to high levels

7. Corruption control: a corrupt practice is the offering or receiving of anything of value to influence improperly the decisions of another party. Corruption should be especially considered by all public entities. An effective anti-corruption program should include:

a. strong anti-bribery provisions
b. a policy of personnel rotation in high-risk positions so that improper relationships are less likely to develop
c. vendor audits of high-risk providers
d. enhanced probity and contracting procedures
e. multiple open channels of communication with employees, customers, vendors and other third parties to encourage those parties to come forward if they have any concerns relating to corrupt conduct

Communication of identified fraud: the deterrent effect

While an entity may have a desire to avoid adverse media attention, the public reporting of summary information in relation to fraud investigations serves the following purposes:

1. illustrates contemporary ethical issues and can be used as part of a fraud awareness program
2. acts as a deterrent to other potential fraudsters
3. demonstrates that disciplinary decisions are taken against those found guilty of committing fraud
4. demonstrates the entity's commitment to having an ethical and anti-fraud culture

Therefore, the public reporting of such information is considered a major preventive measure. Such public reporting, must comply with the principles of justice and equity, namely avoiding exposing the organization to liber and similar charges.

Chapter 3: Detection

Many managers believe that if fraud is occurring in his or her organization, then it will be readily apparent and quickly identified. This is not so. Fraudulent activities can go on for many years undetected.

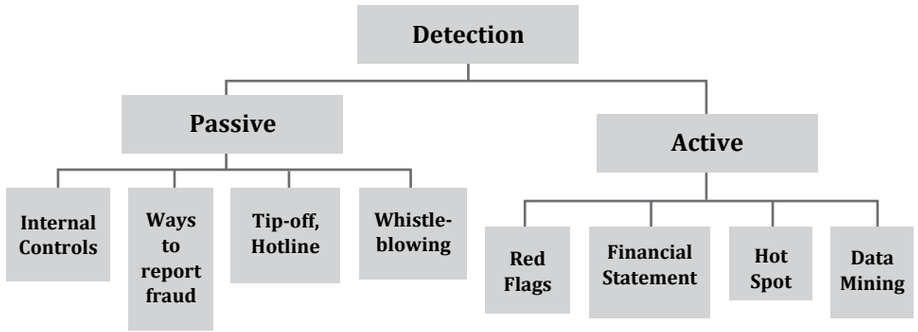
It is also believed that a fraud will sooner or later be discovered by accident, that is, by some unexpected action in the part of the fraudster or in the part of another person. In fact, accidental detection of fraud is very unlikely. Current fraud research indicates that small privately-held companies discover fraud by accident less than one-third of the time. In almost every large, sophisticated fraud case, detection required the implementation of a properly designed fraud control - or a tip from an employee.

Therefore, fraud detection procedures are an important part of fraud control. Their effectiveness in detecting fraud should not be underestimated.

Measures to detect fraud once committed are of two types: passive and active.

- Passive measures include controls or activities that do not require the active and ongoing involvement of management, but exist as a means by which fraud is detectable within an organization. An example of this is a reporting 'hotline' so that employees, customers, clients and the general public can report incidents.
- Active measures include controls that require the assertive involvement of management and by their nature are designed to detect or assist in detecting fraud within an organization. Examples include data mining, targeted audits through hot spot analysis, internal audit, quality assurance and the analysis of management accounting reports.

The figure below details the most significant passive and active detection measures



Passive detection measures

Passive fraud control measures are by far the most effective in detecting fraud and, simply by the fact that they are in place, act similarly as deterrents of fraud (are preventive measures). The 4 most common passive measures used by entities are Internal Controls, Fraud Report Channels, Tip-Off and Hotline facilities and the promotion of whistleblowing.

Effective internal controls

Internal controls are the most effective measures by far. Almost half of committed frauds were detected through internal controls.

Some examples of internal controls:

1. regular independent reconciliation of accounts;
2. independent confirmation of service delivery where suppliers are paid in advance for services
3. physical security, for example, security cameras
4. staff who know their jobs (people who are familiar with their jobs are more likely to be able to identify anomalies)
5. job rotation / mandatory leave
6. comparisons between budgeted and actual figures and the follow-up of discrepancies

7. audit trails and system access logs and the regular review of these
8. exception reporting
9. quality assurance
10. surprise audits
11. management review

Channels to report fraud allegations

Allegations made by employees, contractors, and members of the public can often lead to the uncovering of fraud. One way entities can detect fraud is through encouraging employees, contractors, service providers and, where relevant, members of the public to report their suspicions of fraud.

Employees should be encouraged to report suspected unethical behavior and be provided with a visible process to enable them to report this easily. Easily accessed guidance material supports employees to readily identify what incidents should be reported and to whom. Guidance could include, for example, advice on reporting to line managers; reporting to Human Resources, in particular, the area that investigates employee conduct-related matters; reporting to the entity's fraud control officer; reporting to internal audit; and reporting to an anonymous hotline (if available).

Members of the public (including an entity's customers, suppliers and other stakeholders) can play a role in reporting suspected fraud. These parties may be aware of fraud occurring within an entity, or being committed against an entity by an outside party.

But appropriate channels to report should be in place so that fraud allegations are treated in confidence, properly scanned and treated seriously where appropriate.
Tip-Offs and Hotlines are examples of such channels. Fraud Tip-Off Lines are known to be effective in detecting fraud.

Tip-off and hotline facilities

A hotline is a single point of contact for staff members (and others) to report information on suspected fraud. It gives people a means of contacting the organization at minimal personal risk. A hotline arrangement also enables staff to obtain advice and information.

Other advantages are:

a. A hotline facility is perceived as being independent of management. Entities may find it beneficial to outsource the hotline service to a third-party provider.
b. A hotline facility, while predominantly telephone-based, can also sometimes receive reports via other channels, such as email or mail.
c. A well-designed hotline provides access to a trained interviewer, operates 24 hours a day, supports a multilingual capability, provides a phone number that is toll-free, and applies consistent protocols for gathering and recording relevant information.
d. Matters reported via the hotline are normally treated confidentially, to the fullest extent possible. It can provide anonymity, though it is a good idea to obtain the complainant's name or as many supporting details as possible to enable better follow-up of an allegation.
e. An organization can use the data on fraud allegations to analyze trends and address emerging risks.

Depending on the size and type of the entity (for example, policy, procurement, revenue collection / payment administration, service delivery, or regulatory), a range of mechanisms can be used to enable fraud allegations to be reported, including: a telephone line, manned by an appointed delegate; an email or postal address, which allegations could be sent to; an electronic mechanism, for example, a form available on the internet that could be submitted electronically. An organization's website can provide advice to informants about the kind of allegations that could be referred to the organization, including whether the tip-off concerns a member of staff, a customer, or a business. An organization's website can also facilitate reporting in cases where a member of the public may be reluctant to talk via telephone.

Whistleblowing

Whistleblowing refers to the reporting, in the public interest, of fraudulent activity. Whistleblowers are protected by law and instruments are in place to protect whistleblowers. These instruments provide schemes that give special protection to disclosures made in the public interest about unlawful, negligent or improper public sector conduct or danger to public health or safety or the environment.

It is good practice for an entity to provide information about whistleblowing in its fraud awareness training, specifically the type of information that attracts whistleblowing protections and the persons to whom the disclosure can be made.

Active detection measures

Active fraud detection measures are controls or activities that require the assertive involvement of management. These measures can be broadly categorized as:

a. monitoring and review activities, focused on employees and customers at risk
b. analysis of management accounting reports
c. Hot Spot analysis
d. Data Mining, including data reconciliation, matching and many other checks on data files based on statistical analysis supported by information technologies
e. real-time fraud detection in transaction data, using complex models

Monitoring through early warnings (Red Flags)

There are a number of "red flags" or early warning signs of fraud activity which can be used to help profile possible internal perpetrators. As part of the Fraud Control procedure, red flags should be checked regularly.

The following table exemplifies some common red flags for staff and the workplace.

Early warning signs: people	Early warning signs: areas or activities
Unwillingness to share duties; refusal to take leave.	Financial information reported is inconsistent with key performance indicators.
Refusal to implement internal controls.	Abnormally high and increasing costs in a specific cost center function.
The replacement of existing suppliers upon appointment to a position or unusually close association with a vendor or customer.	Dubious record keeping.
A lifestyle above apparent financial means; the provision of gifts to other staff members.	High overheads.

Early warning signs: people	Early warning signs: areas or activities
Failure to keep records and provide receipts.	Bank reconciliations not up to date.
Chronic shortage of cash or seeking salary advances.	Inadequate segregation of duties.
Past legal problems (including minor previous thefts).	Reconciliations not performed on a regular basis.
Addiction problems (substance or gambling).	Small cash discrepancies over a period of time.

The screening of employee behavior (warning signs in people) is also often explained as a set of 7 popular rules of thumb:

1. become irritable
2. start living outside their means
3. be unusually close with a vendor
4. have addiction problems
5. refuse to take vacation or any unexpected leave
6. claim to be subject to excessive pressure
7. being secretive about work activities

It is important to bear in mind that these behaviors do not automatically mean fraud is occurring; they are potential warning signs. Moreover, if fraud is indeed occurring, it is not enough to identify the potential perpetrator: the whole fraud procedure must be uncovered.

Analysis of management accounting reports

These can reveal anomalies which may be indicative of fraud. Examples of such analyses are:

- monthly actual versus budget comparison reports for individual cost centers;
- reports comparing expenditure against prior periods;
- reports highlighting unusual trends in bad or doubtful debts;

… all may reveal areas which should be further investigated.

“Hot Spot” analysis

Allegations of unethical behavior raised through the organization’s reporting mechanisms (hotlines, reports to management via email and other methods) can be ‘mapped’ to show hot spots of potential fraud throughout the organization.

Multiple allegations about an area or individual potentially highlight an issue of either fraud or control weakness. This can be used to target the activities of internal audit, an investigation team or the fraud control officer.

The fraud risk exposure profile of an entity could be developed to identify the positions of officials who, because of the nature of that position, may be especially vulnerable to fraud. For these positions, action to detect irregularities and fraud could focus on:

a. regular performance appraisals, mandatory disclosure of interests, assets, hospitality and gifts; and
b. close monitoring in relation to existing computer data-mining to draw attention to transactions that appear to depart from established norms.

Data-Mining (post-transactional review)

Indicators of fraud, misconduct and error can, in some cases, be detected through the examination of the transactions produced as part of an organization’s financial and operational activity. The use of data mining / analysis techniques and tools can assist with the identification. Benefits of using data mining include:

1. analysis of suspicious transactions, for example, duplicate payments or claims, repeated payments during a short period, large, undocumented payments; but it is often difficult to distinguish suspicious from normal payments when the analyst is not familiar with the organization
2. identification of unusual relationships, for example, employee bank account matches a vendor bank account; the same difficulty applies here

3. assessing the effectiveness of internal controls, for example, password sharing, employees remaining on the payroll after termination / resignation
4. the identification of irregular trends over periods of time is also able to identify, for example, supplier favoritism or unauthorized payments
5. an ability to analyze large volumes of transactions over periods of time rather than relying on sampling techniques is a data mining characteristic

Generally, there are two types of data mining:

1. retrospective review - the extraction of historical data (usually data relating to more than one year) from the organization's Enterprise Resource Planning (ERP) systems for analysis on a standalone IT system using data analysis software. Retrospective review tools can vary from a spreadsheet or database to software that is specifically designed for data analysis with pre-programmed tests such as duplicate payments tests, and an ability to create tests as required
2. continuous auditing / continuous monitoring (CA/CM) - collection and analysis of current data on a real or near real-time basis, that is, daily, weekly, monthly. CA is generally considered to provide the internal auditor with information regarding risk and controls while CM is generally considered to be a management monitoring function. CA/CM tools can vary from those which monitor transactions real time (much the same way that banks monitor credit card transactions) to tools which analyze data near real time that is, daily, weekly, monthly. CA/CM may also be performed using the inbuilt functionality in an organization's ERP system.

Retrospective review is typical of internal fraud control activities whereas continuous auditing is more frequently employed in the prevention of external fraud.

The role of Information Technologies in the implementation and use of data mining is further developed in a dedicated chapter.

Audit teams should coordinate active measures while conducting internal audits. Internal audit has been responsible for detecting 15 per cent of all frauds identified in the government sector ("Better Practice Guide" of the Australian National Audit Office, 2010). In instances where fraud is detected, it is essential that the matter be reported to the appropriate party, as noted above.

Detecting external fraud committed against public entities

Criminology results indicate that, of the external fraud incidents against the State, the focus of the highest number of activities was on entitlements. This category includes obtaining a State payment, for example, a social, health or welfare payment by deceit. It also includes revenue fraud that is deliberately avoiding obligations for payment to government, including income, customs or excise taxes. These are the strategies required in such case:

1. Compliance reviews: most entities that collect revenue or administer State payments conduct reviews across the various revenue and payment types. Based on previous experience, knowledge of their customers, and evidence from within their systems or from outside information, entities may undertake reviews that ex amine a recipient's circumstances where there is a perceived risk of fraud. The aim of such reviews is to detect a deliberate error, omission, misrepresentation or fraud on the part of a customer. Review activity should be targeted to areas of higher risk, and an entity should pursue the most productive method for undertak ing reviews. Data mining / matching is a cost-effective method of supporting reviews, including cross-organizational approaches.
2. Data mining and data matching: compared with manual or routine record checking, technological advances in data processing allow for efficiencies in locating records and potential fraud. Where relevant information is held by other entities, data mining / matching provides significant benefits including: uncovering and reducing fraud; encouraging better compliance; and improving the quality of data held on the systems of participating organizations. Entities need to be mindful of privacy considerations and implement appropriate processes to ensure that any data mining/matching activities con form to legislative requirements.

Contracting or outsourcing is an integral part of doing business in the public sector and the delivery of many government programs involves contracting with private sector providers. External fraud includes the fraudulent conduct of service providers who charge the State for goods or services that are not delivered, or delivered in an incomplete way.

Most cases of external service provider fraud are discovered through day-to-day contract management and associated controls. The aim of contract management is to ensure that deliverables are provided to the required standard, within the agreed timeframe, and achieve value for money. A central risk to the success of a contract is the management of external service provider performance, including the potential for fraud, or inappropriate conduct by the external service providers.

Audit teams may discover instances of fraudulent activity in the part of contractors. Audit has been responsible for detecting 15 per cent of all frauds identified in the government sector.

The following is suggested treatments for managing external service provider performance ("Better Practice Guide" of the Australian National Audit Office, 2010):

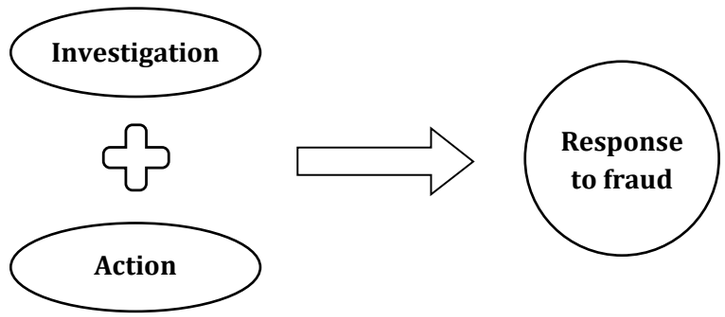
1. establish a clear understanding of the contract and the contract's responsibilities of each party
2. monitor contractor performance regularly, including deliverables and contract conditions
3. hold specific performance review meetings
4. only make payments for satisfactory performance
5. ensure proper documentation and recordkeeping to provide the necessary evidence to demonstrate non-compliance or potential fraud

The sharing of information about risk factors and fraud perpetrators within entities and across the Public Sector is important in the prevention and detection of fraudulent activity. Liaison with other entities may also help target detection activities and the sharing of better practices.

Any forum which brings together organizations with a similar business profile can be used as an opportunity to discuss fraud risk, prevention, detection and response.

Chapter 4: Response, monitoring, evaluation and reporting

Once detected, fraud must be (1) investigated and (2) the appropriate action must be taken:



After an adequate response is made, the follow up consists of monitoring, evaluation and reporting.

Investigation

The purpose of fraud investigation is to gather evidence relating to fraud allegations to determine the facts relating to the matter and to assist in deciding what, if any, action should be taken in relation to the matter. State entities are required to investigate routine or minor instances of fraud against entity programs and to document the reasons for their decisions, irrespective of whether the initial assessment results in the matter being referred for a criminal investigation or no. "Routine or minor" are instances of fraud that, on an initial assessment by the entity, would be unlikely to be accepted by the Police. The identification of fraudulent behavior should include ("Better Practice Guide" of the Australian National Audit Office, 2010):

a. date and time of report
b. date and time of incident detection
c. how the incident was reported to management: anonymous report, line management and others
d. nature of the incident
e. value of the material loss to the entity, if any
f. action taken following detection

Such a register can be used to facilitate an organization's policy for the reporting, analysis and escalation of all detected incidences of fraud and corruption. This policy should be clear on the actions to be undertaken following the reporting of an incident.

Upon receiving an allegation of fraudulent conduct, an entity needs to consider what should be the appropriate response. Moreover, entities must have a procedure covering the initial consideration of a fraud allegation that includes:

a. recording of the allegation in an appropriately secure fraud incident register, file and/or electronic case management system
b. the person responsible for making the initial assessment is appropriately trained and the entity provides an appropriate level of managerial oversight of decision-making
c. timeframes for initial consideration of the allegation
d. the obtaining of any readily accessible evidentiary information from within the entity, where the collection of such evidence would not jeopardize any future investigation, to allow an informed decision on the type of further action required
e. the need to document the reasons for the decision and what action is intended

The decision as to how to respond to an allegation of fraud is a critical decision in the fraud investigation process and one which needs to be appropriately documented.

Conducting investigations: fraud investigations are conducted to determine the facts relating to specific allegations of fraud, through the collection and examination of evidence. Entities must have in place processes and procedures fraud investigations. For example, entities must have written procedures regarding:

a. the process for taking witness statements and conducting interviews with suspects
b. the handling of all physical evidence, including property seizure records, and the storage and disposal of exhibits (there should also be written procedures addressing the audit of the exhibit register as required by the Australian Government Protective Security Policy Framework)

c. the conduct of surveillance, including physical and electronic
d. the management of human information sources (also referred to as informants)
e. the use of legislated powers such as the power of arrest, detention, coercion, search warrant execution, production orders and inspection orders

Investigators must have knowledge of and the ability to apply the principles and elements of their entity's standards and written procedures.

A fraud investigation and response decision-making process should be able to provide an explanation of, and guidance through, the fraud investigation and response process. In some instances, entities will not be sufficiently resourced to conduct an internal investigative response to allegations of fraud. The establishment of an internal fraud investigations team can be costly and takes time to implement effectively. This will not be an issue for the larger program delivery and customer service entities, but for smaller entities (or entities which traditionally focus on policy development), the most cost-effective option will be to engage external investigations services. Notwithstanding an entity's resource constraints with respect to internal fraud response capabilities, all serious and complex fraud matters should be referred to the Police in the first instance. In addition, a relevant entity must consider whether it may still require support from the Police in the form of assistance to execute search warrants or in the provision of forensic services.

Action

Actions in response to detected fraud may comprise the following courses:

1. criminal prosecution
2. civil and administrative remedies
3. implementation of recovery procedures

Criminal prosecution - Entities must to consider criminal prosecution in appropriate circumstances. Prosecutions are important in deterring future instances of fraud and in educating the public generally about the seriousness of fraud. One of the key questions to be considered in the course of an investigation is whether there is a prima facie case for prosecution. That is, is the evidence sufficient to prove the allegation of

fraud beyond reasonable doubt? Factors to be considered in assessing whether it is in the public interest to proceed with a prosecution will vary from case to case but may include ("Better Practice Guide" of the Australian National Audit Office, 2010):

1. whether the offence has been determined to be serious or trivial in nature
2. any mitigating or aggravating circumstances
3. age, intelligence, health or any special infirmity of the alleged offender, witness or victim
4. the alleged offender's antecedents
5. the staleness of the offence
6. the degree of culpability of the alleged offender
7. the availability and efficacy of any alternatives to prosecution
8. the likely outcome in the event of a finding of guilt
9. the need for deterrence

Should there be insufficient evidence to prove an offence to the required criminal standard (beyond reasonable doubt) or there is sufficient evidence for prosecution but the entity concerned considers that the public interest does not require prosecution, the decision not to prosecute should be examined at the highest hierarchical level.

Civil and administrative remedies - there are numerous civil and equity law remedies and administrative processes available to an entity to deal with people who engage in unethical or unlawful behavior (be it fraud or misconduct). Entities need to have their own clear policies on the appropriate remedies and the situations in which these remedies will be sought. For internal fraud, State entities may take administrative action. Remedies available include, but are not limited to: reprimand; suspension; transfer / reassignment of duties; demotion; termination; forced retirement; penalty; financial recovery; counselling; loss of privileges, and greater scrutiny / increased controls.

Recovery procedure - once an investigation is complete an entity should consider attempting to recover financial losses caused by fraudulent activity through proceeds of crime and civil recovery processes or administrative remedies.

Recovery action should be undertaken where the likely benefit will exceed the recovery costs. In this context, "benefit" is not simply financial, but should include consideration

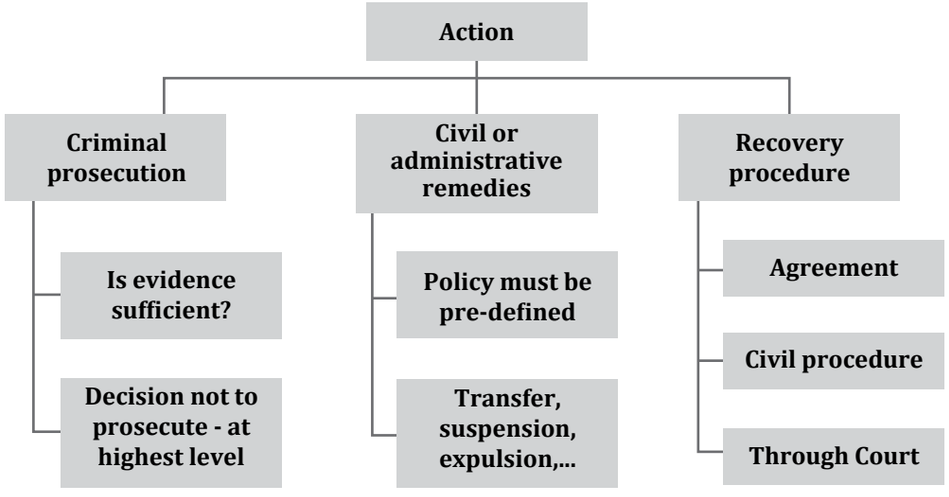
of deterrent value and other non-financial benefits such as public perception and integrity of entity reputation. Entities should not underestimate the deterrence value of loss recovery. This is particularly important given that fraudulent activity is considered to be an economic crime generally involving the weighing of potential benefits against the risk of discovery and subsequent consequences.

While recovering losses may in some cases cost more than the value of the loss recovered, the value of reducing the potential benefit to fraudsters and its deterrent effect must be considered.

Entities have several options for the recovery of losses, including:

1. by agreement through withholding final pay or termination benefits via payroll
2. through civil procedures such as a demand for payment or similar, pursued via the courts if necessary (bankruptcy law can be used to recover losses where the individual has insufficient cash assets)
3. criminally—through a restitution order flowing from a criminal conviction

In short, action to be taken in the face of fraud can be summarized thus:



Monitoring and evaluation

Effective monitoring and evaluation of an entity's fraud control strategies can assist managers and other decision-makers to:

1. assess the continued relevance and priority of fraud strategies in the light of current and emerging risks
2. test whether fraud strategies are targeting the desired population
3. ascertain whether there are more cost-effective ways of combating fraud

Evaluations also have the capacity to establish causal links and, over time, an evaluation strategy has the potential to provide insights into:

a. the appropriate balance between fraud prevention and detection strategies
b. the relative weighting of entity incentives that focus on reducing the potential losses from fraud in the first instance, as opposed to discovering fraud after it has occurred

Analysis can also be undertaken on the effectiveness of established controls through undertaking a cost / benefit analysis both pre and post-implementation of fraud controls. This can often demonstrate savings made by an entity where effective fraud controls have been implemented.

As outlined in previous chapter, an entity's fraud risk assessment needs to be updated at least every two years or in the event of a significant change occurring within an entity. An effective monitoring and evaluation regime needs to be established to ensure that the significant fraud risks of the entity are being accurately captured and recorded. Both tasks require up to date fraud risk data.

The entity's fraud control plan should also be subject to regular monitoring and evaluation, which should seek to answer the following two questions: "Is it up to date?" and "Is it effective?"

Is it up to date? The fraud control plan should be updated regularly to ensure that the individuals tasked with activities under the fraud control plan are still the individuals

in those key positions. Significant changes should trigger an update of the entity's fraud control plan to ensure it contains accurate and up-to-date information. As outlined in the previous chapter, a fraud control plan should be updated at least every two years or sooner if the entity experiences significant change.

Is it effective? Changes including new technologies, changes in entities' operations and the commencement of new initiatives can render existing fraud controls ineffective or inappropriate. An entity should review its fraud control plan to ensure it is implemented appropriately and that it remains relevant to the risks being faced. Testing the effectiveness of a fraud control plan could include:

a. ensuring risk assessments have been undertaken appropriately
b. awareness-raising and training are evaluated and are shown to work well in practice
c. allegations are recorded, analyzed and followed-up in a timely fashion
d. cases of fraud are dealt with according to applicable external and internal standards
e. remedies are applied appropriately
f. information on cases of fraud are used to update the fraud risk assessment and strengthen controls
g. accurate information is provided to the Audit Committee on a timely basis

It is appropriate to evaluate the controls identified in a fraud control plan to ensure they are implemented and achieving the intended outcomes. If the controls seek to minimize significant fraud risks, consideration should be given to the frequency of the evaluations. Any such review should test the effectiveness of control design and operation and, if possible, seek to benchmark the entity's fraud performance (and hence the effectiveness of its controls) against other entities.

The following are examples of benchmarks that might be used for evaluating the effectiveness of the response elements of an entity's fraud control arrangements:

a. the timeframes within which allegations of fraud are investigated and fact-finding is completed;
b. the percentage of fraud investigations that are completed within the timeframes required by law or internal requirements

c. referrals accepted by the Public Prosecutor
d. requests by the Public Prosecutor for additional evidence to support the alleged criminal offence
e. referrals accepted by the Public Prosecutor that are successfully prosecuted (includes convictions that are not recorded)

Evaluation is the final element in consolidating an entity's fraud control activities. After any incidence of fraud, whether or not an offence is proven in a court of law, the entity should investigate the situation which allowed the fraud to occur, so as to determine whether it is a result of:

a. a one-off action by a person in a position of privilege (any new person in this position may be subjected to additional or periodical screening or monitoring)
b. the inadequacy of internal controls (in this case the controls should be re-evaluated and any deficiencies remedied), or
c. collusion (internal control systems can often be overridden by two or more people acting in conjunction with one another)

Evaluation activities can be coordinated by a Fraud Manager so that identified deficiencies and/or recommendations can be applied consistently to similar programs/processes. The outcomes of any hot spot analysis should also be taken into consideration.

An important part of evaluation will be the measurement of the loss incurred. Many entities are now maintaining accurate records of losses due to fraud or are embarking upon forensic audits using statistical sampling and actuarial techniques to measure the cost of fraud. The identified fraud is then analyzed to identify the fraud types and the root causes of the problems, for example, internal control weaknesses / breaches, poorly designed application forms or processing errors. This analysis will generally involve a review of source documents and data and may also include interviews with staff and third parties.

These results provide an entity with the ability to perform a cost / benefit analysis of the implementation of additional controls to either prevent or detect the types of fraud occurring. The assessed savings can then be confirmed in a re-measurement of fraud losses in subsequent periods following the implementation of the improvements.

FRAUD PREVENTION AND DETECTION: METHODS, TECHNOLOGIES AND VENDORS

Reporting and communication

For a fraud control framework to be effectively implemented, both internal and external stakeholders need to be aware of the outcomes of the fraud control activities undertaken. As amply stressed before, the reporting of these outcomes can also provide a deterrent effect which will assist an entity in minimizing the impact of fraud on its operations. Timely, accurate and up-to-date data is critical in this process.

Internal reporting: effective internal reporting channels are critical to the management of fraud risks within an entity. Central to this is the role of a Fraud Manager, who establishes and manages these information channels so that the right level and content of information is reported to the right audiences.

The head of an entity's internal audit area should report to the entity's Chief Executive / Board and Audit Committee on the outcomes of any monitoring and evaluation activities as well as any investigations and/or outcomes of prosecutions or civil action. To assist priority-setting, an entity can set reporting thresholds for the reporting of individual cases of fraud to the Chief Executive / Board and Audit Committee. A useful strategy is to report fraud trends over time including changes to the level of fraud within an entity by type, for example, trends in the inappropriate use of information, travel fraud and identity fraud.

External reporting: State entities are in general required to report on fraud matters to their Minister, to the Minister for Justice, Parliament and other governing bodies. Such reports demonstrate that they comply with Fraud Control Guidelines.

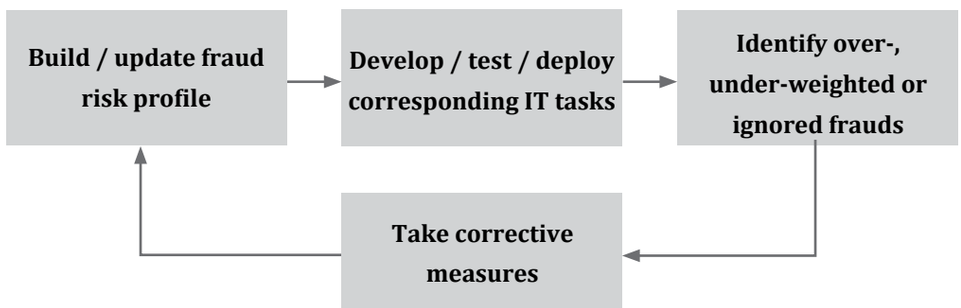
Once the result of an investigation is known (whether the outcome is a criminal prosecution or an administrative remedy), as far as permitted by privacy legislation, the entity should consider communicating the outcomes to staff (employees and contractors) and, where appropriate, the public (customers, clients and suppliers). This demonstrates that disciplinary decisions are regarded seriously and consistently (key factors in the preparedness of individuals to report wrongdoing in the future) and also serves to keep fraud prevention in the front of the minds of staff and/or customers, clients and suppliers.

Proactive media management may also display the entity's attitude and response to fraud positively, thus encouraging further external reporting as well as maintaining public confidence that fraud is a serious matter and will be handled accordingly.

Large entities with a significant number of fraud cases should use a communication strategy to plan the reporting of its various types of fraud in order to ensure the information is effective in targeting the relevant audience.

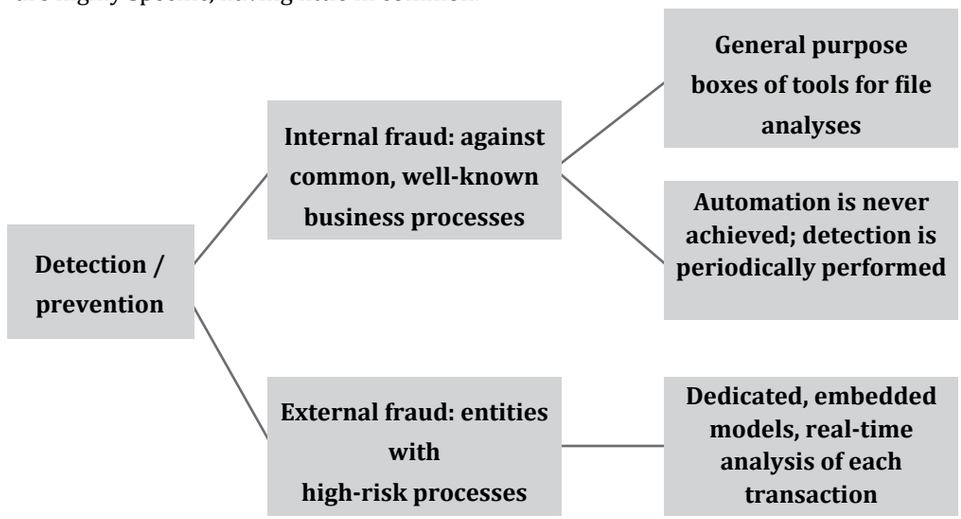
Chapter 5: Information Technology (IT) in Fraud Prevention and Detection

The setup and maintenance of a fraud prevention and detection framework based on IT requires the following procedure to be implemented:



It is clear that the whole implementation of IT-based fraud detection is based on the previous knowledge of an entity fraud profile and its exposures to specific types of fraud. Any new fraud episodes that may come along should add to such current knowledge.

There are two types of IT-based fraud prevention and detection tasks, those corresponding to internal and external fraud. IT tools and procedures used in each case are highly specific, having little in common.



IT-based detection of internal fraud

Internal frauds are more likely to be attempted in common, well-known business process areas such as Purchase to pay, Payroll or Order to Cash. The data-mining detection of internal fraud is a cumbersome task to be regularly carried out using several types of checks and tests in the entity's data files. Amongst others:

1. Classification of data,
2. Stratification or aggregation of files according to a given data field: totals or average purchases by employee, for instance.
3. duplication cases testing in one or in several files,
4. join, match and combine files in other possible ways,
5. compare similar files for differences, compare similar fields across different systems
6. perform statistical analyses of data fields

Some tools also include

1. automation of tasks and procedures, making regular detection easier.
2. complex AI and data analytical tests.
3. recording of procedures in a "log file" (required when generating audit trails that may support investigation and prosecution).

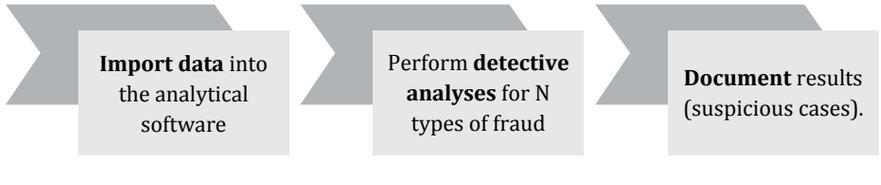
A few examples of internal detective tasks might be:

1. Look for duplicate payments of an invoice, possibly made fraudulently by an employee in collusion with a vendor. Look for duplicate purchases made using payment- or credit-cards within a short time. One of the purchases may be for personal use.
2. Compare recent and previous versions of master files of the entity's ERP database to see if the file has been changed in a fraudulent way.
3. Examine control settings of the same key files, searching for fraudulent changes: a manager may modify the permitted maximum purchase amount from 5,000 to 50,000 just during a few minutes.
4. Non-authorized expenses made by employees using payment-or credit-cards may be detected examining dates (weekend purchases

are suspect), the vendor code or the purchase description. Split transactions are also suspect.

5. Compare procurement (suppliers) and payments data with human resources records to search for "phantom vendors" schemes whereby invoices are paid to a made-up vendor - and other similar schemes set by employees to their advantage. Some type of loose matching is required in this case in order to overcome variations in the spelling and position of words.
6. Compute monthly total purchases by employee (fuel cards, meals' cards, air-tickets and hotel expenses, purchase- and credit-card use and others). Higher than usual level of purchases may indicate a case of fraudulent use of purchasing permission.

The procedure for internal fraud detection using IT comprises the following 3 steps:



Such procedure is carried out again and again for different types of data being analyzed.

IT tools for internal fraud detection basically are enhanced spreadsheets or OLAP cubes to be applied to Data Warehouse searches. Due to the existence of exceptions and false positives and also due to the inevitable changes introduced by entities in data format and location, in procedures and program releases, detection is a laborious and tedious task, difficult to automate and which requires familiarity with the entity's data, present and past, knowledge of data organization and skills spanning both IT and data analytics. It tends to be a well-paid job.

This type of data-mining task has similarities with Forensic Accounting tasks and with auditors' Analytical Review processes. Therefore, IT Tools available to detect internal fraud are similar to those used in the mentioned tasks.

Major players and internal fraud detection difficulties

Two well-known players (low- and high-end) are

- "IDEA", "CaseWare" (and other products) from "Audimation" http://www.audimation.com/ is aimed at small- medium-sized entities, not expensive, hands-on, offering little field support and training.
- ACL Analytics (and other products) from ACL http://www.acl.com is aimed at middle- large-sized entities, offering the full-range of services including the deployment of specialists into customers' sites.

Besides these two extreme cases, there is a multitude of other players.

Potential difficulties in the use of these tools:

1. In spite of vendors' claims, the task of importing data from the entity's files into the data-mining tool may prove to be extremely difficult or even impossible.
2. This type of task requires knowledge of where to look for fraud (a good quality risk exposure list, experience in detection methods and knowledge of the entity's data).
3. The task is unfeasible without trained staff familiar with the entity's organization details.
4. Some of the data-mining tasks require data to compare to (past data).
5. Most tests detect exceptions that are not frauds: they are true exceptions or "false positive cases". Knowledge and experience is the only guidance here. When false positives or exceptions are of many different types, the test becomes useless.
6. In spite of vendors' claims, the task is, as mentioned, not amenable to automation as it requires human knowledge, intuition, experience, common sense and especially discretion in making decisions. Reasons for human presence are

    a. Changes in an entity systems lead to the need to rebuild detecting processes.

    b. Exceptions and false positives must be recognized.
    c. Before accepting a case as suspicious, common sense must be exercised.

7. Time is required before effectiveness and efficiency is attained: it is a steep learning process until being acquainted with data patterns of the entity.

Tools for internal fraud detection

The following table details internal fraud detection tools.

Data Mining Technique	Description
Ageing	Produces aged summaries of data based on cutoff dates.
Append / Merge	Combines two files with identical fields into a single file: merge two years' accounts payable history into one file.
Calculated Field/ Functions	Creates a calculated field using data within the file: the net payroll pay to an employee could be recalculated using the gross pay field deducting withholding / taxes.
Cross-tabulate	Counts occurrences of character fields, setting them in rows and columns of cross-tabulated counts or percentages.
Benford's Law	Gives the expected frequencies of digits in tabulated data. Authentic, non-manipulated data exhibit known patterns. If a data set doesn't follow these patterns there may be a cause for review.
Duplicates	Identifies duplicate items within a specified field in a file: identify duplicate billings of invoices and others.
Export	Creates a file in different software format: Excel, Word. Export customer address information to Word for "Mail Merging to customer confirmation letters.
Extract/Filter	Extracts specified items from one file and copies them to another file, normally using "if" or "where" statement: extracting all balances over a predefined limit.
Gaps	Identifies gaps within a specified field in a file: identify any gaps in check sequence or others.
Index/Sort	Sorts a file in ascending or descending order: sorting a file by social security number to see if any blank or "99999" numbers exist.

Data Mining Technique	Description
Join/Relate	Combines specified fields from two different files into a single file using key fields, creating relational databases on key fields. It can also be done in an unmatched fashion to identify differences between data files.
Regression	Calculates a variable balance such as net sales based on other related variables: product purchases, inventory levels, number of customers, etc.
Sample	Creates random or monetary unit samples from a specified population.
Statistics	Calculates statistics on a selected numeric field: total positive items, negative items, average balance, etc.
Stratify	Counts the number, total dollar value, largest, smallest, and average of records of a population falling within specified intervals.
Summarize	Accumulates numerical values based on a specified key field: travel and entertainment expense amounts by employee to identify unusually high payment amounts.

The basic operations with files of records are:

Join by appending two files with similar attributes:

Month	Quantity	Amount	Customer
June	67	4020	45
June	39	2340	36
June	100	6000	37
June	243	14580	43
June	835	50100	45

+

Month	Quantity	Amount	Customer
July	120	7200	45
July	80	4800	45
July	60	3600	36
July	90	5400	43
July	600	36000	36

→

Month	Quantity	Amount	Customer
June	67	4020	45
June	39	2340	36
June	100	6000	37
June	243	14580	43
June	835	50100	45
July	120	7200	45
July	80	4800	45
July	60	3600	36
July	90	5400	43
July	600	36000	36

Join by matching two files with similar records:

Month	Qt.	Amount	Cus.
June	67	4020	45
June	39	2340	36
June	100	6000	37
June	243	14580	43
June	835	50100	45

+

Ivoice	%
AA3443	5%
AA3444	0%
AA3445	0%
AA3446	0%
AA3447	5%

→

Month	Qt.	Amount	Cus.	Ivoice	%
June	67	4020	45	AA3443	5%
June	39	2340	36	AA3444	0%
June	100	6000	37	AA3445	0%
June	243	14580	43	AA3446	0%
June	835	50100	45	AA3447	5%

Sort one file by a given attribute (in this case it is “customer”):

Month	Quantity	Amount	Customer
June	67	4020	45
June	39	2340	36
June	100	6000	37
June	243	14580	43
June	835	50100	45
July	120	7200	45
July	80	4800	45
July	60	3600	36
July	90	5400	43
July	600	36000	36

→

Month	Quantity	Amount	Customer
July	60	3600	36
July	600	36000	36
June	39	2340	36
June	100	6000	37
July	90	5400	43
June	243	14580	43
July	120	7200	45
July	80	4800	45
June	67	4020	45
June	835	50100	45

Aggregate records by a specified attribute (in this case it is “customer” and summarizing other attributes (adding, averaging or finding last values):

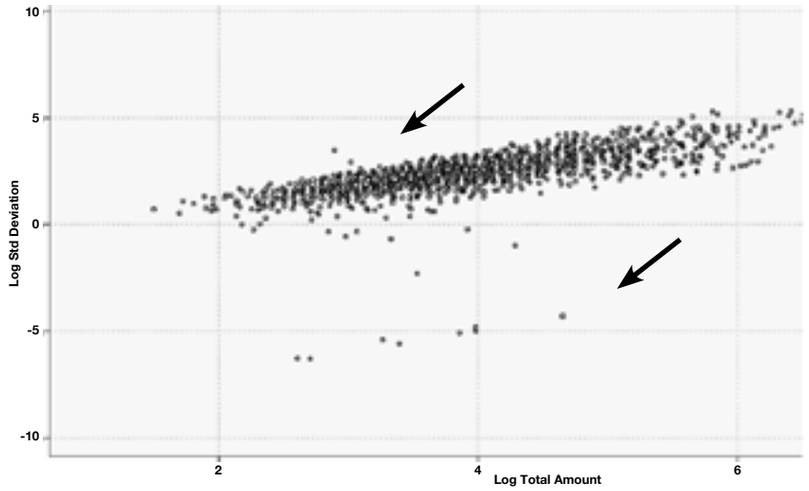
Month	Quantity	Amount	Customer
July	60	3600	36
July	600	36000	36
June	39	2340	36
June	100	6000	37
July	90	5400	43
June	243	14580	43
July	120	7200	45
July	80	4800	45
June	67	4020	45
June	835	50100	45

→

Last M	Quantity	Amount	Customer	No_tran
July	699	41940	36	3
June	100	6000	37	1
July	333	19980	43	2
July	1102	66120	45	4

Aggregation may be used to detect uncommon groups of cases in several different ways. For example, in a file containing a large quantity of payments made to suppliers, it is good practice to aggregate records by supplier and observe the relationship between suppliers' average of the logarithm of payments and the suppliers' standard deviation of the same logarithm of payments. Given that the relationship between average logarithmic values and the corresponding standard deviations is bounded within a given region, any suppliers which are outside such region are worth observing in more detail.

A process leading to the corresponding analysis of suppliers is illustrated below, in the form of a data-processing flow.



A cross-tabulation is a counting of the number of cases belonging to two discrete attributes. The number of purchases made by 4 customers during 2 months would generate the following cross-tabulation:

Month	Customer			
	36	37	43	45
June	2	1	1	2
July	2		1	2

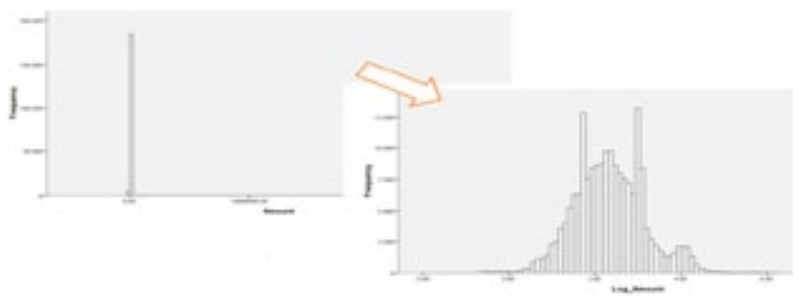
In the example above, it is verified that customer 37 didn't make any purchase in July. Cross-tabulations are a powerful way of summarizing counts, frequencies or percentages of the total.

A one-dimensional tabulation is a frequency distribution. "Distributions" are lists of possible states of an attribute, together with the number of cases observed in each of such cases. For example, the summation of the purchases for both months would be a distribution of the attribute "customers" having 4 states.

Distributions summarize counts, frequencies or percentages of a total. As such, they are effective in detecting any abnormal number of cases.

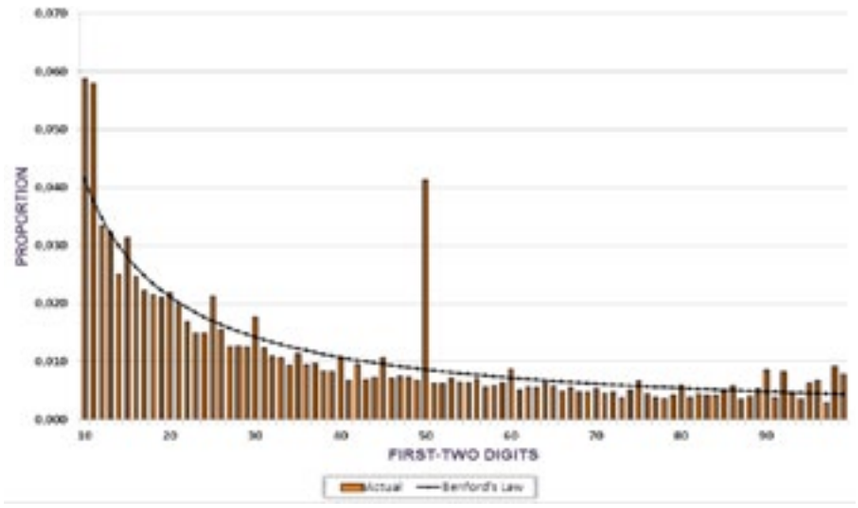
When states are continuous, for example, in the case of money amounts, logarithmic-transformed values should be used in distributions so as to allow interpretation.

Due to their lognormal character, distributions of non-transformed money amounts are not capable of conveying any useful information, as depicted in the example below, in the left-hand side. After the logarithmic transformation takes place, however, distributions become informative. Below, in the right-hand side, 3 values stick out as more frequent than expected while the whole of the distribution is shown to be bimodal (two distinct groups of transactions with separate distributions).



The "Benford's Law" is another case of distribution interpretation. It is based on the fact that, in large series of money transactions, the frequency distributions of first and second digits of such transactions' amounts exhibit a regular, well-known pattern. When invented or erroneous amounts are introduced in such series, however, frequency distributions patterns change denouncing such spurious amounts.

In the example below, the unexpected existence of numbers beginning by 10, 11, 15, 20, 25, … may denote a "rigged" set of transactions. But the exaggerated frequency of numbers beginning in 50 has a simple explanation as it corresponds to a standard posting fee.



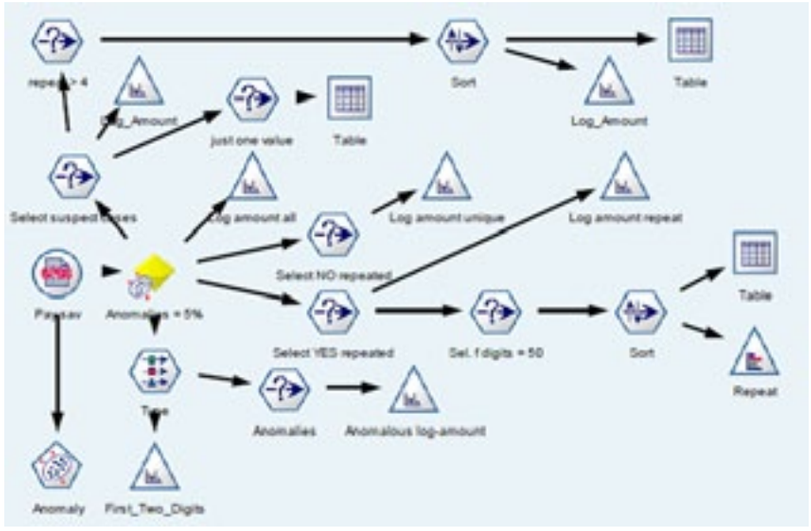
The difficulty posed by tools such as the Benford law is not the discovery of unusual patterns but the separation between unusual patterns that are non-fraudulent from others that are.

Examples of data-analytical internal fraud detection tasks

More complex tools can be used in the detection of internal fraud. The anomaly detector, for instance, is a type of "Cluster Analysis" designed to isolate records with anomalous attributes (that is, attributes which, on the whole, form an uncommon pattern) in data files. Detection is based, not just on the usual attributes measuring money amounts, locations, employee, customer or supplier codes, or industry type, but also on relative positions (proximity) of records according to the time period. Depending on the analyst,

the algorithm will output a desired percentage of most anomalous records. The example below examines the 5% most anomalous cases in a large file containing payments made by a company.

The data-flow process aimed at detecting anomalous records is apparently complicated:

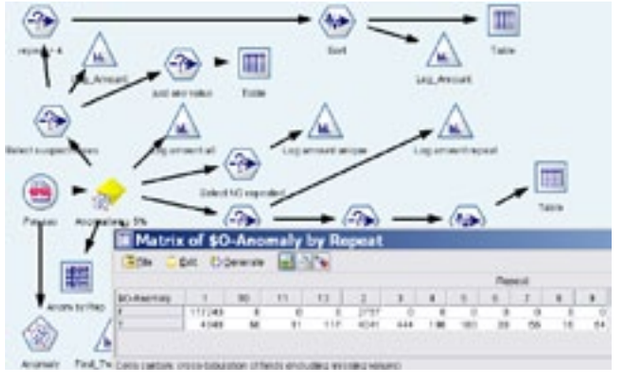


In fact, however, such data-flow is just a collection of searches and examinations of repeated invoice numbers, unexpected frequencies, namely of the two initial digits in payments, cases considered as anomalous and the crossing between them.

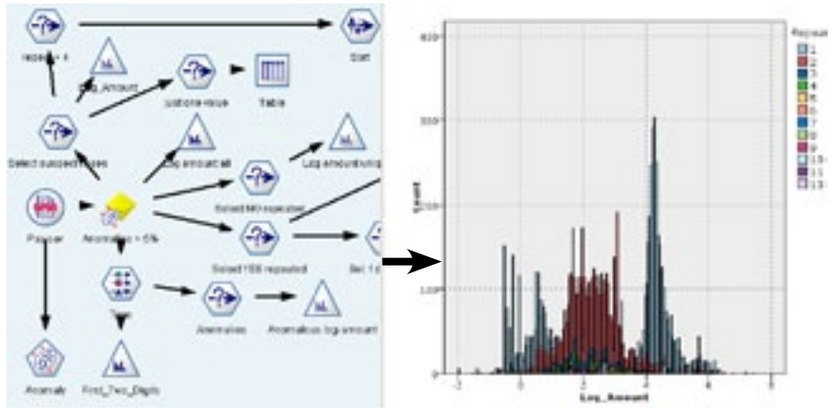
After the file is input into the process, the anomaly algorithm generates the anomaly identifier . From this point on, interactive graphic tools are used to identify cases worth observing more closely. Such cases are then selected and examined with the help of cross-tabulations , other graphics and sorted lists .

Inputs to the anomaly tool are the year, month, day of the month, day of the week, the supplier code, the invoice number, the payment amount, the initial two digits of such amount, the logarithm of the same amount and the number of invoice repetitions found.

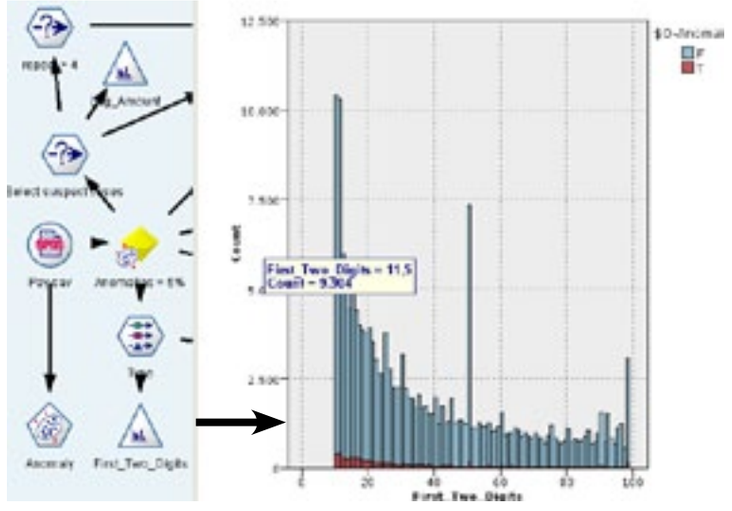
First, it is verified, using a cross-tabulation, that the 5% percentage of anomalous cases comprises all repetitions above 2 while there are non-anomalous non-repeated cases:



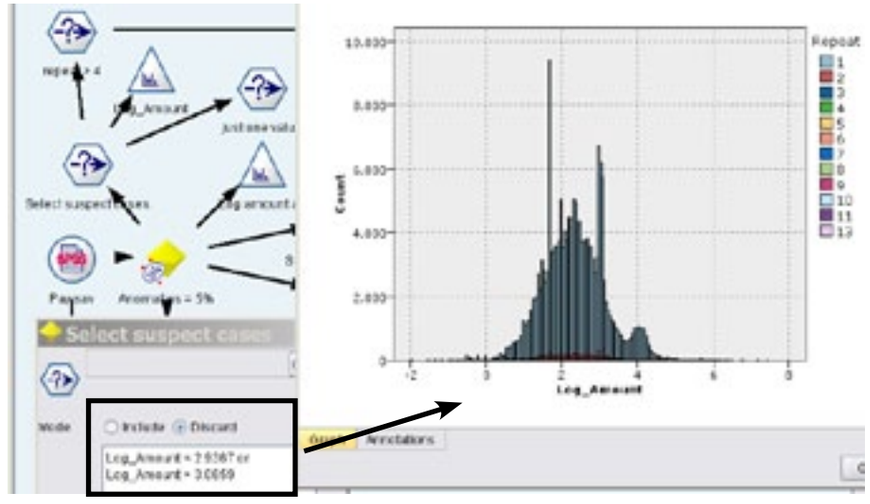
The anomalous amounts are now examined for different number of repeated invoices. Iterative graphic tools are extremely useful in identifying peaks or outliers in distributions. With them, it is easy to isolate the distributions of the logarithm of amounts for repetitions between 3 and 13. Several suspect cases are found and examined using this procedure.



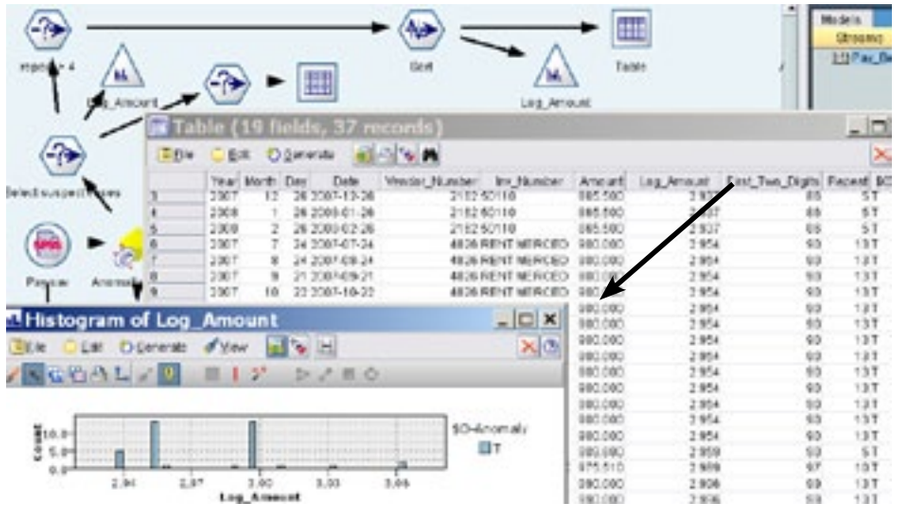
As mentioned, Benford graphics of the two initial digits of payment amounts are also employed to compare anomalous with non-anomalous records. In the case at hand, tow such graphics were compared, one for non-repeated invoices and the other for repeated invoices as shown below:



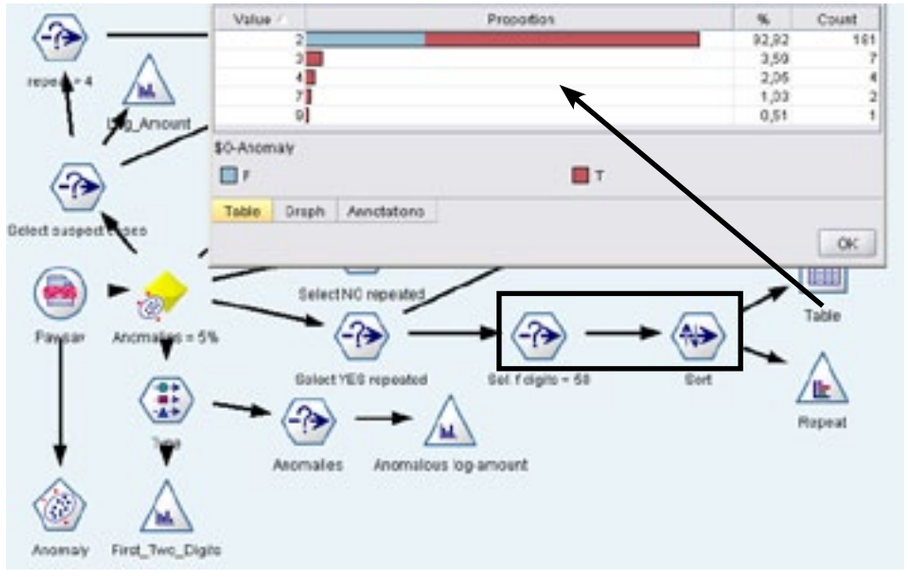
It is clear that most of the peaks are repetitions, some of them in non-anomalous records. Therefore, peaks in repeated records are examined graphically. In the case exemplified here, the peak contained in the interval 2.9367 to 3.0859 (log amounts corresponding to around 900 USD) is isolated and all the records contained therein are examined.



From this selection, those anomalous cases are observed closely. After being sorted by payment amount and by invoice number, several suspect payments are listed.



All the remaining records registering amounts with the two initial digits of 50 and marked as repeated are now examined closely.



This search leads to another set of suspect records. As mentioned, the highest peak (around 50 USD) is not a suspect but a quite expected feature as this amount is the posting fee.

The example just presented is necessarily limited in scope but it shows the cumbersome type of searching tasks required to detect fraud internally. The use of IT tools, namely data-mining tools, is indeed helpful but the whole process is far from being automatic.

Most common suspect transactions

An extensive list is now presented, showing symptoms which may indicate fraud associated with a given transaction. The source is an ACL pamphlet available at www.acl.com/fraud . The list is organized according to the type of transaction examined.

Payments made to suppliers and to other entities: the most suspect transactions are

- Payment orders with blank or zero amounts
- Split payment orders: multiple, just under the approval threshold
- Duplicate invoices: same number, amount on date, vendor on amount
- Invoice amount paid is larger than goods received
- Invoices with no matching receiving report
- Multiple invoices for same payment order and date
- Pattern of sequential invoices from a vendor
- Non-approved vendors, purchases of consumer items
- Employee and vendor with the same: name, address, phone number, bank account,
- Vendor address is a mail-drop
- Payment made without invoice
- Vendor master file: changes observed during brief periods

The use of purchasing cards (all types, including credit and debit cards)

- Purchases of consumer items
- Suspect vendors
- Prohibited merchant codes
- Transactions made on weekends or holidays
- Split transactions (multiple items under threshold)
- Duplicate purchases (same item multiple employees)

Anomalies in the "order to cash" process (all transactions, beginning with an order from a customer till the payment is received from the same customer):

- Unusually high sales discounts
- Unusually high credit terms/credit limits
- Frequent credit memos to the same customer
- Shipments where employee address matches the shipment address

Payroll and human resources:

- Terminated employees still on payroll
- Multiple employees with same address
- Unusually high amounts and rates
- Invalid social security numbers
- Unusually high commissions

These are the most common sources of suspicion. It is clear that their detection requires the existence of a centralized, well-organized, well-kept and updated data in the part of the organization, together with the ability to reconcile several files, some of them external. The quality and availability of data is the true difficulty when using IT to detect fraud.

IT-based prevention and detection of external fraud

Externa fraud is likely to be attempted in specific institutions and processes such as:

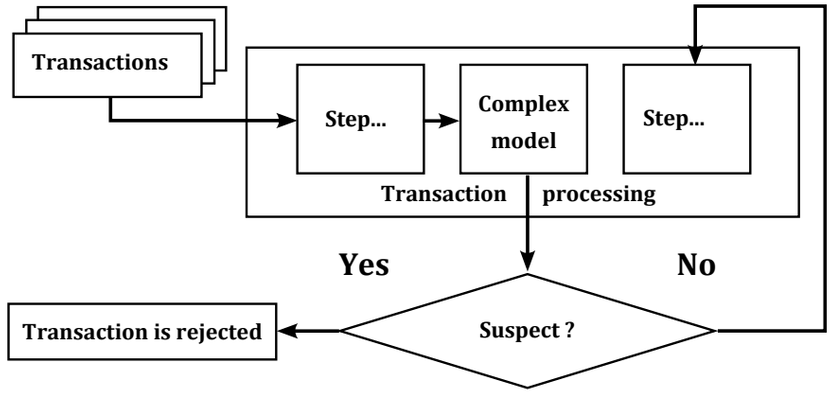
- Insurance: false claims or false statements
- Bank loan: false statements
- Healthcare: false billing
- Retail post-of-sale or Internet credit card fraud
- Telecom billing fraud

and similar. Particularly relevant is identity theft, which is a first step towards several types of fraud and other criminal activities, namely money laundering.

The detection of attempted external fraud is currently carried out in real time by

embedding, inside the transaction processing software, one or several complex models able to check the plausibility of transactions. Basically, it is a preventive task.
Although models used in external fraud detection are complex, the detection process is itself simple and transparent. Most of the transactions are expected to be classified as non-suspect; however, once in place, a fraud-detection model will inevitably require the support of staff in order to separate unlikely from likely suspects. This decision cannot be made automatically.

IT-based external fraud detection may be depicted thus:

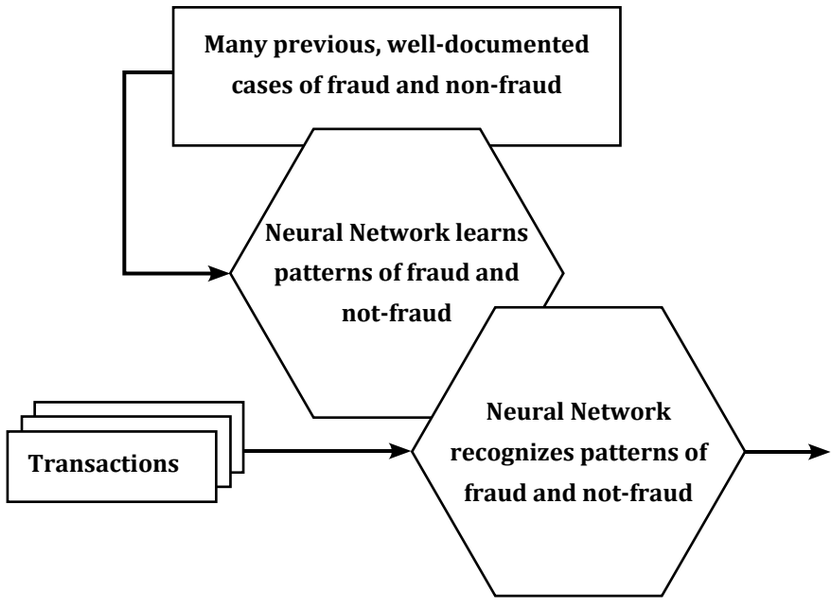


Typical complex models for external fraud detection use Neural Networks and other algorithms available, such as Support Vector Machines, Cluster Analysis or Rule Induction.

Large accumulated experience (a large, well-documented basis of previous cases) is required, so that the algorithm may learn the fundamentals of each fraud's "pattern". After learning such patterns, those complex models generated by the algorithm can then be used to recognize transactions where such patterns exist, separating them from transactions where suspect patterns are not present.

Therefore, a previous process is required consisting on the learning or training of the algorithm; such process is based on the existence of good quality data.

After learning has taken place, then the resulting model can be put in place so as to identify suspect transactions, that is, transactions where patterns resemble fraudulent transactions.



The quality of fraud detection will depend, not so much on the sophistication and complexity of the algorithm, but essentially on the abundance, reliability and completeness of the data-set employed to train the algorithm. However, it should be noted that most of the algorithms available are task-specific and cannot be used to perform tasks outside their specificity.

Major players and potential difficulties in the use of complex models

Potential buyers of complex model's solutions should be keenly aware of the following:

1. Complex models require the existence of many, good-quality, well-documented data on fraud and non-fraud so that they may learn the underlying pattern. Each type of fraud requires its own dataset. In some cases such data does not exist or is small.
2. Complex models are expensive, both in the investment required, in maintenance, support and updating. Typically, only large entities implement them.
3. Contracting of one such vendor is "a marriage for life" affair. The getting out is difficult, expensive and especially, it may be highly disruptive.

4. Some fraud areas are not yet contemplated by extant research. Credit card transactions are the object of much research and results are good. But some other areas are not so thoroughly researched and results are not convincing.
5. In such less developed areas the number of false positives is high which prompts otherwise good customers to seek alternative companies.

Players in this area are the same as in other areas requiring complex analytical solutions such as risk management and Basel III compliance in the Banking Sector, actuarial modes for Insurance companies, Business-Intelligence solutions for targeted marketing and CRM, internet intelligence gathering, internet marketing and others. Examples of such players are:

- IBM Counter Fraud Management (for Banking, healthcare, Insurance, Government) http://www-03.ibm.com/security/counter-fraud/solution/index.html
- ACL may detect external fraud through continuous transaction analysis in, for example, SAP software http://www.acl.com/solutions/products/acl-direct-link/
- SAS Institute, SAS security intelligence http://www.sas.com/en_us/software/fraud-security-intelligence.html stand-alone solutions that work with several transaction processing software.
- ORACLE (Financial Services division) may have fraud-detecting models embedded in their transaction-processing products http://www.oracle.com/us/products/applications/financial-services/fraud/index.html
- SAP may provide native fraud detection models embedded in their transaction-processing products http://www.sap.com or may accept models from other vendors.

The initial three vendors are dedicated to analytical solutions whereas the last two vendors offer entity-wide solutions inclusive of, but not limited to analytics.
Fraud detection based on complex models is progressing every year and technologies must follow such changes. When selecting a proposed solution, the most important characteristics to be considered are proximity, flexibility and transparency.

1. Proximity: without a great deal of support and training an organiition will not be able to take advantage of this type of applications. These tools require in-house support, not just during a few months but during an unlimited period. Support and training is the most important of all. If a vendor offers deficient support in Macau / HK, it cannot be chosen.
2. Given the complex and changing nature of solutions, flexibility comes next in importance. Vendors must be able to correct and improve existing releases without excessive costs to organizations.
3. Finally transparency is demanded by common sense. The lack of transparency has caused legal difficulties to many organizations. Besides detecting fraud, solutions must be able to explain how fraud was detected and the confidence associated with such detection.

Example of complex modelling: financial misstatement

The first example is a financial misstatement detecting tool. This type of fraud is committed internally but, since it involves publicly available reports, it can be detected externally, that is, without necessarily having to access and audit internal data.

As mentioned, the misstatement of financial statements is one of the most widespread types of fraud, together with asset misappropriation (an internal type of fraud) and corruption (a complex type, typically involving internal and external agents).

Appendix A offers an extended discussion of the misstatement of financial statements.

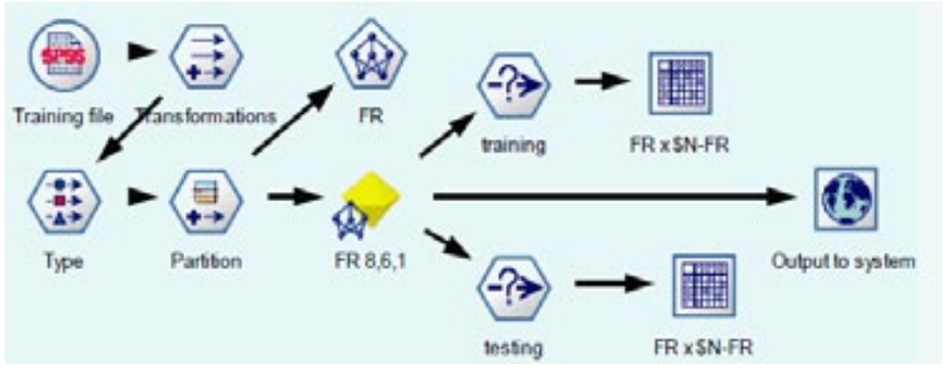
This example uses a Neural Network which has been trained to differentiate the patterns of fraudulent from those of non-fraudulent statements. Such training requires the pre-existence of a trustworthy data set where many instances of fraudulent and non-fraudulent reports are gathered. In the present case, the data-set is organized as a table or file with attributes such as the following (and others):

Key / year	Fraud	Company name	Industry	Size	Cash	Receivables	Property	Assets
0105151986	NO	TEXON ENERGY CORP	2010	3	0,08	1,92	7,32	12,34
0071551990	YES	MCDONNELL DOUGLAS	2010	10	226,00	3.781,00	3.253,00	14.965,00
0231231993	NO	MICROLYTICS INC	4510	2	0,16	0,15	0,17	3,33
0121411998	YES	MICROSOFT CORP	4510	10	13.927,00	1.460,00	1.505,00	22.357,00
0075852002	NO	MOTOROLA INC	4520	9	6.566,00	4.437,00	6.104,00	31.152,00
0116362000	YES	XEROX CORP	4520	10	1.741,00	7.378,00	2.495,00	29.475,00
0011642001	NO	MCI INC	5010	9	1.409,00	4.634,00	36.792,00	91.901,00
0061272000	YES	ENRON CORP	5510	10	1.374,00	12.270,00	11.743,00	65.503,00

Values are in millions of US$. There is a total of 1,200 cases, 600 frauds, matched with 600 non-frauds. Of these, half are used to train the Neural Network and the other half are used to test the accuracy of fraud detection.

Each record contains financial statement data (accounts and other) and each misstatement is matched by industry and size with a sound statement.

The major steps in the whole process are depicted as a data-processing flow:



Such data-processing flow can be summarized in 7 major steps:

1. The data-set described above is input into the model (symbol in the data flow displayed below).
2. Numbers taken from accounts are appropriately transformed .
3. Preliminary calculations are also made, leading to the selection of a set of relevant attributes (accounts in this case) to be used by the Neural Network (not shown).

4. Input and target attributes are defined so that a Neural Network algorithm may learn patterns from data. Fraud or no-fraud (the two states of the target attribute in this case) is predicted from the transformed accounts. Accuracy, balance and other characteristics of the resulting model are assessed .
5. When the modelling process is finished, the Neural Network has learnt the relationship capable of explaining fraud and no-fraud based on financial statement numbers. Neural Network resulting model thus created is now made available for the detection of unusual patterns.
6. New cases can now be input to the model, transformed and presented to the model created by the Neural Network (not shown).
7. Diagnostics (financial statements identified as likely frauds and non-frauds) are then output into the external system.

Typically, complex models such as the one depicted here, are able to accurately predict 87% of cases in average. The remaining 13% are either "false-positives" (non-fraud cases predicted as fraud) or "false-negatives" (fraud cases which go undetected).

Both "scores" (indices) and fraud likelihoods can be estimated from the model output. Scores and likelihoods are useful in deciding whether a given transaction is worth observing closely or not.

Example of complex modelling: farm grant claim

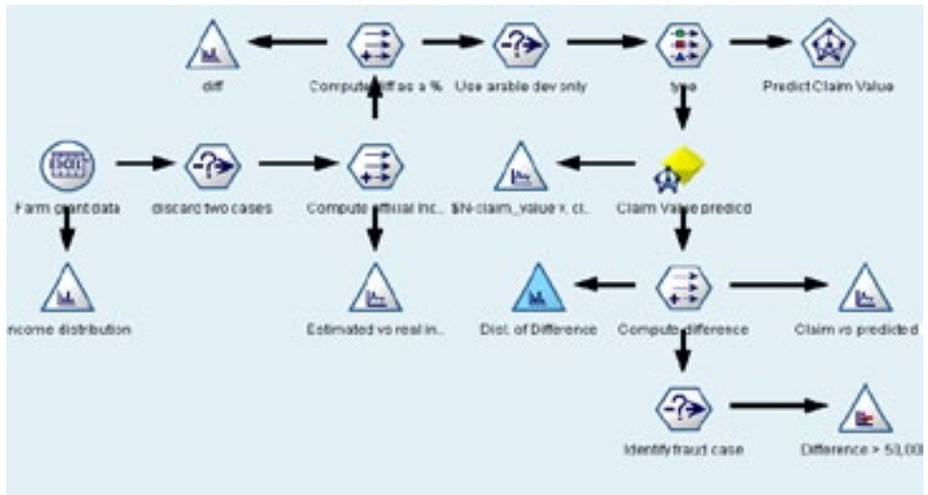
The following example uses a Neural Network where amounts claimed by farmers in their applications for grants are compared with predicted claim values based on farm size, crop type, rainfall and other data.

First, the complex model requires instances of fraud and non-fraud cases from which the Neural Network can learn patterns of fraud and non-fraud. In the present case, all the 298 instances (claims) available are organized in a file or table with the following format:

id	region	farm size	rain fall	land quality	farm income	crop	claim type	claim value
id601	midlands	1480	30	8	330729	wheat	decommission_land	74703
id602	north	1780	42	9	734118	maize	arable_dev	245354
id603	midlands	500	69	7	231965	rapeseed	decommission_land	84213
id605	north	1700	46	8	621148	wheat	decommission_land	122006
id606	southeast	1580	42	7	445785	maize	arable_dev	122135

... total of 298 claims

The whole model is depicted as a data processing flow:



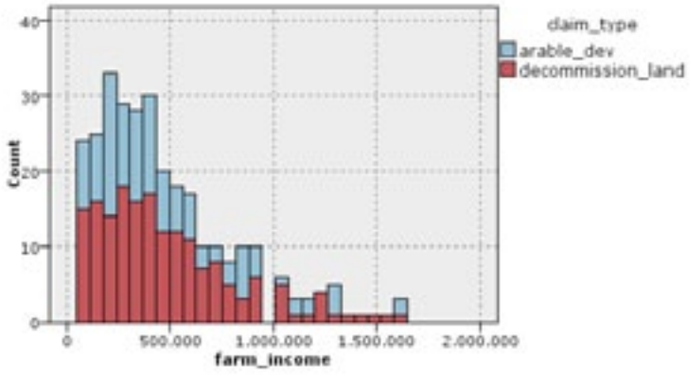
The modelling process requires, in this case, the execution of 7 data-processing steps.

8. Data is input into the model (symbol in the data flow displayed below).
9. Transformations and the selection of cases are then performed.
10. Preliminary calculations are also made, leading to expectations regarding the claim value based on an official formula. Such expectations are added to the set of attributes available for prediction. Claims belonging to one of the two types, arable land, are put aside at this stage.

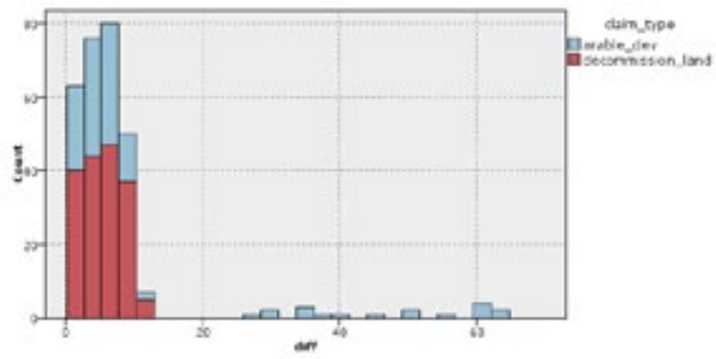
11. Input and target attributes are defined so that a Neural Network learns from the data provided : the claim value (the target attribute in this case) is predicted from other attributes in the file, such as rain fall, farm income, farm size, main crop and the mentioned expectations.
12. When the modelling process is finished, the Neural Network has learnt the relationship capable of explaining claim values based other attributes. Neural Network model thus created is now made available for the detection of unusual patterns.
13. Predicted claim values are compared with the real values and the largest differences are examined as candidates to fraud.
14. Claims which were identified as likely frauds are then output into the external system (not shown in the data flow below).

Some further details are now offered.

Below it is shown that farm income is, similarly to most other types of income, distributed lognormally. The frequency distribution also shows that the majority of claimants want to use the proceeds to decommission their land while others want to develop arable land.

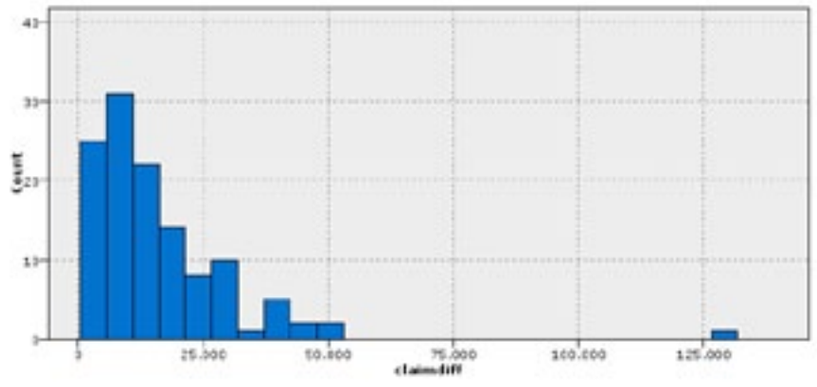


Expected farm income is calculated using a legal formula involving farm size, land quality and rain fall. Then, the percentage difference between expected and real income shows a distribution (below) where only cases of claims for arable development display significant differences in relation to the official formula. Therefore, only such cases are scrutinized.



The following step consists of creating the predicting model based on the Neural Network. After the model is built, it is used to predict the claim that would be predicted, not the real claim, based on existing variables.

It is found that the difference between claims and the values which the Neural Network predicts as claim values is distributed in such a way as to show a clear case of exaggerated claim (figure below).



The model was able to detect unusual claims based on past experience. External fraud prevention contains similar steps applied to distinct types of data.

Appendix A: Financial Misstatement

The 2010 Report to the Nations on Occupational Fraud and Abuse, from the US Association of Certified Fraud Examiners (ACFE 2010) estimated that fraud cost US companies $400 billion annually. Some estimates suggest an even higher figure. Thus fraud is a significant problem for which preventive and detective remedies are needed. Fraudulent activities of interest include asset misappropriation, purchasing transactions fraud including card fraud, internal reporting fraud, and financial statement fraud. This appendix is concerned with the latter.

In 2001, following the ENRON scandal, worldwide legislators enacted a series of laws which better identify responsibilities and aggravate the punishment level associated with financial misstatement. The Sarbanes-Oxley low is an U.S. instance of such laws. But in spite of all the measures put in place to punish fraudulent book-keeping, manipulation is still ongoing, probably in a huge scale.

Investigation of accounting fraud is known as “forensic accounting”. As part of the audit process, auditors are required to estimate the possibility of management fraud. The AICPA, the professional body of auditors in the U.S., explicitly acknowledges auditors’ responsibility for fraud detection. Such responsibility is seldom demanded from auditors but such situation will have to change.

Analytical review procedures are the tools used by auditors to detect fraud, mistakes and inadequate practices. Such tools determine whether a financial statement contains items and relationships that are unusual. Analytical review procedures may vary depending on the kind of institution involved and the amount of financial information under review but they typically range from simple basic comparisons of items to complex analytical models of relationships.

Analytical review procedures are of three types:

- non-quantitative,
- quantitative and

- advanced quantitative techniques, which include sophisticated methods derived from probability theory, statistics and artificial intelligence.

The general belief exuding from a review of the extant literature is that analytic procedures alone are rarely effective in detecting fraudulent activities relative to financial statements. This seems to follow from the fact that most of such fraudulent activity is carried out at the top level of the organization. Company books are "cooked" by managers with the assistance of accountants, not so much by clerks. And the detection of management fraud is a difficult task when using normal audit procedures since:

1. There is a shortage of knowledge concerning the characteristics and modus operandi of management fraud.
2. Given its infrequency, most auditors lack the experience necessary to detect it.
3. Finally, managers deliberately try to deceive auditors thus making detection especially difficult for auditors.

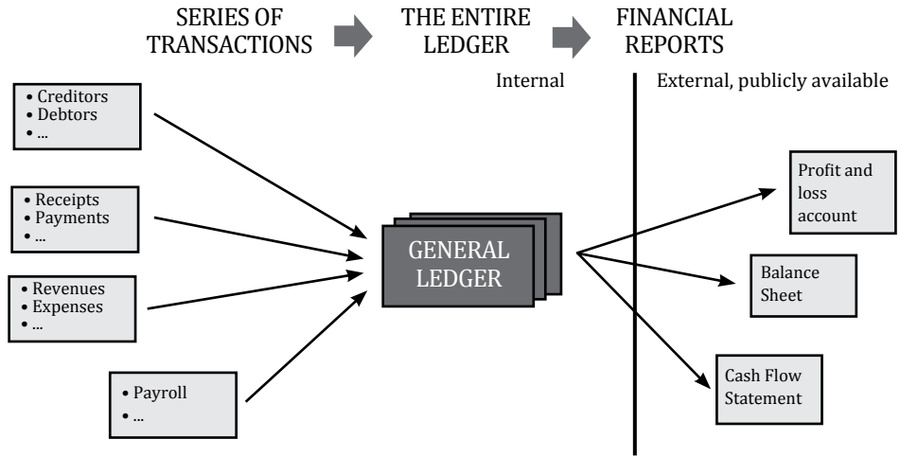
There is a need for more effective procedures, capable of better detecting management's fraudulent misstatement of accounts.

In response to such concerns about audit efficiency and effectiveness, advanced quantitative techniques such as the statistical modelling of relationships underlying the data is being used in place of and as a supplement to substantive tests of details in analytical review processes. But in order to achieve efficiency and effectiveness when using this type of procedure the analyst must possess expertise in statistical modelling and a first-rate knowledge of the data. In general, however, such expertise is difficult to reconcile with other pre-requisites. Auditors are thus in need of appropriate, effective support.

Probably the most widespread quantitative technique employed to detect fraudulent transactions is Benford's Law, stating that the digits in many real-life data sets are not distributed uniformly, the left-most digit in a set of numbers being biased in the direction of smaller values. A set of numbers satisfies Benford's Law if the leading digit d ($d \in \{1, \ldots 9\}$) occurs with probability $P(d) = \log(d+1) - \log(d)$. Deviations from Benford's Law are seen as red flags that suggest an elevated risk of fraud or error. The series of tests related to Benford's Law is called the Nigrini Cycle. They include first-

and second-order tests, summation tests, number duplication, last-two digits tests and other analytic methods aimed at detecting fraud in a continuous monitoring setting. It is possible to combine all such tests in a risk-score which aggregates fraud evidence on several predictors.

Nigrini methods are helpful at the internal detection level but, again, they are ineffective in detecting fraud committed by manager at the top. The alternative is to use complex modelling to detect, not fraudulent transactions, but fraudulent published financial statements, that is, the final result of the Accounting procedure, not its constituting parts as depicted below.



It has also been mentioned that the increased emphasis on the use of complex models capable of assessing the likelihood of fraud by examining published financial statements, not the books and sets of transactions from which such published financial statements are created, is at odds with the auditing profession's position regarding fraud detection, since most material frauds originate at the top levels of the organization, where controls are least prevalent and effective. The extant methodologies' limitations should motivate researchers to extend and advance the application of forensic analytics in detecting fraudulent financial reporting in an effort to refute the general viewpoint that these techniques are ineffective.

Complex modeling tools such as Neural Networks are used to compare fraudulent and non-fraudulent reports thus learning fraud patterns from example. Results from a Neural Network model comparing 400 fraudulent with 400 no-fraudulent financial statements, indicate that sound financial statements have boards with significantly higher percentages of outside members than fraudulent boards. This is a significant, yet expected result.

Complex models also use a-priori knowledge about how is fraud committed: financial distress may be a motivation for management fraud; high debt structure may increase the likelihood of fraud; the need for continuing growth is also fraud-trigging.

As for the actual method used to distort the books, examples are the recording of sales before they are earned, the manipulation of inventories or failure to match sales with the corresponding cost of goods sold and several others, as listed in Appendix C.

To sum-up, accounting fraud detection tools are of two types:

1. Tools aimed at detecting transaction fraud. They examine internal data thus they are used by auditors. An example is the Nigrini Cycle.
2. Tools aimed at detecting fraud in publicly available financial statements.

The latter can be used by any party interested, not just auditors concerned. Complex models such as Neural Networks and other Artificial Intelligence tools are employed to identify suspect statements.

Considerable effort has been devoted to the development of software to support the detection of fraud in published financial statements of companies. Until the present date, however, the applied use of such research has been extremely limited. A demolishing fact about the external tools described above is that practitioners do not use them because models are far too specific, difficult to implement, they suffer from inferior generalization capability and, most important of all, are “black boxes”: results seldom can be explained to auditors. Since auditors are responsible for their decisions, tools must be transparent in their diagnoses. The cumbersome input task these tools require also precludes their applied use.

An application developed at MESA, in Macau under the sponsorship of the special administrative region’s scientific funding body (FDCT) solves the above problems while significantly improving performance. It is based on Web-mining and on the use of three Neural Networks where a modified learning method leads to the formation of meaningful internal representations. Such representations are then input to a features’ map where trajectories towards or away from fraud and other financial attributes are identified. The result is a Web-based, self-explanatory, financial statements’ fraud detection solution. The list of representations presently in use is as follows:

1. Logarithmic-transformed ratio of Liabilities (total) to Assets (total)
2. Logarithmic-transformed ratio of Cash and Short Term Investments to Revenue (total)
3. Logarithmic-transformed ratio of Long Term Debt to Common Stock (equity)
4. Logarithmic-transformed ratio of Receivables (total) to Common Stock (equity)
5. Logarithmic-transformed change in Liabilities (total) in relation to previous year
6. Logarithmic-transformed ratio of Revenue (total) to Common Stock (equity)

Using these 6 predictors, a predicting accuracy of 86% is expected.

Appendix B: Asset misappropriation

Asset misappropriation is the most frequent type of internal fraud. It is also extremely varied, so much so that it became known as “the fraud tree” due to its numerous branches. This appendix closely follows an excellent introduction using such name, issued by the Association of Certified Fraud Examiners of the U.S.

In what concerns fraud, there are only three major asset types: cash, inventories and all the rest. Fraudsters clearly favor misappropriating cash: nearly nine in 10 illegal schemes uncovered involve cash. The reasons should not be surprising: cash is fungible, has a specific value and is easily transported. Inventory—except for consumer goods and metals such as copper—has limited usefulness to a thief; an employee in a factory can have a hard time converting the loot into cash. And of course, many business enterprises don’t have a physical inventory.

On the branches of the fraud tree are three, already mentioned main ways to embezzle cash: skimming, larceny and fraudulent disbursements.

1. Skimming can be described as the removal of cash prior to its entry into the accounting system. Here are some examples:
    a. The manager of a movie theater skimmed $30,000. During the theater’s slow times, when he thought he was not being observed, the manager would print a viewer’s ticket but keep it for himself and allow the customer to enter the movie without a ticket. Then during busy times, he would resell the tickets he had withheld and pocket the cash. The manager was caught by an alert employee who happened to pass by and saw what he was doing.
    b. The manager of a retail store with six cash registers brought in his own register and set it up in an empty checkout lane. All sales going through the seventh register went directly to the manager. This scheme went undetected until a physical count showed huge inventory shortages.

c. A government mail-room employee skimmed more than $2 million in taxpayer refund checks that had been returned by the post office for bad addresses. The employee, with the help of several outside accomplices, was able to deposit the stolen checks into various banks and withdraw the proceeds. The scheme was uncovered when a taxpayer called about an overdue refund and found out that his check had already been cashed.

2. Larceny is the removal of cash from the organization after it has been entered into the records. Most of these schemes are detected through bank reconciliations and cash counts. Larceny is therefore not one of employees' favorite illicit methods; it accounted for only 3% of the cases and 1% of the losses. Here are some examples of cash larceny:
   a. A bookkeeping employee, responsible for posting accounts receivable in a small business, stole some of the cash payments but nonetheless posted the transaction to the company's accounts-receivable detail. Withinmonths, the theft had risen to more than $200,000, seriously depleting the business's cash. When a bank reconciliation revealed a major discrepancy between the accounts-receivable detail and cash, the scheme was uncovered.
   b. An employee in charge of taking the company's money to the bank would regularly remove currency, then alter the company's deposit slip to reflect the lower deposit amount. The worker, obviously not an accounting genius, didn't realize the discrepancy would be discovered when sales and cash were reconciled.

3. Research on 732 fraudulent disbursement cases showed that they can be subdivided into at least six specific types:
   a. check tampering,
   b. false register disbursements,
   c. billing schemes,
   d. payroll schemes,

   e. expense reimbursement schemes and
   f. other fraudulent disbursements.

In the following, a few common examples are given.

   a. A purchasing agent for a major corporation set up a vendor file in his wife's maiden name, then went on to approve more than $1 million in company payments to her. The supporting documentation consisted of the wife's invoices for "consulting services" that were never rendered. A clerk in the purchasing department, suspicious of the agent's recent purchase of a new boat and car, uncovered the scheme.
   b. The CEO of a small nonprofit agency stole $35,000 from its coffers by submitting "check requests" to the accounting department. The checks were made payable to outside bank accounts the CEO controlled. The accounting personnel, fear ful of angering the boss, made out the checks and delivered them to him. One accounting clerk finally had enough and alerted the outside auditors, who confirmed the disbursements were not legitimate.
   c. A worker for one company submitted an expense reimbursement for a trip he supposedly took for business purposes. Actually, he took his girlfriend to a bicycle rally and attempted to charge the expense to the company. One problem: On his itinerary, the worker listed the independent auditor who was examining his expense reimbursement as his traveling companion—not a smart move.

Employees who set up dummy companies for fraudulent disbursements often give clues to their activities. They will use their own initials for the company name, rent a post office box or mail drop to receive checks, or use a dummy company name and their own home address.

Regardless of the method or the asset involved, all asset misappropriation has the same effect on the books of an organization. Take the following actual case as an example.

A seemingly respectable grandmother stole $416,000 from a small store where she had been employed for 20 years as a bookkeeper. She confessed that she'd been rigging the books for eight years. This crime is typical of the risk to small business.

The store's accountant prepared only the company's tax returns, so the business was not audited. The fraudster also acted as the store's "accounting department." She made deposits, signed checks and reconciled the store's bank account. This situation, absence of separation of functions, is the most direct way for many frauds.

After 12 years of unrelenting temptation, this person finally gave in. Thereafter, for years, she systematically stole money from the store using the same method. She would make out a company check to herself (in her own true name), sign it and deposit the proceeds in her personal checking account. To cover the theft, she would do three simple things: First, she entered "void" on the check stub when she wrote the check to herself. Next, she would add the amount of the theft to the check stub when she paid for inventory. For example, if she took $5,000 and was paying a vendor $10,000, she would show $15,000 on the vendor's check stub. That way, the cash account would always stay in balance. Finally, when the checks paid to her were returned in the bank statement, she would tear them up and throw them in the trash bin.

In looking at this scheme from an accounting perspective, one can see that she had her choice of three techniques to cover her tracks:

- false debits,
- omitted credits or
- forced balances;

and all the three leave traces which can be early warning signs of cash misappropriation. The three principle methods employees use to misappropriate cash can show up early in an organization's books. Accountants should be alert to simple trends when determining a company's risk of material embezzlement. Consider one or more of the following:

1. Skimming
    a. Decreasing cash to total current assets.
    b. A decreasing ratio of cash to credit card sales.

    c. Flat or declining sales with increasing cost of sales.
    d. Increasing accounts receivable compared with cash.
    e. Delayed posting of accounts-receivable payments.

2. Larceny
    a. Unexplained cash discrepancies.
    b. Altered or forged deposit slips.
    c. Customer billing and payment complaints.
    d. Rising "in transit" deposits during bank reconciliations.

3. Fraudulent Disbursements
    a. Increasing "soft" expenses (for example, consulting or advertising).
    b. Employee home address matches a vendor's address.
    c. Vendor address is a post office box or mail drop.
    d. Vendor name consists of initials or vague business purpose. (Employees often use their own initials when setting up dummy companies; for example, "JTW Enterprises").
    e. Excessive voided, missing or destroyed checks.

False debits: the mentioned fraudster chose the most logical (and common) method for covering cash embezzlement: the false debit. When she credited the bank account for the checks she made out to herself, the corresponding debit was false. Still, from the standpoint of the accounting equation, the books were in balance.

Embezzlers have two choices concerning the false debit: The transaction can be allocated to an asset account or an expense account. In Lemon's case, she added her thefts to the inventory account--an asset. As we know, that false debit will stay on the books until some action is taken to remove it. In this situation, the store's inventory was overstated by $416,000 over eight years, as the store never performed a physical count of its inventory. As a result, when this crime came to light, a huge write-off was necessary, almost bankrupting the store.

A less obvious move would have been to charge the false debit to an expense account, which is written off every year. It doesn't matter what the expense is, although these are some favorites: advertising, legal expense, consulting fees and other "soft expenses."

Here, the expense for fraud is written-off annually. If the fraud perpetrator can conceal the fraud long enough for the account to be closed to profit and loss, he or she has gone a long way toward avoiding detection—at least on a current basis.
Omitted credits: to understand how omitted credits affect the books, imagine the above-mentioned fraudster had taken a different tack. Instead of writing checks to herself, she would instead intercept incoming cash receipts before they were posted. Presume further that she would negotiate the checks by forging the endorsement of the store, then endorsing her own name on the checks, subsequently depositing them in her checking account.

The net effect would have been that she stole the debit (the cash) and omitted the credit (sales or accounts receivable); in short, she skimmed the money. This is known as an "off-book fraud," as evidenced by the omission of the transaction from the accounting records altogether. If she had skimmed from the store's sales, there would be only indirect proof of her crime through falling revenue and/or rising costs. But if she had skimmed from accounts receivable, she would need to create a fictitious entry to credit the customers' accounts; otherwise, the books would be out of balance.

Forced balances: another technique to conceal asset misappropriation is not the best choice. The same fraudster could have attempted to force the balance of the bank accounts and inventory to cover her withdrawals. In that situation, she would have forced the bank reconciliation to equal the amount she was stealing by purposely adding the transactions. But that technique requires constant attention. Unless the store business has lots of cash, forcing the bank balance will eventually result in bounced checks. A simple proof of cash that's routinely missing, an audit will usually catch this scheme.

That's not what happened to the mentioned fraudster, though. She had a nervous breakdown because of the pressure from all those years of stealing and covering it up; she came forward and confessed. Her embezzlement points out one real benefit of an audit in a small business: Almost any degree of independent review by an external accountant would have uncovered what the fraudster was doing. Embezzlements can be uncovered, but more importantly, fraudsters will be much less likely to steal knowing that an accountant will be scrutinizing their activities.

Appendix C: Major types of fraud

This appendix lists and comments on major types of fraud. By far, the most worrying and aggressive type of petty fraud nowadays is identity theft and other types of identity fraud. Amongst internal fraud, the lead comes from financial statement fraud. These will be commented first.

Identity fraud

Identity fraud is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen / assumed identity.

Fraudsters often use an existing name and identifying information to:

a. obtain credit cards
b. register phone and telecoms
c. apply for consumer bank loans
d. apply for mortgages
e. rent apartments
f. present as true identity if required to do so

…and then leaving the true individual with the debts and problems.

The term identity fraud has gained prominence throughout the last decade. In the US there were 10 million victims of identity theft in 2003 with an average individual loss of USD 5,000. Nearly 300 million hours were spent in resolving ID theft issues in 2003 (Association of Certified Fraud Examiners of the US). Typically it takes up to two years to sort out the problems, reinstate credit rating and reputation, after detection.

The fraudulent use of identities has been in existence for some time. For example, submitting a fraudulent claim for social security benefits in the name of a deceased relative or opening a bank account in a false name.

In 2007, an identity fraud report issued by the United Nations stated that a substantial amount of identity-related crime is associated with economic fraud, as a means of avoiding fraud prevention measures and avoiding criminal liability and, in most cases, as a means of deception central to the fraud offence itself.

In recognition of the fact that a purpose of identity fraud is to avoid detection, entities should ensure that when implementing fraud prevention and detection strategies, consideration is given to the risk of identity fraud. The extent of prevention and detection strategies will depend on:

1. the risk posed by identity fraud on the activities of the organization
2. the risk posed to others (whether government, business or individuals) through the organization issuing a proof-of-identity document to a fraudster which could be used to commit identity fraud

In addition to the fraud prevention and detection measures discussed in previous chapters, the following are some fraud prevention and detection measures organizations might consider to minimize the risk of identity fraud.

a. Know your customer: a strategy for assisting with the prevention of identity fraud is to identify a customer on initial engagement. The Gold Standard Enrolment Framework developed through the NIS Strategy has been developed to assist organizations with knowing their customers. Organizations should identify what and how much documentation a customer should provide to establish their identity before the provision of services and this information should be publicized.
b. Fraud awareness training: a strategy for assisting with the prevention of identity fraud is training front-line staff to detect fraudulent documentation. Some State documentation contains security features such as a passport with a computer chip embedded in the document. A working knowledge of, and familiarity with, these security features by front-line staff may assist in the early detection of a fraudulent document.

c. Document verification: a strategy for assisting with the detection of identity fraud is checking the authenticity of a State document. A common technique for fraudsters is the creation of false documentation.
d. Data matching: a strategy for assisting with the detection of identity fraud is matching entity data with other sources and State organizations' data. Data matching allows information from a number of sources to confirm the legitimacy of a person and/or data.

Integrity of data: while the strategies above may assist with preventing and detecting identity fraud, this is only as useful as the data which is maintained by an entity. If an entity's data is not accurate and up-to-date, this will create opportunities for fraud to be committed. Entities should continually review the currency and accuracy of their data.

Financial Misstatement

As mentioned in the previous appendix, this type of fraud leads to huge losses to banks, investors, employees, the State and other parties involved. The most commonly used practices leading to rigged accounts are as follows:

a) Inappropriately reported revenues

(1) Fictitious revenues
(2) Premature revenue recognition
(3) Contract revenue and expense recognition

b) Inappropriately reported expenses

(1) Period recognition of expenses

c) Inappropriately reflected balance sheet amounts, including reserves

(1) Improper asset valuation
(a) Inventory
(b) Accounts receivable
(c) Mergers and acquisitions
(d) Capitalization of intangible items

(2) Misclassification of assets
(3) Inappropriate depreciation methods
(4) Concealed liabilities and expenses
    (a) Omission
    (b) Sales returns and allowances and warranties
    (c) Capitalization of expenses
    (d) Tax liability

d) Inappropriately improved and/or masked disclosures

1. Liabilities omissions
2. Subsequent events
3. Related-party transactions
4. Accounting changes
5. Management frauds uncovered
6. Backdating transactions

e) Concealing misappropriation of assets

f) Concealing unauthorized receipts and expenditures

g) Concealing unauthorized acquisition, disposition, and use of assets

Overstatement of revenue in detail:

1. Accelerating shipments towards the end of the accounting period
2. Keeping books open beyond the end of accounting period
3. Treating consignments as sales
4. Bill-and-hold transactions (auditors should question business purpose)
5. Goods shipped ion evaluation basis
6. Sales where right of return exists
7. Round-trip trades and swaps
8. Related party transactions
9. Overstating percentage of completion in long term contracts
10. Understatement of returns, allowances, discounts, markdowns

11. Fictitious sales
12. Alteration, falsification or backdating of sales/shipping documents
13. Channel Stuffing
14. Partial shipments where the entire sale is recognized
15. Early delivery of products
16. Shipment of goods not ordered
17. Recognition of revenue where contract calls for multiple deliverables (set up, installation, testing, etc.)
18. Misallocation of value in multiple-element revenue arrangements (sale + service ion software)
19. Up-front fees (subscriptions, maintenance contracts)

Criteria for recognition of revenue fraud are:

1. Persuasive evidence of an arrangement
2. Delivery occurred or services rendered, title transferred, risk of ownership transferred
3. Price to buyer is fixed or determinable
4. Reasonable assurance that the receivable is collectible

Detection Techniques

1. Audit of transactions close to the end of the accounting period (cutoff tests)
2. Audit of large transactions
3. Audit of transactions with new customers and related parties
4. Audit of unprocessed returns
5. Audit of returns at the beginning of the subsequent accounting period
6. Receivables confirmation (sometimes called circularization)
7. Manual sales entries in the books
8. Audit of long term contracts (percentage of completion)
9. Analytical tests of sales data

Inventory Misstatements

1. Inflation of inventory on hand
2. Inflation of inventory value by postponing write-downs
3. Capitalization of inventory

Investments Misstatements

1. Fictitious investments
2. Misclassification of equity investments (trading or available for sale)
3. Misclassification of debt securities held as investments (trading, held to maturity, or available for sale); trading and available for sale investments in debt securities are stated at fair market value; unrealizedgains/losses on trading securities are shown as part of income for the period, such gains/losses on those held as available for sale are shown as other comprehensive income. Held to maturity investments in debt securities are shown at amortized value.
4. Failure to write down declines in the value of investments that are not expected to recover

Other types of financial statement manipulation:

1. Fictitious assets
2. Treatment of a part of the purchase price in mergers as in-process research & development so that they can be expensed by the acquiring company
3. Capitalization of startup costs
4. Improper capitalization of interest costs
5. Understatement of liabilities and expenses
6. Off-Balance Sheet transactions
7. Cookie-jar reserves and earnings management
8. Improper and inadequate disclosures
9. Check tampering
10. Expense reimbursement padding
11. Payroll schemes (phantom employees and falsification of time cards)

Asset Misappropriation

It was mentioned that this type of fraud, due to its variety and multiple branches, is known as the fraud tree.

The major types of asset misappropriation are now summarized.

Tangible assets misappropriation, 10 types:

(1) Cash theft

(a) Sales register manipulation
(b) Skimming: cash stolen before recorded
(c) Collection procedures
(d) Understated sales
(e) Theft of checks received
(f) Check for currency substitution
(g) Lapping accounts
(h) False entries to sales account
(i) Inventory padding
(j) Theft of cash from register
(k) Deposit lapping
(l) Deposits in transit

(2) Fraudulent disbursements

(a) False refunds
(b) False voids
(c) Small disbursements
(d) Check tampering
(e) Billing schemes
(f) Personal purchases with company funds
(g) Returning merchandise for cash

(3) Payroll fraud

(a) Ghost employees
(b) Falsified hours and salary
(c) Commission sales

(4) Expense reimbursement

(a) Mischaracterized expenses
(b) Overstated expenses
(c) Fictitious expenses
(d) Multiple reimbursements

(5) Loans

(a) Loans to nonexistent borrowers
(b) Double pledged collateral
(c) False application information
(d) Construction loans

(6) Real estate

(a) Appraisal value
(b) Fraudulent appraisal

(7) Electronic transfer

(a) System password compromise
(b) Forged authorizations
(c) Unauthorized transfer account
(d) ATM

(8) Check and credit card fraud

(a) Counterfeiting checks
(b) Check theft
(c) Stop payment orders
(d) Unauthorized or lost credit cards
(e) Counterfeit credit cards
(f) Mail theft

(9) Insurance fraud

(a) Dividend checks
(b) Settlement checks
(c) Premium
(d) Fictitious payee
(e) Fictitious death claim
(f) Underwriting misrepresentation
(g) Vehicle insurance — staged accidents
(h) Inflated damages
(i) Rental car fraud

(10) Inventory

(a) Misuse of inventory
(b) Theft of inventory
(c) Purchasing and receiving falsification
(d) False shipments
(e) Concealing inventory shrinkage b) Intangible assets

Intangible assets misappropriation, 3 types:

(1) Theft of intellectual property

(a) Espionage
(b) Loss of information

(c) Spying
(d) Infiltration
(e) Informants
(f) Trash and waste disposal
(g) Surveillance

(2) Customers

(3) Vendors

Finally, the misuse of proprietary business opportunities or the misuse of other valuable information is asset misappropriation.

Corruption

Corruption is difficult to punish yet easy to detect. Criminal evidence requires, in most countries, proof that corruption favored a given person or entity. But in most exchanges of favors and other type of high profile corruption, such proof is difficult to establish.

The most common types of corruption are:

a) Bribery and gratuities to

(1) Companies
(2) Private individuals
(3) Public officials

b) Embezzlement

(1) False accounting entries
(2) Unauthorized withdrawals
(3) Unauthorized disbursements
(4) Paying personal expenses from bank funds
(5) Unrecorded cash payments
(6) Theft of physical property
(7) Moving money from dormant accounts

c) Receipt of bribes, kickbacks, and gratuities

(1) Bid rigging

(2) Kickbacks

(a) Diverted business to vendors
(b) Over billing

(3) Illegal payments

(a) Gifts
(b) Travel
(c) Entertainment
(d) Loans
(e) Credit card payments for personal items
(f) Transfers for other than fair value
(g) Favorable treatment

(4) Conflicts of interest

(a) Purchases
(b) Sales
(c) Business diversion
(d) Resourcing
(e) Financial disclosure of interest in vendors
(f) Ownership interest in suppliers

(e) Money laundering: this crime often includes corruption and other fraud types. It is no longer classified as a fraud but as an independent type of crime.

f) Aiding and abetting fraud by other parties (customers, vendors)

Deceptive Sales practices

Based on revenues manipulation:

1. Fictitious sales revenue: sale of non-existent goods, sales to non-existent customers
2. Inflated sales: shipping of goods not ordered, treating consignments as sales, ignoring shipping terms that deal with ownership transfer
3. Over-billing customers: billing customers above agreed upon price

Other deceptive sales practices

1. Defective parts: sale of defective parts that will be returned subsequently
2. Reimbursement for services not provided or not covered under government programs
3. Underwriting fraud schemes: usually, rigging the research reports on companies to gain advantage in underwriting, e.g., bullish reports by Smith Barney on AT&T to benefit in the underwriting of AT&T spinoff of its wireless subsidiary
4. Billing, collection, or recording of vendor allowances and support: Earnings management by setting unrealistic sales targets, reporting underachievement to vendors, marking down prices, and claiming allowances from vendors to shore up revenues, e.g., Saks case
5. Deceptive sales practices, including slamming: slamming is the practice of switching the long distance telephone service from one carrier to another without the customer's consent
6. Skimming: abstracting cash by delaying the recording of transactions, or not recording it at all
7. Product diversion: diversion of products to markets/uses not intended; usually in export sales, promotional offers, excess merchandise destruction, charitable donations (www.investigation.com)
8. Inflated claims: often by pharmacy and other benefit managers

Manipulation of Stock market transactions

The most common types are as follows:

1. Round-trip trading: an action that attempts to inflate transaction volumes through the continuous and frequent purchase andsale of a particular security, commodity or asset. (http://www.investopedia.com/terms/r/round- triptrades.asp)
2. Ricochet trading, sometimes known as Megawatt laundering: arbitrage trading involving buying at a low price from one market and selling the same product in another market at a much higher price. Enron indulged in it by buying power in California below their ceiling prices to sell it at almost five times the price elsewhere (http://www.larry-adams.com/200507 article.htm)
3. Inter-positioning Specialist in a stock inter-positioning himself by trading separately with the buy order and the sell order rather than executing the orders, thereby obtaining higher profits. In July 2008, the US Court of Appeals set aside a guilty verdict under securities law, holding that absent proof that the defendant actually conveyed a misleading impression to customers, finding securities fraud liability would invite litigation beyond the immediate sphere of securities litigation.
4. Trading ahead: a specialist trades for his own account before trading for the public accounts. Recently in July 2008, the US Court of peals (Second Circuit) set aside a guilty verdict under securities law, holding "that absent proof that the defendant actually conveyed a misleading impression to customers, finding securities fraud liability would invite litigation beyond the immediate sphere of securities litigation. United States v. Finnerty, 2008 U.S. App. LEXIS 15296 (2d Cir. July 18, 2008)
5. Late trading and market timing: violations facilitating unlawful late trading and deceptive market timing of mutual funds by its customers and customers of its introducing brokers. (http://www.sec.gov/news/press/2006-38.htm)

Sources and references

The initial chapters of the manual contain extensive references to the following sources:

- "A Guide to forensic accounting investigation", T. W. Golden et al., Wiley, 2006.
- "Managing the business risk of fraud: a practical guide", American Institute of Certified Public Accountants (AICPA) and the Association of Certified Fraud Examiners (ACFE) of the U.S., no date mentioned.
- "Fraud Examination", W. Albrecht, C., Albrecht C. and M. Zimbelman, 3rd edition. Mason, OH: South-Western Cengage Learning, 2009.
- "Fraud Control in Australian Government Entities: Better Practice Guide", Australian National Audit Office and KPMG, March 2011.
- "Global economic crime survey 2007", PriceWaterhouseCoopers editors, 2007.
- "Fraud data interrogation tools: comparing best software for fraud examinations", Rich Lanza, Fraud Magazine, no date mentioned.
- Wells, J. (1997). "Occupational Fraud and Abuse", I. Wells, Austin, TX: Obsidian Publishing, 1997.

Hopefully, the manual is able to summarize, clarify and simplify most of the contents referenced above, thus making their consultation largely redundant.

Contents devoted to the use of Information Technologies (IT) in the detection of fraud, are the direct result of professional experience acquired by the author. Although contents are kept at an introductory level, it would be difficult to find complementary readings at the same level; a few, specialized references might be referenced as:

Bolton, R. and Hand, D. (2002). Statistical Fraud Detection: A Review (With Discussion). Statistical Science 17(3): 235-255.

Coderre, G. (1999). Fraud detection. Using data analysis techniques to detect fraud. Global Audit Publications.

Kirkos, E., Charalambos, S.and Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements, Expert Systems with Applications 32 995–1003.

Nigrini, M. (2011). Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations. Hoboken, NJ: John Wiley and Sons Inc. ISBN 978-0-470-89046-2.

Palshikar, G. (2002). The Hidden Truth – Frauds and Their Control: A Critical Application for Business Intelligence, Intelligent Enterprise, vol. 5, no. 9, 28 May 2002, pp. 46-51.

Phua, C., Lee, V., Smith-Miles, K. and Gayler, R. (2005). A Comprehensive Survey of Data Mining-based Fraud Detection Research. Clayton School of Information Technology, Monash University.

ISBN 978-99965-689-0-9

澳門基金會
FUNDAÇÃO MACAU