ACCID

Associació Catalana de Comptabilitat i Direcció

TECHNICAL NOTE

January 2017

ANTI-FRAUD STRATEGY[1]

[1] Document written by Nicola Eusebio, Università degli studi di Milano – Bicocca.

Summary

The subject of the following article regards the main pillars of the **anti-fraud strategy:** prevention, detection, deterrence and response to the fraud.

We have started from its first necessary step: **fraud risk assessment**.

Then, several **Fraud Prevention** methods will be described, such as Fraud Awareness program, Authority Limits, Pre-employment screening, with particular attention on the most important antifraud tool: developing a working environment oriented to honesty and fairness.

In the **Fraud Detection** part, we will analyze the importance of the Whistleblower Hotline**,** Process Controls and Technology tools.

One aspect of new technology will be then developed, describing a new global threat: cyber fraud. There will be indicated the frequent forms of internet crimes, indicated by FBI. Particular attention will be given to the fasted growing form of cyber fraud called **Business E-Mail Compromise (BEC).** The solutions concerning the prevention of such internet attacks, will be reported.

The final consideration is dedicated to the importance of the Low in fraud prevention and its detection.

Keywords: fraud prevention, detection, cyber fraud, risk assessment

1. "PREVENTION IS BETTER THAN CURE"

The recent cases of corporate fraud have focused the attention on the mechanisms which could be more suitable to prevent the occurrence of the fraudulent actions.

It has been widely proven that those companies that undertake proactive paths in the implementation of anti-fraud strategy, recorded the lowest number of cases of fraud.

It is more profitable to prevent losses because once a fraud has already occurred, the likelihood of recovering stolen funds from the perpetrator is often relatively low. Therefore, it is preferable to try to prevent the loss from occurring as the old adage "prevention is better than cure" certainly applies to fraud.

Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring.

However, many organizations do not have a formal approach to fraud prevention.

2. "FINANCIAL SHERLOCK HOLMES"

The companies are already subjected to various form of supervision and control of internal or external matrix: internal audit, inspection services, governance functions, compliance, external auditors etc.

The work of these committees, inspectorates, councils, departments and commissions follows specific protocols which sometimes are very different but sometimes overlapping.

But does exist, in an organization, a specific structure dedicated to handle, test and improve the anti-fraud business programs?

The professionals involved in fraud risk management have different titles: Fraud manager, Director of security, Responsible for fight against fraud, Threat Management Manager, but their method of working will be the same: observation, deduction and surveys.

The specific position for this target, called "**Fraud manager**" is a craft prevalent in the Anglo-Saxon world, but it is slowly gaining ground in other countries.

What are the main tasks of a fraud risk manager?

He is primarily responsible to detect risk factors, simulate the possible scenarios which favor fraudsters and monitor the performance of the chosen protection models.

The fraud manager establishes an effective anti-fraud program, which should be well integrated with every other element of the internal control system.

Such anti-fraud program must be suitable to preside over time the risk of the occurrence of internal or external fraudulent activity.

Besides the position responsible for the fight against fraud, some large groups go further in their approach and establish a **multidisciplinary team created "ad hoc"**, imagined and structured as autonomous unit entirely responsible for the management of anti-fraud programs.

The team includes the individuals with complementary specializations in management control, information systems, risk management but also in law or statistics.

Even if the fraud manager is charged specifically for anti-fraud actions it is necessary to point out that entire management is called to be responsible for the continued updating of the management processes of fraud and most notably risk, such as the Board of Directors, the Executive Committee and Operating, the Supervision and Control Committee, the Internal Audit and Fraud Risk Management, Security, and so on.

In fact, to combat fraud effectively the organization needs to adopt a complex "anti-fraud strategy" which can be carried out effectively only if all levels of management and employees are involved in it.

The anti-fraud strategy consists principally, in four main components:

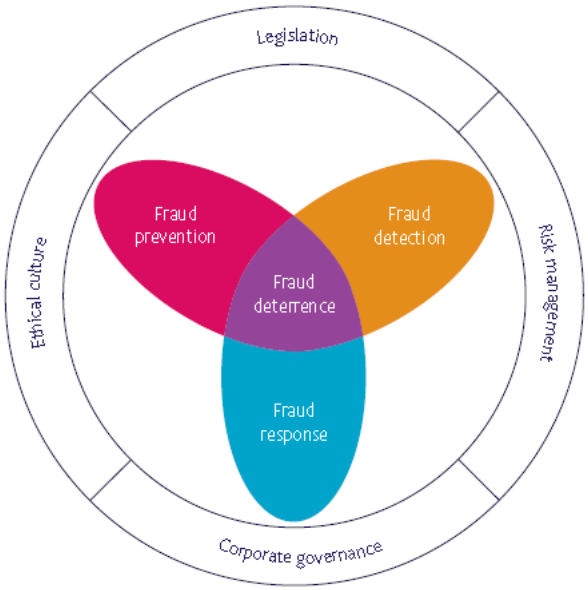
1. Fraud prevention
2. Fraud detection
3. Deterrence
4. Response

These components are closely interlinked and furthermore they are conditioned by:

1. Ethical culture in the organization
2. Current legislation
3. Risk management
4. Corporate governance

The following diagram summarizes the main aspects of "anti-fraud strategy ":

Fig.1 Anti- fraud strategy



Source: "Fraud risk management", CIMA 2009

We will start our anti-fraud strategy analysis from the fraud risk assessment, the first necessary step, to be aware about the level of the weaknesses in the organization.

Such activity takes part of the risk management activity.

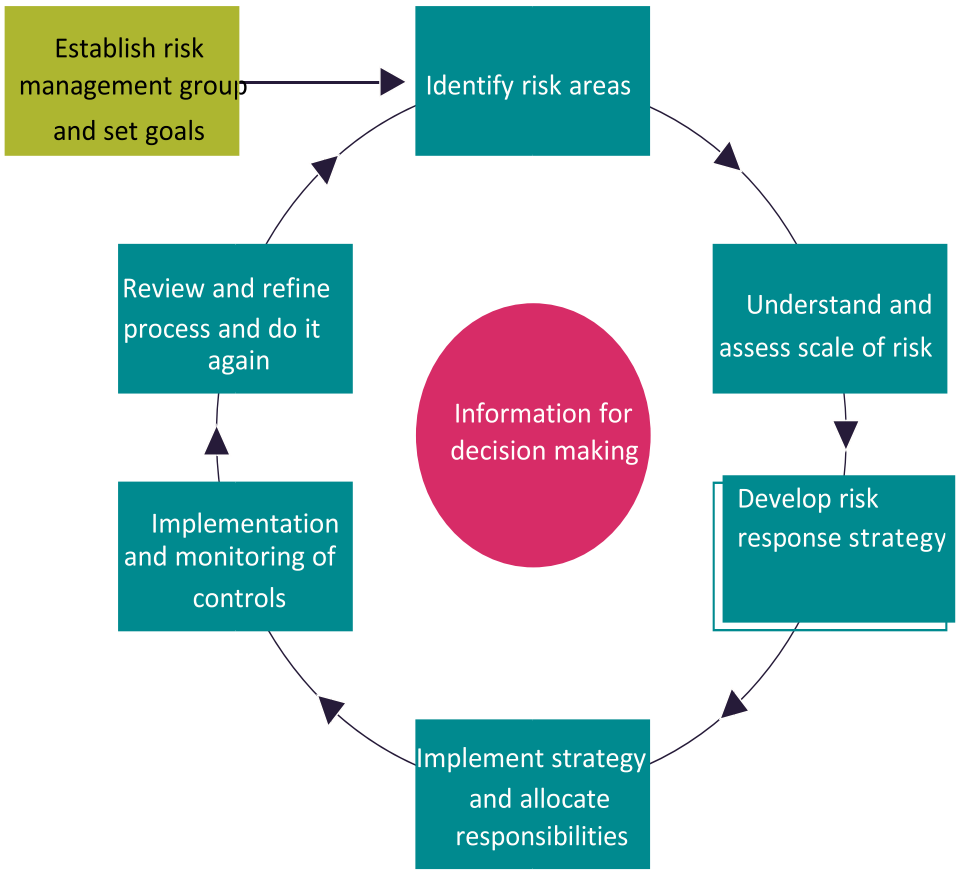
3. RISK MANAGEMENT

Our aim is to focus on managing the risk of fraud, but first, see at more general aspects of risk management.

Risk management is defined as the "process of understanding and managing risks that the entity is inevitably subject to in attempting to achieve its corporate objectives" (CIMA Official Terminology, 2005).

It means to understand the nature of such events and, if they represent threats, making plans to mitigate the risks. It is interactive process which could be called risk management cycle as following:

Fig. 2 Risk management cycle



Source: "Fraud risk management" CIMA 2009

Organizations face risks or threats from both internal and external sources. Such risks include: regulatory, environmental, technological, processing risk and fraud, which represents a major risk for business since it threatens the business, not only in terms of financial health but also its image and reputation.

Fraud risk has a different nature comparing other risks:

In fact, frauds are not resulting of accidental occurrences but represent a deliberate act.

For this reason, fraud risk should be assessed independently of the general risk assessment process.

3.1 Fraud Risk Assessment

Therefore, an efficient anti-fraud strategy should identify the weaknesses in the existing system of controls and figure out if they can arise potential damage to the company.

This activity is called "**Fraud Risk Assessment**".

The fraud risk assessment needs to *anticipate the behavior of a potential fraud perpetrator*, asking:

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

Consequently, **fraud risk assessment** includes the following three elements:

a) risk identification,
b) risk likelihood and significance assessment,
c) risk response.

3.1.1 Fraud risk identification

- It includes gathering (1):
  - ✓ **external information** from regulatory bodies (e.g., securities commissions), industry sources (e.g., law societies), key guidance setting groups (e.g., Committee of Sponsoring Organizations of the Treadway Commission (COSO)), and professional organizations (e.g., The Institute of Internal Auditors (IIA), and comparison with other organizations etc.
  - ✓ **internal information** for identifying fraud risks: interviews, questionnaires, and brainstorming with personnel of the organization and review of whistleblower complaints,
- Analytical procedures which includes:

- ✓ **an assessment of the incentives, pressures, and opportunities to commit fraud**. For example, an *employee incentive programs* and the metrics on which they are based, can provide a map to where fraud is most likely to occur.

- ✓ potential **override of controls** by management as well as **areas where controls are weak** or there is a **lack of segregation of duties**.

- ✓ Analyzing an internal and external threats to **data integrity, system security**, and theft of financial and sensitive business information.

3.1.2 Fraud risk likelihood and significance assessment

Assessing the relative likelihood and potential significance of identified fraud risks should be based on historical information, knowledge of the fraud schemes, and interviews with staff.

The likelihood of a risk occurring should be assessed on a **gross**, a **net** and a **target** basis (3)

a) The gross basis assesses the inherent likelihood of the event occurring *in the absence of any processes* which the organization may have in place to reduce that likelihood.

b) The net basis assesses the *likelihood, taking into account processes to mitigate the chance* of the event occurring.

c) The target basis of a risk occurring reflects the *risk tolerances* which can be different in individual organization.

The likelihood of risk we can assess in terms of:

- high – probable
- moderate – possible
- low – remote.

This step, should consider not only monetary significance, but also significance to an organization's financial reporting, operations, and reputation, as well as legal and regulatory compliance requirements.

3.1.3 Risk response

Once the risks have been identified and assessed it is necessary to decide what the response should be given to them and perform a cost-benefit analysis of fraud risks over which the organization wants to implement controls or specific fraud detection procedures.

The strategy of the organization for a single risk fall into one of the following categories:

a) risk retention (e.g. choosing to accept small risks)
b) risk avoidance (e.g. stopping sale of certain products to avoid the risk to occurring)
c) risk reduction (e.g. through implementing controls and procedures)
d) risk transfer (e.g. contractual transfer of risk; transferring risks to insurers)

3.2 ACFE Fraud Risk assessment model

ACFE proposes an exhaustive fraud risk assessment model, which should include the following modules (2)

1 - Employee Assessment

2 - Management/Key Employee Assessment

3 - Physical Controls

4 - Skimming Schemes

5 - Cash Larceny Scheme

6 - Check Tampering Schemes

7 - Cash Register Schemes

8 - Purchasing and Billing Schemes

9 - Payroll Schemes

10 - Expense Schemes

11 - Theft of Inventory and Equipment

12 - Theft of Proprietary Information

13 - Corruption

14 - Conflicts of Interest

15 - Fraudulent Financial Reports

The full **Fraud Risk Assessment Model** (11) is attached here. It could be very useful in the practical application of our consideration of this subject. See Attach.1 (source: https://nevadasmallbusiness.com)

Here below is showed an example of the framework used in fraud risk assessment which focuses solely on potential revenue recognition risks within financial reporting.

It includes: a list of identified fraud risks, relative likelihood and significance of occurrence. Then, the risks are mapped to the people/departments that may be impacted and to relevant controls, which are evaluated for design effectiveness and tested to validate operating effectiveness. Next, residual risks are identified, and a fraud risk response is developed.

A full fraud risk assessment, in other areas of organization should be assessed in the same manner.

Fig.3. Fraud risk assessment within financial reporting - Example

Identified Fraud risks and Schemes (1)	**Likelihood (2)**	**Significance (3)**	**People and/or Department (4)**	**Existing anti-fraud Controls (5)**	**Controls effectiveness assessment (6)**	**Residual risks (7)**	**Fraud risk response (8)**
Financial Reporting Revenue recognition • Backdating agreements	Reasonably possible	Material	Sales personnel	Controlled contract administration system	Tested by IA	N/A	Periodic testing by IA
•Channel stuffing	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
•"Holding books open"	Reasonably possible	Material	Accounting	Standard monthly close process Reconciliation of invoice register to general ledger Established procedures for shipping, invoicing, and revenue recognition Established process for consolidation	Tested by IA Tested by management Tested by IA Tested by IA	Risk of management override	Testing of late journal entries Cut off testing by IA

•Late shipments	Reasonably possible	Significant	Shipping dept.	Integrated shipping system, linked to invoicing and sales register Daily reconciliation of shipping log to invoice register Required management approval of manual invoices	Tested by IA Tested by management Tested by IA	Risk of management override	Cut off testing by IA
• Side letters/ agreements	Probable	Material	Sales personnel	Annual training of sales and finance personnel on revenue recognition practices Quarterly signed attestation of sales personnel concerning extra contractual agreements Internal audit confirming with customers that there are no other agreements, written or oral, that would modify the terms of the written agreement	Tested by management Tested by management	Risk of override	Disaggregated analysis of sales, sales returns, and adjustments by salesperson

• Inappropriate journal entries	Reasonably possible	Material	Accounting & Finance	Established process for consolidation Established, systematic access controls to the general ledger Standard monthly and quarterly journal entry log maintained. Review process in place for standard entries, and nonstandard entries subject to two levels of review	Tested by IA Tested by IA Tested by management	Risk of override N/A N/A	Data mining of journal entry population by IA for: • Unusual Dr/CR combinations • Late entries to accounts subject to estimation
Identified Fraud risks and Schemes (1)	**Likelihood (2)**	**Significance (3)**	**People and/or Department (4)**	**Existing anti-fraud Controls (5)**	**Controls effectiveness assessment (6)**	**Residual risks (7)**	**Fraud risk response (8)**
•Roundtrip transactions	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Manipulation of bill and hold arrangements	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Early delivery of product	Reasonably possible	Significant	Sales and shipping	Systematic matching of sales order to shipping documentation; exception reports generated.	Tested by management	Adequately mitigated by controls	N/A

• Partial shipments	Reasonably possible	Significant	Sales and shipping	Systematic shipping documents manually checked against every shipment. Systematic matching of sales order to shipping documentation; exception reports generated. Customer approval of partial shipment required prior to revenue recognition.	Tested by management	Adequately mitigated by controls	N/A
• Additional revenue risks				Systematic shipping documents manually checked against every shipment.			

Source: Managing the business risk of fraud (Appendix D) , AIPCA, ACFE

FRAUD PREVENTION AND DETECTION

Once the potential fraud risk assessed, their probability should be reduced by developing and implementing an anti-fraud strategy across the organization.

Fraud prevention and detection are related, but are not the same concepts. Prevention encompasses policies, procedures, training, and communication that stop fraud from occurring, whereas, detection focuses on activities and techniques that promptly recognize timely whether fraud has occurred or is occurring.

4. FRAUD PREVENTION

In opinion of the criminologists, there are three general categories of crime prevention (punitive, defense, and interventionist methods (12).

Also in fraud crime, we can apply three categories of prevention:

Punitive fraud prevention methods use increasing punishment to make individuals too fearful to commit it. The Sarbanes-Oxley Act of 2002 in which, for example, an individual can go to prison for lying to the auditor, use the punitive fraud prevention method (9)

Defense methods concentrate on limiting the opportunity for committing a crime, such as improving internal controls within an organization or adopt an adequate risk assessment procedure.

But sometimes the fraud can occur because individuals are unaware that their actions are fraudulent or because individuals' intuitions tells them it is acceptable to commit fraud.

In these cases, none of above methods will be effective but an **interventionist method of fraud prevention** should be more useful through an ethical culture creation or fraud awareness program.

Therefore, it is the duty of all, who influence the behavior and mentality of the people e.g. schools, universities, media, to consolidate the importance to act with integrity, to respect the laws, to disseminate the concept that "**doing the right thing' is foundational to everything we do".**

Considering our earlier analysis about why people commit fraud, one of the most effective ways to deal with the problem of fraud is to adopt methods that **will decrease motive**, **restrict opportunity** and **limit the ability** for potential fraudsters **to rationalize their actions**.

But the most important pillar in fraud prevention strategy is however, to develop and maintain a working environment oriented to honesty and fairness.

4.1 Developing an ethical culture as fraud prevention tool

The most effective way in preventing frauds, is to promote and maintain a corporate culture based on ethics and honesty. Anyone should be aware that the organization is carrying out its business only in honest and ethical way. That means in practice that dishonest people are aware that honest employees will not tolerate their potential deceit and will do everything to prevent frauds.

The corporate culture, that is "the climate that reigns" in working environments, can be oriented to honesty and fairness, or be unhealthy and therefore prepared to tolerate injustices of various kinds of violations.

A corporate culture based on ethics and on "doing the right thing" is in fact the best antidote to inhibit or stop the dishonest or unfair conduct.

The anti-fraud culture is strongly influenced by the ethics of chairman and CEO. They are called first to set a good example for the rest of organization. 'Tone at the top' is key. Employees are more likely to do what they see their superiors doing than follow an ethics policy, and it is essential that management do not apply double standards.

Among the means available to achieve the purpose of the ethical culture, can be indicated the Code of Conduct or the Code of Ethics, to be spread at all corporate levels.

A positive work environment, in which the worker does not feel abused, exploited or simply ignored, is a good guarantee of success in the struggle to internal corporate fraud. In this favorable environment for employees, usually those more productive, become real "anti-fraud" watchmen observing firsthand the rules and demanding that these are also respected by colleagues less disciplined. (7)

In an environment where cutthroat competition is the norm someone may believe that ethics and productivity are irreconcilable propositions. But it is not true. Integrity, ethical choices in the strategy of the company can increase workability and company performance. One of the examples could be given by biggest beauty company in the world: L'Oréal.

4.1.1 Case study - L'Oréal

The company has a presence in 130 countries and more than 70,000 employees.

L'Oréal has been nominated by the Ethisphere Institute, one of the « World's Most Ethical Companies » for the sixth times.

The company adopts an exceptional ethics program which is managed through a dedicated organization and is deployed through "a complete monitoring system with tools in place to integrate ethics into daily reality" (6)

The company strongly believes that the excellence can be reach applying four core principles: **respect, integrity**, **courage** and **transparency.**

The strong ethical approach in the company, is demonstrated not only by adopting of the Code of Business Ethics which now is available in 45 languages and serving people with vision impairment and blindness. Some other examples of the L'Oréal's strong ethic commitment could be these examples:

- In 2007, it was appointed **Chief Ethics Officer** who is in charge of strengthening and implementing an ambitious ethic policy. The role of the Chief Ethics Officer is to support directors and managers in their decision making and to promote the principles and best practices set out in the Code of Business Ethics and its supplements. The Chief Ethics Officer can rely on a worldwide network of 66 Ethics Correspondents whose role is to support Country Managers in deploying L'Oréal's Ethics Program.

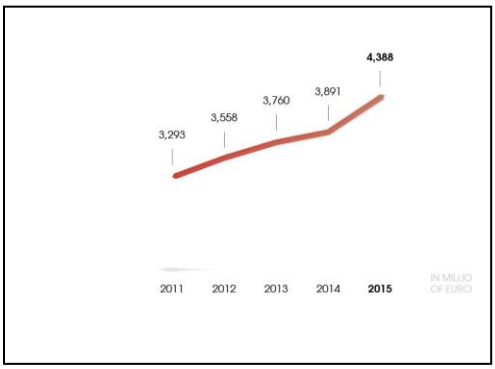
- Every year, the company organizes **Ethics Day**. Employees from around the world can chat with the Group's Chief Executive Officer via a worldwide live webchat.

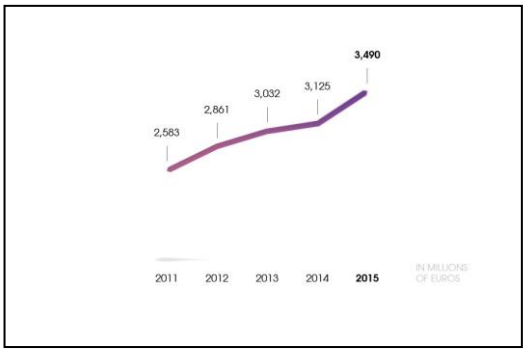
- **Two ethical competences** have been introduced in the **manager appraisal system**

- The company is Promoting a culture of dialog and transparency: the **"Open Talk" policy** encourages employees to express their opinions and report unacceptable demands and behavior. It is possible to handle this subject directly at a local level, or to contact the Chief Ethics Officer, namely via a secure internet site.

On its WEB site, the company affirms: *"*We aim to make L'ORÉAL a great place in which to work. We know that our employees are our greatest assets. They are entitled to a safe and healthy working environment: one in which personal talent and merit are recognized, diversity is valued, privacy is respected, and the balance between professional and personal life is taken into account. We believe in offering our employees a stimulating environment, exciting personal opportunities and a chance to make a difference. We encourage an atmosphere of openness, courage, generosity and respect, so that all our employees feel free to come forward with their questions, ideas and concerns" (6)

Research by the Institute of Business Ethics (IBE) has demonstrated that, through helping to establish an ethical culture, there is a correlation between ethics training and improved financial performance (13). How profitable can be a "*great place in which to work"* is showed below by Operating Profit and Net Profit of the L'Oréal Group, over the last 5 years:





Operating profit in L'Oréal: 2011-215 (billions €)

Net profit in L'Oréal: 2011-215 (billions €)

Considering the financial results of our example and considering that ethics it is best way to prevent the frauds and the losses which they involve.

4.2 Strong Internal Control System

ACFE considers a strong system of internal controls as a the most valuable fraud prevention device by a wide margin.

A strong system of internal control is another valuable fraud prevention device since a preventative control can reduce opportunity and remove temptation from potential offenders.

According the Committee of Sponsoring Organizations of the Treadway Commission (COSO): "Internal Control is a process effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance"

The result of such functionality will be increased chances that processes and procedures are operating as intended and risk is being kept at tolerable levels.

Key benefits of the internal control system include (5):

- Treatment of risk
- Achieving higher standards
- Compliance with laws and regulations
- Improved communication and procedures

Particularly in the fraud prevention the Internal Control can reach the following objectives:

- Protect against financial loss following disaster
- Prevent fraudulent activity by employees
- Maintain high password security
- Ensure disaster recovery capability

The number and type of internal controls that an organization can introduce will depend on the nature and size of the organizations but always the overall responsibility for the organization's system of internal control must be at the highest level in the organization.

The majority of U.S. publicly traded companies, (but not only they) have adopted the "Internal Control—Integrated Framework" published by the COSO which last updated version, was published in 2013.

Internal controls typically deal with factors such as approval and authorization processes, access restrictions and transaction controls, account reconciliations. These procedures often include the division of responsibilities and checks and balances to reduce risk.

The following box gives an example of division of responsibilities within Financial Reporting:

Table1. The division of responsibilities within Financial Reporting (8)

Segregation of Duties

This refers to separating out operational or administrative functions that, if combined, could be used to steal from the company. The most important segregation of duties is having different employees responsible for the recording and the custody of assets. For example, if one employee had full access to inventory in the warehouse and was also responsible for recording the accounting transactions related to that inventory, the employee would have the opportunity to steal goods and to cover up the theft with fake transactions. Separating those functions removes the ability to easily appropriate company assets.

Dual-Signature Company Checks

Another important control that protects company assets is to require two authorized signatures on all company checks. This ensures that two people must agree that the check is legitimate and that the payment is appropriate. This curbs direct theft (where an employee with signing authority simply writes checks to himself) and indirect theft (where one employee creates a fake supplier that bills the corporation). Two sets of eyes are more likely to discover such fraud.

Bank Reconciliations

A bank reconciliation is a control that ensures that all physical cash transactions have been correctly recorded during a specified period. The reconciliation is performed by someone other than the transaction clerks who are in charge of billing, accounts payable and receipts. The reconciliation clerk reviews cancelled checks that are returned with the statements of the examined time period to ensure that they are made out to the same names as those in the accounting system. This procedure not only catches many inadvertent transactional errors but also theft and fraud.

Purchase Order Authorization

Companies with good internal control systems require that a manager or other authorized person signs all purchase orders prepared by the company. This ensures that employees are not over-ordering, which can be expensive to the company. It also ensures that employees are not ordering goods for themselves and then destroying the purchase orders.

Source: http://www.objectivecontrols.com/

4.3 Human resources procedures

Among the many elements in fraud prevention we can include the Human Resources procedures as such: anti-fraud training, authority limits, transaction level procedures.

4.3.1 Anti-fraud training and Fraud Awareness program as a tools of fraud prevention

As a fraud prevention tools, should be considered **fraud awareness** developed through periodic **anti-fraud trainings.**

The Human Resources of the organization should developing and providing the necessary training on the purpose of the fraud risk management program, including the codes of conduct and ethics, what constitutes fraud, and what to do when fraud is suspected. The effectiveness of this training is dependent on mandatory attendance with periodic updates and refresher sessions

A fraud awareness programs, must indicate: who should attend it, its frequency and length and consider the cultural sensitivities. Such training should be attended by all personnel, also by the board or board committee members.

The documentation used in the training of fraud awareness should provide examples of the types of fraud that could occur and identify potential perpetrators of fraud.

The ongoing communication in an organization, should inform the personnel about the existence of the real, enforced, antifraud actions.

The information on the potential disciplinary, criminal, and civil actions that the organization could take against the individual, is necessary in order to decrease the motivation for fraudulent actions.

In fact, prevention and deterrence are interrelated concepts. **If effective preventive controls are in place, they serve as strong deterrents** to those who might otherwise be tempted to commit fraud.

4.3.2 Authority Limits

Another defense in fraud prevention is right alignment between authority and responsibility.

When an individual's level of authority is not commensurate with his or her level of responsibility the fraud is more likely.

The segregation of duty must be appropriate. Furthermore, the individuals working within a specific function should have a limited IT access as a process-level control.

4.3.3 Pre-employment screening

Research has also shown that employers who conduct pre-employment screening have fewer cases of fraud.

Pre-employment screening is a process of verifying the qualifications, suitability and experience of a potential candidate for employment. Techniques used include confirmation of educational and professional qualifications, verification of employment background, criminal history searches, and credit checks. For all screening, the organization must obtain the individual's written permission and all documents must bear the individual's name.

Pre-employment screening will reduce the likelihood of people with a history of dishonest or fraudulent behavior so it would be considered as an important **fraud prevention** procedure.

4.3.4 Transaction-level Procedures

According the anti-fraud experts, reviews of third-party and related-party transactions can help prevent fraud. "Because fraud schemes often involve the use of third-party entities/individuals, organizations need thorough measures at the front-end that will prevent the back-end activities. False vendors or employees are two of the more obvious and noted schemes in this arena.

Preventive measures are especially needed for related-party transactions that can be controlled by board members or by employees of authority with an interest in an outside entity with which the organization may conduct business.

Such individuals may mandate transactions that ultimately benefit them at the expense of the organization**.** (1)

5. FRAUD DETECTION

In the essential components of the "Fraud risk strategy" we have to include the **fraud detection techniques** to use in the case preventive measures fail.

In fact, a well visible, effective detective controls represent very strong deterrents to fraudulent behavior.

The example of the detection techniques are: an anonymous reporting mechanism (whistleblower hotline), process controls, and proactive fraud detection procedures specifically designed to identify fraudulent activity.

5.1 Whistleblower hotline

A whistleblower is a person working within an organization who reports misconduct. In most cases, the misconduct reported by the whistleblower violates a law and threatens the public in one way or another, though any form of misconduct may be reported.

There have been many famous whistleblower cases in the United States. One of the most notable involved Enron, a corporation that caused millions of people to lose money in their financing fraud.

Typically, the hotline takes the form of a dedicated telephone number that can be called to report every type of suspected fraud. The aim of the whistleblower hotline is to provide a means for citizens to alert authorities to suspected economic fraud without placing themselves in any type of danger.

Some corporations have chosen to establish this type of hotline for internal use, making it possible for people within the organization to report suspicious behavior without being in fear of losing their jobs. When a tip is received from a whistleblower, the information is investigated, making it possible to determine if there is in fact any type of fraudulent activity taking place.

Besides a traditional telephone communications, there is also the option of use of email transmissions. Individuals who believe there is reason to suspect that some sort of fraud is taking place can set up an anonymous email account, then use the account to send an email to the address provided by the hotline that outlines the suspected activity. An alternative is a web site that allows messages to be typed in and forwarded to the email address without requiring the sender to provide any type of identification.

Provision for anonymity to any individual who willingly comes forward to report a suspicion of fraud is a key to encouraging such reporting and should be a component of the organization's policy.
The most effective whistleblower hotlines preserve the confidentiality of callers and provide assurance to employees that they will not be retaliated against for reporting their suspicions of wrongdoing including wrongdoing by their superiors. Another key is demonstrating that their reporting will result in appropriate and timely action being taken.
The whistleblower process should be independently evaluated periodically for effectiveness, including compliance with established protocols

5.2 Process controls

Process controls specifically designed to detect fraudulent activity include: physical inspections/counts, reconciliations, independent reviews, analyses, and audits.

Each industry is susceptible to different types of fraud schemes.

Particularly difficulty will meet the organizations with multiple and different business units which will need to first perform a broad organization wide assessment and then perform more detailed and focused assessments of individual business units to identify the necessary process controls to detect fraud.

5.3 Technology tools.

Fraud detection is also possible by using technology able to identify anomalies as such: data analysis, data mining, and digital analysis tools.

These tools may allow users to look for journal entries posted to revenue or expense accounts that improve net income to meet analysts' expectations or incentive compensation targets. Moreover, data analysis allows users to identify relationships among people and organizations,

The use of data analytics on a continuous or real-time basis, thereby allowing management or auditing to identify and report fraudulent activity more rapidly. For example, a **Benford's Law analysis** can examine expense reports, general ledger accounts, and payroll accounts for unusual transactions, amounts, or patterns of activity that may require further analysis.

Similarly, continuous monitoring of transactions subject to certain "red flags" may promote quicker investigation of higher-risk transactions. **SAP fraud management** system can be also useful in the fraud detection.

Evidence of fraud can sometimes be found in e-mail as well. The ability of an organization to capture, maintain, and review the communications of any of its employees has led to the detection of numerous frauds in the past.

This is possible using strict and regular **backup programs** that capture all data.

6. RESPONDING TO FRAUD

An organization should clearly describe in its fraud policy so called "**fraud response plan**". It is a formal procedure apply for dealing with detected or suspected cases of fraud.

There will be benefits arising from **the publication of a corporate fraud response plan** due to its deterrence value**.**

Responding to detected or suspected instances of fraud include:

• clear reporting mechanisms

• a thorough investigation

• disciplining of the individuals responsible (internal, civil and/or criminal)

• recovery of stolen funds or property

• modification of the anti-fraud strategy to prevent similar behavior in the future.

6.1 Fraud Investigation and Response Protocols

Once an allegation is received, from employees, customers, vendors; internal audits; external audits; or by accident, the organization should follow the **process approved by the board to evaluate the allegation**. The process should include designating an individual or individuals with the necessary authority and skills to conduct an initial evaluation of the allegation and determine the appropriate course of action to resolve it.

The allegation should be examined to determine whether it involves a potential violation of law, rules, or company policy. Depending on the nature and severity of the allegation, other departments may need to be consulted, such as HR, legal counsel, senior management, IT, internal auditing, security, or loss prevention.

The next step is investigation which consist in following tasks (1):

1) **Interviews** with:

a) Neutral third-party witnesses.

b) Corroborative witnesses.

c) Possible co-conspirators.

d) The accused.

2) **Evidence collection**, considering:

a) **Internal documents**, such as:

i) Personnel files.
ii) Internal phone records.
iii) Computer files and other electronic devices.
iv) E-mail.
v) Financial records.
vi) Security camera videos.
vii) Physical and IT system access records.

b) **External records**, such as

i) Public records.
ii) Customer/vendor information.

iii) Media reports.
iv) Information held by third parties.
v) Private detective reports.

3) **Computer forensic examinations**.

4) **Evidence analysis**, including:

a) Review and categorization of information collected.
b) Computer-assisted data analysis.
c) Development and testing of hypotheses

The investigation team should report its findings to the structure which oversees the investigation: senior management, directors, or legal counsel.

After the investigation, has been completed, the organization will need to determine what action to take in response to the findings.

Any findings of material impact needs to be reported to the board, the audit committee, and the external auditor.

Possible **actions** include one or more of the following:

• **Criminal referral** (referring the case to law enforcement)

• **Civil action**

• **Disciplinary action** (termination, suspension, demotion, or warnings)

• **Insurance claim** (for some or all losses)

7. NEW, EMERGING GLOBAL THREAT: CYBER FRAUD

In the mid-1990s the Internet revolutionized the way we do business: with just a click of a mouse created almost endless opportunities for businesses.

With this new frontier also came new opportunities for fraud which takes name of "cyber fraud", internet fraud, or "cyber crime" which actually flourishes in all continents.

Internet crime schemes steal millions of dollars each year from victims and continue to plague the Internet through various methods.

An **Internet fraud** is "the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them". (14)

Frequent instances of Internet fraud include business fraud, credit card fraud, internet auction fraud, investment schemes and non-delivery of merchandise.

7.1 Types of cyber crimes

The FBI indicates the following examples of internet crimes (15):

Business E-Mail Compromise (BEC): A sophisticated scam targeting businesses working with foreign suppliers and companies that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

- **Data Breach:** A leak or spill of data which is released from a secure location to an untrusted environment. Data breaches can occur at the personal and corporate levels and involve sensitive, protected, or confidential information that is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

- **Denial of Service:** An interruption of an authorized user's access to any system or network, typically one caused with malicious intent.

- **E-Mail Account Compromise (EAC):** Similar to BEC, this scam targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms. Perpetrators of EAC use compromised e-mails to request payments to fraudulent locations.

- **Malware/Scareware:** Malicious software that is intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds from victims.

- **Phishing/Spoofing:** Both terms deal with forged or faked electronic documents. Spoofing generally refers to the dissemination of e-mail which is forged to appear as though it was sent by someone other than the actual source. Phishing, also referred to as vishing, smishing, or pharming, is often used in conjunction with a spoofed e-mail. It is the act of sending an e-mail falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The website, however, is not genuine and was set up only as an attempt to steal the user's information.

- **Ransomware:** A form of malware targeting both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through spear phishing emails to end users, resulting in the rapid encryption of sensitive files on a corporate network. When

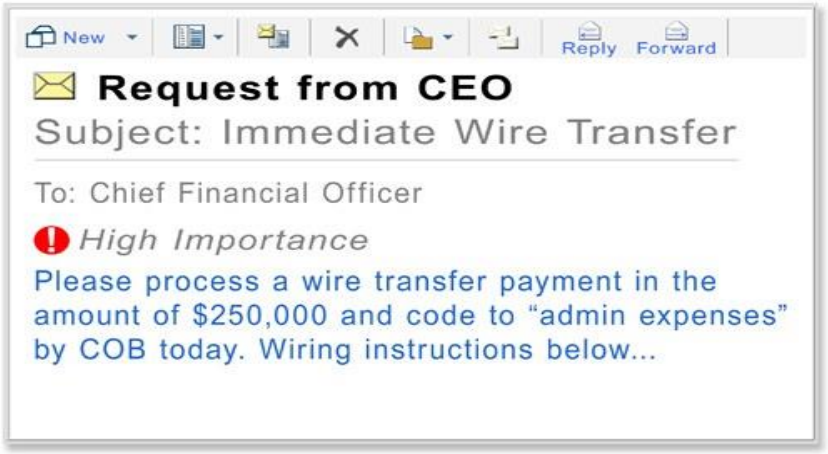
the victim organization determines they are no longer able to access their data, the cyber perpetrator demands the payment of a ransom, typically in virtual currency such as Bitcoin, at which time the actor will purportedly provide an avenue to the victim to regain access to their data.

7.2 CEO Email Wire Fraud Attacks

One of the fastest growing forms of cyber fraud, rising in frequency and increasing in financial losses is so called: **CEO Email Wire Fraud Attacks** (also known as **CEO email schemes** or Business **Email Compromise** (**BEC**s, for short).
It is very simple attack. There's no malware to write and no malicious code or links to implant but it's a text only email and with its social engineering, this cyber fraud works very well.

BEC is a serious threat on a global scale," said FBI Special Agent Maxwell Marker, who oversees the Bureau's Transnational Organized Crime–Eastern Hemisphere Section in the Criminal Investigative Division. "It's a prime example of organized crime groups engaging in large-scale, computer-enabled fraud, and the losses are staggering."

7.2.1 How "Business e-mail compromise" works?



This example reported by FBI, can easily to show the method used (16):

The accountant for a U.S. company recently received an e-mail from her chief executive, who was on vacation out of the country, requesting a transfer of funds on a time-sensitive acquisition that required completion by the end of the day.

The CEO said a lawyer would contact the accountant to provide further details.

"It was not unusual for me to receive e-mails requesting a transfer of funds," the accountant later wrote, and when she was contacted by the lawyer via e-mail, she noted the appropriate letter of authorization—including her CEO's signature over the company's seal—and followed the instructions to wire more than $737,000 to a bank in China.

The next day, when the CEO happened to call regarding another matter, the accountant mentioned that she had completed the wire transfer the day before. The CEO said he had never sent the e-mail and knew nothing about the alleged acquisition.

Since the FBI's began tracking BEC scams (in late 2013), it has compiled statistics on more than 7,000 U.S. companies that have been victimized—with total dollar losses exceeding $740 million. That doesn't include victims outside the U.S. and unreported losses.

The scammers, believed to be members of organized crime groups from Africa, Eastern Europe, and the Middle East, primarily target businesses that work with foreign suppliers or regularly perform wire transfer payments. The scam succeeds by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques. Businesses of all sizes are targeted, and the fraud is proliferating.

According to Internet Crime Complaint Center (IC3) since the beginning of 2015 there has been a 270 percent increase in identified BEC victims. Victim companies have come from all 50 U.S. states and nearly 80 countries abroad. The majority of the fraudulent transfers end up in Chinese banks.

The scammers' methods are extremely sophisticated. They use language specific to the company they are targeting, along with dollar amounts that lend legitimacy to the fraud.

To make matters worse, the criminals often employ malware to infiltrate company networks, gaining access to legitimate e-mail threads about billing and invoices they can use to ensure the suspicions of an accountant or financial officer aren't raised when a fraudulent wire transfer is requested.

Instead of making a payment to a trusted supplier, the scammers direct payment to their own accounts. Sometimes they succeed at this by switching a trusted bank account number by a single digit. "The criminals have become experts at imitating invoices and accounts," Marker said. "And when a wire transfer happens," he added, "the window of time to identify the fraud and recover the funds before they are moved out of reach is extremely short."

In the case mentioned above—reported to the IC3 in June—after the accountant spoke to her CEO on the phone, she immediately reviewed the e-mail thread. "I noticed the first e-mail I received from the CEO was missing one letter; instead of .com, it read .co." On closer inspection, the attachment provided by the "lawyer" revealed that the CEO's signature was forged and the company seal appeared to be cut and pasted from the company's public website. Further assisting the perpetrators, the website also listed the company's executive officers and their e-mail addresses and identified specific global media events the CEO would attend during the calendar year.

The FBI's Criminal, Cyber, and International Operations Divisions are coordinating efforts to identify and dismantle BEC criminal groups.

FBI Special Agent. Maxwell Marker, who oversees the Bureau's Transnational Organized Crime, said, "We are applying all our investigative techniques to the threat, including forensic accounting, human source and undercover operations, and cyber aspects such as tracking IP addresses and analyzing the malware used to carry out network intrusions. We are working with our foreign partners as well, who are seeing the same issues."

He underlined, that companies should make themselves aware of the BEC threat and take measures to avoid becoming victims.

7.3 The Top Five recent victims of BECs attacks:

The examples of the five recent victims of BEC's fraud are following (17) : https://blog.cloudmark.com/2016/04/14/the-top-5-email-wire-fraud-email-attacks-rising-in-frequency-increasing-in-financial-losses/

- **Xoom, $30 million (US)** – January 2015

  In January of 2015, Xoom Corp., an international money transfer reported that it a $30.8 million loss in the fourth quarter of 2015 due to fraud scam.

- **Scoular, $17.2 million (US)** – Feburary 2015

  Scoular Co., an Omaha based commodities trader (and one of the top privately held companies in the U.S.), lost $17.2 million in a spear phishing wire fraud scam.

- **Ubiquiti Networks, $46.7 million (US)** – August 2015

  Months later, in August, Ubiquiti Networks, a San Jose based networking technology company, fell victim to a $46.7 million attack, wiring this sum to a Hong Kong bank account controlled by the attackers.

- **FACC, $54 million (Austria)** – January 2016
  Fraudsters topped all previous records, making off with $54 million from FACC, an Austrjan aerospace parts manufacturer that designs and supplies parts to Airbus and Boeing.

- **Crelan Bank, $76 million (Belgium)** – February 2016
  The record for the largest loss from a targeted spear phishing wire fraud attack was broken when Crelan Bank in Belgium reported it lost $76 million.

7.4 SUGGESTIONS FOR PROTECTION

Raised awareness of the BEC scam has helped businesses detect the scam before sending payments to the fraudsters. Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.
For added protection, the businesses can use the following measures (18):

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of *abc_company.com would flag fraudulent e-mail of abc-company.com*.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign- off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

8. FRAUD AND THE LAW

The importance of the law in the fraud prevention is enormous. Most of the tools here described, have their origin in the legislation. The subject is wide so here we can only give some example:
The Internal control systems, Risk management, Ethics Code are required, or indicated as "Best practice", by specific laws or corporate governance codes, adopted in various countries (for example: Unified Code, Combined Code, Sarbana-Oxley Act, Prada Code).
Also the" whistleblower hotline" was mandated by the U.S. Sarbanes-Oxley Act of 2002 and the other examples can be given.
The **European Anti-Fraud Office** (OLAF) investigates fraud against the EU budget, corruption and serious misconduct within the European institutions, and develops anti-fraud policy for the European Commission.
Between 2010-2015, OLAF:

- Concluded over 1,400 investigations
- Recommended the recovery of over €3 billion to the EU budget

- Issued over 1,600 recommendations for judicial, financial, disciplinary and administrative action to be taken by the competent authorities of the Member States and the EU

As a result of OLAF's investigative work, sums unduly spent were gradually returned to the EU budget, criminals faced prosecution before national courts and better anti-fraud safeguards were put in place throughout Europe (10).

For years, cyber fraud wasn't part of the official crime survey and wasn't seen as a priority by police and politicians. But the widespread use of computers, laptops and smart-phones to facilitate fraud has changed all that - and the survey is finally catching up.

Just two more recent examples: President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is a solid legislation that combats cybercrime.

The European Union adopted directive 2013/40/EU introducing new rules which harmonize the penalties for crimes against information systems. These rules include **outlawing the use of so-called botnets** -- malicious software designed to take remote control of a network of computers. It also calls for EU countries to use the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology.
All offences of the directive, and other definitions and procedural institutions are also in the Council of Europe's Convention on Cybercrime.

Instead, due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals.

For these reason, the awareness of the cyber fraud risk, the knowledge of the main tools of defense against these attacks, is necessary.

CONCLUSIONS

A constant increase in the number and severity of cases of corporate fraud, requires from all us: a single, a society, the state and the supranational structures, to adopt effective measures to combat this serious social problem.

To be aware of the fraud risk, of its several aspects, is essential in identifying effective tools for prevention, detention and punishment of fraud.

This was the main objective of the article. We have furnished some theoretical aspects and practical examples, in order to help the management to start in facing the problem.

Some measures of fraud prevention and detection, both, traditional and cyber fraud, have been showed.

But beyond all possible techniques, the condition to achieve a successful outcome in the fight against fraud is to impose the values such as: **respect, integrity**, **courage** and **transparency.**

Therefore, it is the duty of all, who influence the behavior and mentality of the people e.g. schools, universities, media, to consolidate the importance to act with integrity, to respect the laws, to disseminate the concept that "**doing the right thing' is foundational to everything we do".**

Bibliography

1. ACFE (2007): Managing the Business Risk of Fraud: A Practical Guide.
2. http://www.acfe.com/
3. CIMA (2008): Fraud risk management: A guide to good practice.
4. www.cimaglobal.com/
5. Internal Control System, (http://www.objectivecontrols.com/)
6. L'Orèal, Financial Reports 2013-2015.
7. Martinazzo, S. And Migliorini, S. (2012): Sistemi antifrode: I pilastri fondamentali" Diritto 24Ore.
8. Mohr, A. (2016): Examples of Internal Control Over Financial Reporting. http://smallbusiness.chron.com/examples-internal-control-over-financial-reporting-3808.html http://smallbusiness.chron.com/
9. Murphy, P. and Dacin, M.T (2011): Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations", Journal of Business Ethics.
10. OLAF (ec.europa.eu/anti-fraud/)
11. https://nevadasmallbusiness.com
12. Sutherland, E. H., Cressey, D.R. and Luckenbill, D.F. (1992): Principles of Criminology.
13. Webley, S. and More, E. (2003): Does Business Ethics Pay?, IBE.
14. https://www.fbi.gov
15. https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud.
16. https://www.fbi.gov/news/stories/business-e-mail-compromise

17. https://blog.cloudmark.com/2016/04/14/the-top-5-email-wire-fraud-email-attacks-rising-in-frequency-increasing-in-financial-losses/
18. https://www.ic3.gov/media/2015/150827-1.aspx

DOCUMENTS TÈCNICS

- Tancament comptable i fiscal per a les Pimes desembre 2016 (Manuel Rejón)
- Tractament comptable de la cessió d'un terreny a canvi de la reserva d'aprofitament. BOICAC Nº 101: Consulta 2 (Comissió Comptabilitat-Fiscalitat)
- Comptabilització de llegats de caràcter no reintegrable rebuts per una entitat sense ànim de lucre. Concordança amb la norma NRV 20ª del Pla General de Comptablitat d'entitats sense finalitats lucratives (PCESFL). BOICAC Nº100, Consulta 6 (Comissió Comptabilitat-Fiscalitat)
- La valoració posterior dels fons de comerç en els estats financers. Un estudi introductory (Joan-Emili Masferrer)
- Preparant els pressupostos 2017 de l'empresa (ACCID-CECOT)
- Programari gratuït interactiu dels Ràtios Sectorials 2014 (Luis Muñiz)
- RÀTIOS SECTORIALS 2014 Comptes anuals (balanç i comptes de resultats) de 166 sectors. 25 ràtios per cada sector (ACCID-UPF-BSM-CGE-ICJCE)
- Memòria normal
- Introducció a la filosofia del marge. Claus de la gestió del marge per maximitzar beneficis (Comissió de Comptabilitat de Gestió)
- Plantilla Memòria Pimes 2016
- Plantilla Memòria Abreujada 2016
- Determinación de las pérdidas computables para la reducción obligatoria de capital y para la disolución por pérdidas (BOICAC Nº102 de 2015: Consulta 5) (Comissió Comptabilitat-Fiscalitat)
- Relació de consultes ateses el 2015 (ACCID)
- Codi d'Ètica per a Professionals de la Comptabilitat (versió catalana per: ACCID-CCJCC)
- L'obligació de conservació de la documentació comptable i els seus efectes sobre la normativa fiscal (Comissió Comptabilitat-Fiscalitat)
- Comentari tècnic sobre consulta ICAC Tractament comptable dels costos d'ubanització i del dret de superfície (BOICAC Nº102/2015 Consulta 4)
- 10 errors clau en la negociació bancària (Joan Anton Ros Guasch)
- Comentario técnico sobre consulta ICAC. Fecha de efectos contables en un proceso de fusión entre sociedades de un grupo (BOICAC Nº102/2015 Consulta 2). (Comisión Contabilidad-Fiscalidad)
- La nova normativa Comptable dels ens públics locals (Josep Viñas-Comissió Comptabilitat Pública)
- Tancament Comptable i fiscal per a les pimes - Revisió febrer 2016 (Manuel Rejón)

- Projecte de modificació del PGC PIMES i del PGC de 2007, de les Normes de Formulació de Comptes Consolidats de 2010 i del PGC d'entitats sense finalitats lucratives de 2011 (Comissió comptabilitat ACCID-CEC)
- Mejoras a introducir en la cuenta de pérdidas y ganancias (Subcomisión 2ª)
- Comentarios a la nueva ley del impuesto sobre sociedades y al proyecto de reglamento del impuesto sobre sociedades (Com. Comptabilitat i Fiscalitat)
- Anàlisi canvis règim econòmic de la nova Llei de Cooperatives de Catalunya (Com. Cooperatives)
- El despacho de nueva generación (Oriol López Villena)
- Aspectes clau del perfil emprenedor global (Ferran Lemus)
- Principales novedades de la Ley de Sociedades de Capital (Departamento Técnico del Col·legi de Censors Jurats de Comptes de Catalunya)
- Cierre contable fiscal para las Pymes (Manuel Rejón)
- La factura electrónica: una realidad de las administraciones (Comisión OSI-comisión conjunta CEC-ACCID)
- La fase final de migración a SEPA (Pere Brachfield)
- Efectos contables de la Ley de apoyo a los emprendedores (Ley 14/2013 de 27 de septiembre) (Anselm Constans)
- Impuesto sobre el valor añadido. Criterios de caja: Aspectos relevantes y contabilización (Gemma Palet y José Manuel Lizanda)
- El control presupuestario en las empresas editoriales (Nati Sánchez Aznar)
- El cuadro de mando: soporte de sistema de indicadores (Luis Muñiz)
- Capital humano: un intangible relevante durante la crisis (Joan Anton Ros Guasch)
- El ABC del Credit Manager (Joan Anton Ros Guasch)
- El nuevo impuesto sobre sociedades (Comisión Relaciones Contabilidad-Fiscalidad)

Nuevas tablas de amortización (Jordi Baqués)

Per a consultar els documents relacionats **clica aquí**

DOCUMENTS DE RECERCA

- How to write a study case (Jordi Carrillo)
- Tesi de Màster (TM). Guia per a l'elaboració (Daniel Ferrer i Marc Oliveras)
- Com redactar un cas (Jordi Carrillo)
- Treball Final de Grau (TFG). Guia per a l'elaboració (Daniel Ferrer)
- Perspectives de la ciutadania de la RS corporativa de les empreses a Catalunya (F.Marimon i M.Alonso)
- Anàlisi de les relacions indirectes i les variables d'entorn en la cadena de valor del Quadre de Comandament Integral (Josep Llach Pagès)
- Detecting Accounting Fraud – The Case of Let's Gowex SA (Elena Helbig)

- Un altre finançament per a les empreses Cooperatives (Montserrat Sagarra)
- El método de estudio de casos en la investigación empírica en contabilidad (Maria J.Masanet Llodrà)
- Associació de Comptables de Catalunya (1924-1940) (Marc Amat)
- Análisis de las modificaciones estatutarias para adaptar el régimen de reembolso del capital social a las normas contables de las Cooperativas (Yolanda Montegut, Joan Josep González, Joseba Polanco y Ramon Bastida)
- Investigación en contabilidad en Cataluña: Diagnóstico de la situación actual y perspectivas (Soledad Moya, Diego Prior y Gonzalo Rodríguez)
- Efectes econòmics de la primera aplicació de les normes Comptables de les Cooperatives adaptades a la NIC 32 i la CINIIF 2 (Ramon Bastida i Lluís Carreras)
- Los indicadores no financieros como herramienta para la gestión de la empresa: análisis empírico en PYMES (Jordi Perramon)
- Efectos de la aplicación de las NIIF en el coste de capital de las empresas españolas (David Castillo Merino, Carlota Menéndez Plans y Neus Orgaz Guerrero)
- Análisis de la inversión empresarial catalana en China (Ana Beatriz Hernández)
- Indicadores de responsabilidad social de las organizaciones del ámbito de trabajo (Montserrat Llobet Abizanda)
- Percepciones de las cooperativas catalanas auditadas sobre el proceso de implementación de la NIC 32 en el capital social (Comisión Contabilidad de las Cooperativas)
- Aplicación de herramientas de la contabilidad de gestión en la administración local (Josep Viñas y Pilar Curós)
- Grado de Implantación del USALI en el sector hotelero de Cataluña (Lucia Clara Banchieri y Fernando Campa)
- El Impacto de la transición al nuevo PGC de las grandes empresas catalanas (M.Àngels Fitó, Francesc Gómez, Soledad Moya)
- El grado de implantación del CMI en las empresas catalanas (Lucía Clara Banchieri y Fernando Campa)

Per a consultar els documents relacionats **clicka aquí**

ACCID
Associació Catalana de Comptabilitat i Direcció
Associació Catalana de Comptabilitat i Direcció
Edifici Col·legi d'Economistes de Catalunya 4a. Planta, Barcelona
Tel. 93 416 16 04 extensió 2019
info@accid.org
www.accid.org
@AssociacioACCID