Cloud P2P Automation. Easy. Powerful. Smart.

Game of Fraud: Return of the CFO

July 2019

Executive Summary

Security, which involves preventing and fighting fraud—especially for documents—is a topic that continues to grow in today's world of ongoing digital transformation. Warning lights are flashing red at many companies: The Association of Certified Fraud Examiners reports that U.S. Businesses **will lose an average of 5%** of their gross revenues to fraud. This same 2018 report reveals that private companies and small business rank highest in occupational fraud frequency at 42% and a median loss of $164,000 compared to large corporations, government and non-profits.[1]

Nonetheless, awareness regarding this reality has yet to be followed through with actions. Most organizations do not have a contingency plan that they can activate in case fraud occurs, despite the considerable risks: Financial impact is at the top of the list, followed closely by data theft and potential impact on the company's reputation.

Companies with a proactive approach gain many benefits, including: Greater loyalty from their clients; reduced operating costs; better brand image for their company; and promotion of their brand value as an employer.

Responsible for the company's financial health, the CFO is therefore explicitly involved with any losses caused by fraud, naturally on the front-line for leading the fight. Nonetheless, the fight against fraud must be part of a global strategy based on three core pillars: New technologies, the organization itself, and behavior.

It involves behavioral organizational solutions that include raising employee awareness significantly, communicating clearly at all levels of the company, systematizing and increasing controls, special audits, and more.

Lastly, it is important to pay attention to technology, which happens to also be the fraudster's favorite tool. Many solutions are available today that leverage advanced technologies for automatically detecting fraud. This includes Big Data as well as invoice digitalization solutions powered by artificial intelligence (AI).

If CFOs are going to be effective in leading the fight against fraud, they will need to adapt their defenses to face new and more aggressive forms of fraud, and fraudsters who are better organized than ever. **This leads us to the seven responsibilities of the CFO:**

1. **Make risk management your priority**
2. **Automate your processes**
3. **Communicate with IT**
4. **Acquire new skills**
5. **Engage internal stakeholders**
6. **Implement a cloud-based automation solution**
7. **Choose the right technology tools**

[1] AFCE 2018 Report to the Nations Global Study on Fraud and Abuse

Table of Contents

Introduction

Despite the implementation of increasingly sophisticated mechanisms, corporate fraud continues to gain ground, as illustrated by data that is both surprising and worrisome: U.S. businesses ***will lose an average of 5%*** of their gross revenues to fraud.[1]

It is important to note that not all companies are on equal footing when it comes to their fight against fraud. The human, organizational, and financial means implemented for protection will be different for small- or medium-sized enterprises (SMEs) as Fortune 500 companies.

Nonetheless, two indisputable facts can be mentioned: On one hand, no company can escape the danger of fraud; on the other hand, there is no direct connection between company size and the monetary amounts of fraud. It is also observed that the human factor is both an Achilles heel for the company and its savior. In fact, most fraud attempts are defeated by human intervention.

While digital transformation has been a strong boost for productivity within companies, it also opened a new window through which fraudsters—ever more well informed and better organized—can enter; the two are intrinsically linked with each other.

CFOs are the guardians of financial information and are therefore ideally positioned to administer a solution. CFOs are the ones who diagnose the problem and mobilize all available resources to mitigate and ultimately prevent fraud.

Still, they will legitimately ask themselves several questions. The answers to those questions are the backbone of this white paper, written for general directors, finance leaders, accountants/controllers, and IT security staff:

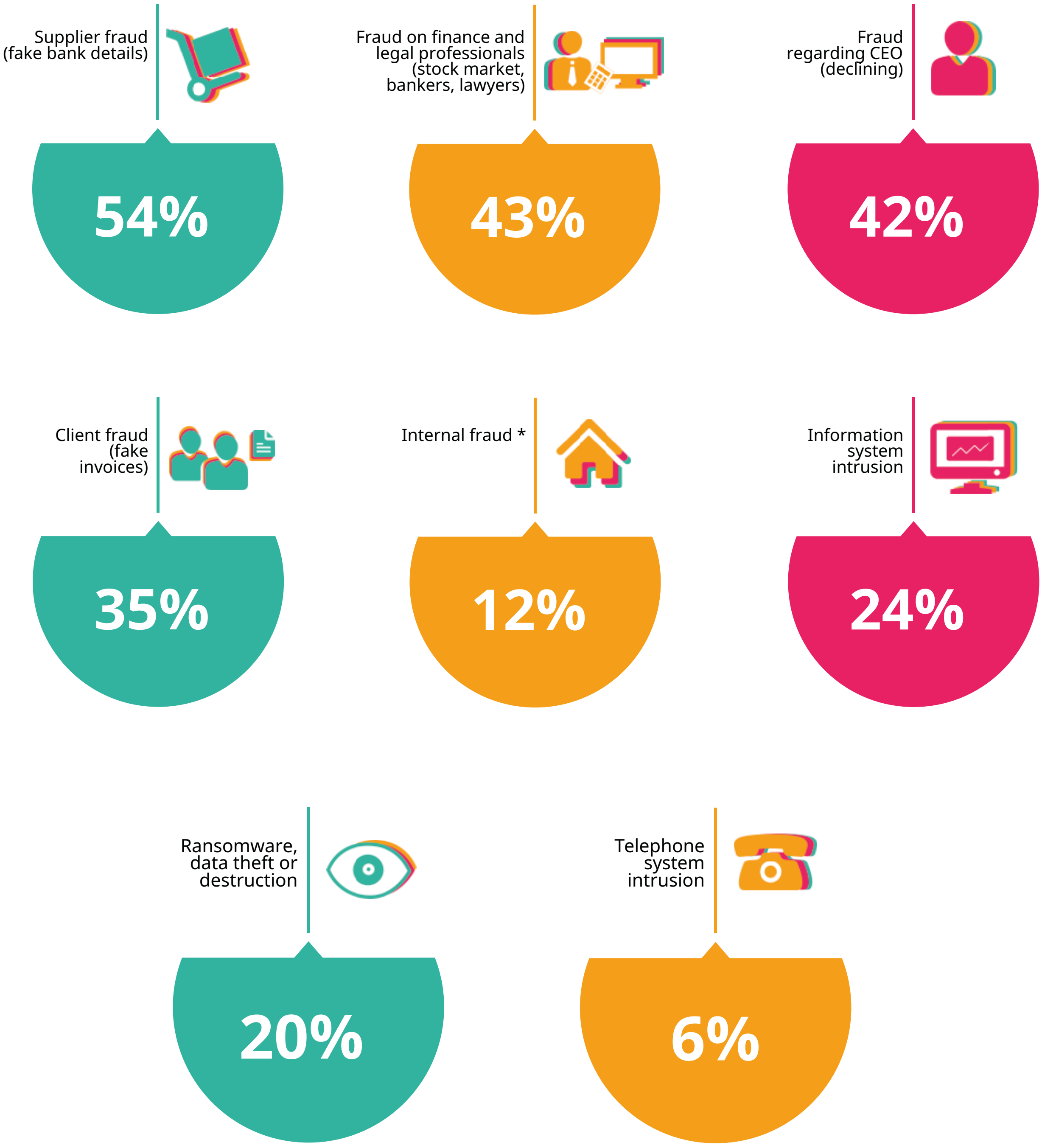
1. What exactly are the threats and what risks do they represent?
2. Why invest in fraud prevention?
3. What are the best human, organizational, and technological practices, and what are the most effective tools to implement?

[1] ACFE 2018 Report to the Nations Global Study on Fraud and Abuse

PART 1

What are the different types of fraud?

Types of **fraud** affecting **companies** in 2017



Supplier fraud (fake bank details)	54%
Fraud on finance and legal professionals (stock market, bankers, lawyers)	43%
Fraud regarding CEO (declining)	42%
Client fraud (fake invoices)	35%
Internal fraud *	12%
Information system intrusion	24%
Ransomware, data theft or destruction	20%
Telephone system intrusion	6%

** (Breach of trust; embezzlement; fraudulent checks, ghost employees; employee overpayment; reimbursement of fictitious expense reports; theft of raw materials, finished products or semi-finished products)*

Other types of fraud include corruption, funding terrorism, money laundering, unethical behavior, circumventing embargoes.[1]

[1] Euler Hermes-DFCG study, 2018

This leads to a preliminary conclusion...

Technologies can continue to offer better performance and security, but the reality is that the ***human factor*** is still the main source of vulnerability in terms of exposure to fraud today.

An employee is somehow involved in most confirmed cases of fraud. Sadly, in the U.S., fraudsters who have longer tenure with their company (five years or more) stole twice as much! An average of $200,000 compared to employees with tenure of less than five year.[1]

68 percent of the fraud committed by individuals outside the company is actually the act of people close to the company in some manner, notably partners such as sales agents, clients, service providers, and others.[2]

Tweet now!

Only 19 percent of the cases of corporate fraud are perpetrated by the company's senior management, but the median loss is $850,000.[1]

[1] ACFE 2018 Report to the Nations Global Study on Fraud and Abuse

[2] Euler Hermes-DFCG study, 2018

PART 2

What are the risks for companies?

Financial risk

The company's **cash** is the first aspect impacted when fraud occurs. An invoice that you thought was paid, but whose payment really got lost on the beaches of some exotic country, must be paid again, this time to the right supplier.

An urgent wire transfer to cover a transaction that needs to remain confidential, demanded by someone who does a very good job convincing a naive staff member that he's the CEO, could literally empty the company's bank account from one day to the next.

Operating income is affected as much by posted losses as by provisions for bad receivables. Once recorded in the accounting system, they both result directly in a loss in cash flow from operations, lower net profit and potentially even tension with shareholders.

Data theft

Plain and simple, data theft is both real and problematic. It may have an internal cause (such as an unhappy or dismissed employee), or external, with malicious or criminal intent. The fraudster gets into the information system and copies everything needed for some benefit.

We know today that the value of many companies is largely comprised of immaterial assets. One of the greatest riches of a commercial company are its client data files as well as the nature of its business agreements and partnerships. It is easy to see the seriousness of this threat, which can take two forms:

- Inaccessibility to data, which would block the company's commercial, operational, and industrial activities.
- Malicious use of corporate data, which could incur significant legal liability for the company, serious damage to its reputation, and potential financial consequences for its customers.

In addition to these two impacts, which can be measured precisely, two other types of impact are also relevant—though inherently less quantifiable—and just as detrimental for the company and its employees.

HR and psychological impact

Nobody remains unaffected by fraud, especially if the source is internal. Once revealed, it always shocks the company to its core. It affects employees psychologically when they feel betrayed by a work colleague that they have known for a long time, as well as the fraudster’s managers, who may wonder whether they truly respected company procedures to the fullest extent. Also, is job seniority a factor for trust or just the opposite, something to be wary of? (Remember our statistic earlier in this report that fraudsters who have longer tenure with their company stole twice as much.)

In this context, it is important to not underestimate the impact of fraud on the person abused by scammer. He or she surely will have talked with the fraudster on the phone or exchanged e-mails. The person’s own involvement might even be questioned, even if there was none. Their professional abilities and judgement may be doubted, and it may be hard to trust this “collateral victim” again.

The human factor is clearly at the heart of the problem. The company will no doubt have to revisit basic concepts of trust and routine, as management has less of a tendency to supervise the tasks of employees who have held their jobs for a long time.

It might also be a good idea to think ahead of time about how to manage the post-fraud phase suffered by employees so that they do not feel weakened.

Impact on reputation

Similar to properly managing the stress following fraud by one or more employees, it is important to know how to manage that type of incident on a company-wide basis.

Falling victim to fraud impacts the company’s reputation, which means external communication must also be fully controlled with all stakeholders:

- The company’s main commercial partners, namely its clients and suppliers. (Suppliers could question their allowed debt amounts, while clients could even consider changing providers due to fear for the security of their data.)

- Financial partners such as banks, angel investors, and venture capital firms.
- Shareholders, who may worry about managers’ lack of professionalism, leading to a bad reputation for the entire company.

Even if this last point is only relevant for some types of companies, such as large organizations and highly funded start-ups, the overall issue of reputation concerns ***all*** companies, even small businesses.

PART 3

What ar
of advanced fraud
mitigation?

Beyond the understandable peace of mind that security brings and assurance that the company will not (or will no longer) become the victim of attempted or successful fraud, security for processes represents a competitive advantage due to its reinforcement of the company's reputation for reliability, reassurance for commercial partners, and more.

Increasingly tighter regulations, such as Europe's GDPR, the Sapin 2 law in France, the California Consumer Protection Act (CCPA), and other recent and highly restrictive anti- corruption laws, were first seen by managers as an obstacle or nuisance for their companies, potentially even slowing their growth. Various types of fraud and embezzlement have clearly been around in companies for a long time, but the issue used to remain more or less in the background, or "something that only happens to others."

The turning point happened at least a decade ago, when authorities categorically asserted that fraud could also be used as a means to finance terrorism and money laundering. Companies therefore progressively began to consider the potential of fraud in their operations. The most responsive and best-organized companies quickly derived a number of benefits.

Client loyalty

Clients will remain loyal to companies that they have confidence in. Rigorous compliance with procedures and the application of a variety of regulations often embodied by standards and certifications reassure the company's partners and are often even a determining selection criteria for clients and suppliers.

Reduced operating costs

Eliminating exposure to financial risks, avoiding production shutdown, and even maintaining business activity by mitigating or even preventing fraud all impact the bottom line.

Improving brand image

Communicating a company's fraud prevention practices, how it manages the risk of fraud, and how it shields itself from outside threats contributes to a strong corporate reputation. In the event of a breach, implementing a solid crisis communications plan achieves the same.

Promoting the employer brand

Companies reinforce their attractiveness with respect to employees by combining strength and security, encouraging people to dedicate themselves more deeply, and inciting interest from job candidates.

PART 4

Which prevention method?

Anti-fraud effectiveness

Anti-fraud procedures are more likely to exist and be effective in larger and morewell-organized companies. Actions that may seem obvious and even essential for a large enterprise may be less so for SMEs and VSEs.

But their exposure to the risks of fraud is the same. A good strategy to fight against fraud is based on three key pillars: Advanced technologies, the organization itself, and human behavior.

Advanced technologies:

- Technologies are at the origin of modernization and digitization within companies.
- Technologies help finance departments systematize fraud detection.
- Technologies offer more "firepower" against fraud and enable adaptation that is not offered by more traditional methods.

The most advanced technologies in this battle are ***Big Data, machine learning*** and ***digitization.***

Big data enables handling vast volumes of information, often in real-time. Machine learning is a component of artificial intelligence in its broader meaning, seeking to create and use algorithms to obtain predictive analysis based on data. Together, they make it possible for the company to go even further, such as risk scoring its clients and suppliers.

Digitization, or automation, technologies that leverage AI are the other essential tools and an important part of any effort to mitigate risks. It not only increases speed, but it also reduces costs and improves agility. Creating and organizing a rigorous process that includes complete traceability and security makes these solutions extremely effective in fighting fraud.

Tweet now!

Internal control weaknesses were responsible for nearly half of frauds.[1]

[1] ACFE 2018 Report to the Nations Global Study on Fraud and Abuse

More advanced technologies

RPA (Robotic Process Automation) is another technology based on machine learning and further automates tedious and repetitive tasks. For example, a “software robot” can query databases, maintain records, establish accounting reports, and even process simple transactions.

At the same time, it is important to remember that new technologies also hel fraud- sters who often release a treasure trove of imagination and ingenuity to achieve their goals.

Companies and their finance departments can leverage all of these advanced technologies to stay one step ahead of fraud and its ever more challenging landscape.

Behavior

Raising employee awareness is one of the most important aspects of fraud prevention. As mentioned earlier, most fraud takes advantage of a lack of vigilance, a level of employee naivety, or even cooperation within the company or its close partners.

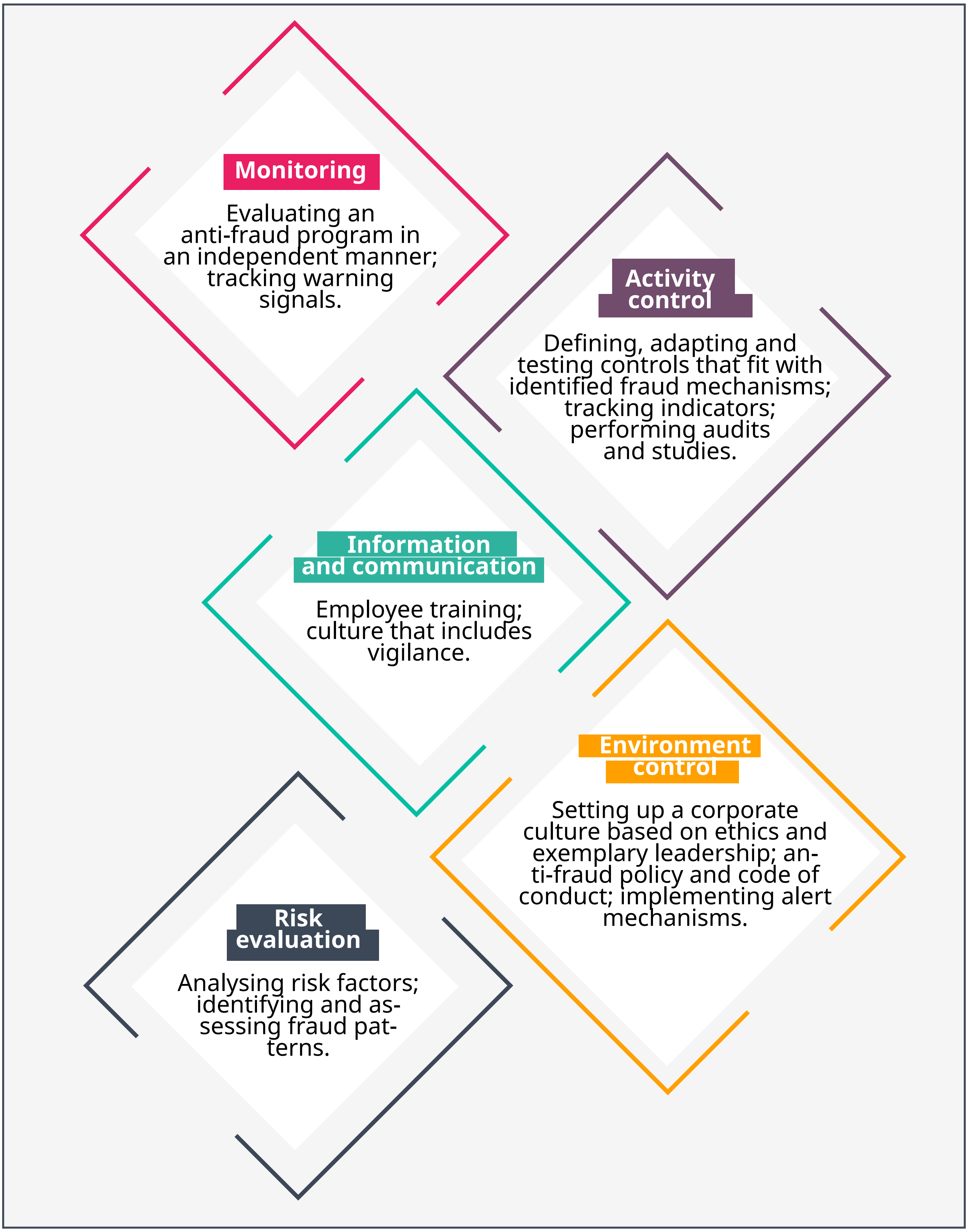
Two points stand out in particular:

- Raising awareness and providing training to all departments and every hierarchical level within the company, including top management, is important so everyone knows the role they play in identifying warning signs and exposing potential fraud.
- It is also important to implement communications that are adapted to each different stakeholder group within the company, that reflect the company’s commitment to fraud prevention, and identifies the consequences of not taking fraud prevention seriously as well as the benefits of executing well-defined fraud prevention plans and practices.

Messaging and communications need to be presented according to the company’s size, business sector, and internal specifics (work practices and target employees) to avoid the risk of creating a disconnect between theory and practice.

Your organization

Internal control is certainly not a new idea. Furthermore, companies can leverage the COSO (Committee of Sponsoring Organizations of the Treadway Commission, a joint initiative to combat corporate fraud) framework created in 1992, followed more recently by COSO 2. But even if the framework's components are increasingly challenged by new technologies, they remain a fundamentally appropriate guideline based on the following:



Monitoring

Evaluating an anti-fraud program in an independent manner; tracking warning signals.

Activity control

Defining, adapting and testing controls that fit with identified fraud mechanisms; tracking indicators; performing audits and studies.

Information and communication

Employee training; culture that includes vigilance.

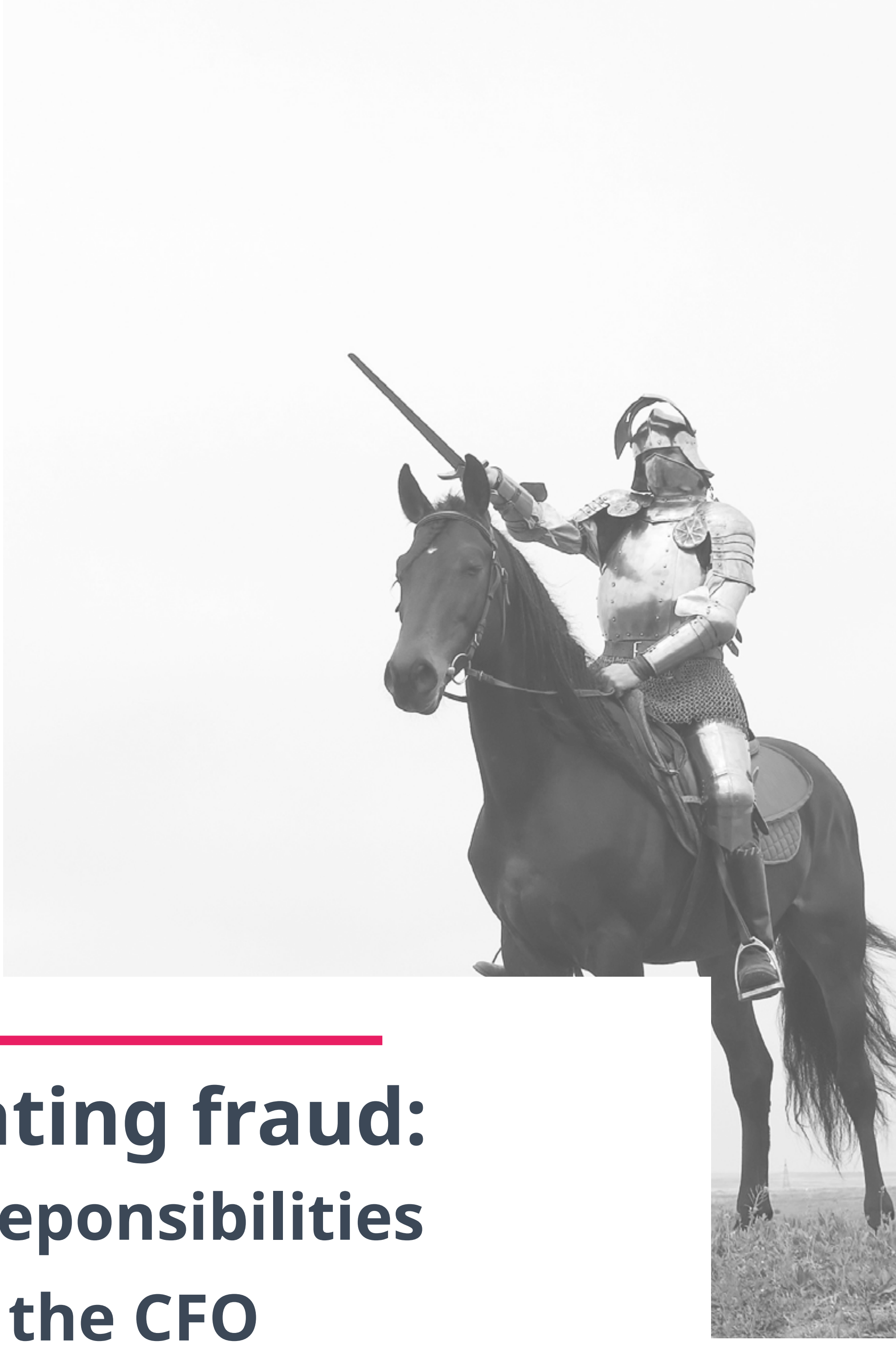
Environment control

Setting up a corporate culture based on ethics and exemplary leadership; anti-fraud policy and code of conduct; implementing alert mechanisms.

Risk evaluation

Analysing risk factors; identifying and assessing fraud patterns.

PART 5



Mitigating fraud:

Seven reponsibilities of the CFO

Chief Financial Officers have always played a strategic part in managing risk, notably regarding their advisory role and position as a stakeholder, their ability to clarify and facilitate decision-making, and their in-depth knowledge of organizations through financial data analysis. Today, they must adapt all these skills to face new and more aggressive forms of fraud, extending beyond traditional types such as internal embezzlement and industrial espionage.[2]

How?

Key elements CFOs should adopt to mitigate against fraud.

1

Make risk management your priority

Companies worldwide lost more than $7 billion due to fraud![1]

However, despite these alarming figures, a report by PwC confirms that only half of the companies surveyed say that they carried out a global risk evaluation regarding fraud over the past two years. That figure is still far too low given the many downsides of falling victim to fraud.

[1] ACFE 2018 Report to the Nations Global Study on Fraud and Abuse
[2] PwC, 2019 Priorities for Chief Financial Officers
[3] PwC Global Economic Crime and Fraud Survey 2018

2

Automate your processes

Opportunities for fraud may arise from vulnerabilities in processes.

In many cases, these vulnerabilities may be “easily” rectified by automating time-consuming and repetitive tasks that are sources for errors.

Chief Financial Officers who have adopted automation also see an additional opportunity to enable their team to focus their effort on statistical analysis, risk prevention, and strategic consulting.

3

Communicate with IT

30 percent of CFOs and Chief Information Officers (CIOs) agree on at least one point: CFOs have an outdated perspective of CIOs.[4]

People often talk about a conflictual relationship between CFOs and CIOs: Misunderstanding, notably a lack of technical expertise versus a lack of business vision. In today’s context of digital transformation, facing increasing security vulnerabilities, sensitive data may be at risk, including client files, bank account details, patents, and more. CFOs and CIOs must therefore learn how to work together. While the CFO remains the protector of cost-related factors, the CIO’s role is essential for helping finance departments manage data and technology tools.

[4] Forbes Insight, 2017

4

Acquire new skills

Data, which has become an undisputed source of value for the company’s strategic growth decisions, is now also the cornerstone for finance departments, nonetheless introducing risks related to data integrity and security.[5]

CFOs need to work with experts to master this data science and therefore rise to the occasion in their effort to fight fraud and improve reporting. The PwC report confirms this trend, stating that CFOs in 2019 were convinced of the need to surround themselves with new talent, people with technical-operational profiles able to master software robots. This includes data scientists, business analysts, and more.

5

Engage internal stakeholders

Regardless of their form, organizational transformation projects yield their full potential when teams are actively committed. This applies even more when handling issues related to fraud, as the human factor is often the primary source of risk. Training employees and raising awareness must therefore be among the CFO’s top priorities.[2]

[2] PwC, 2019 Priorities for Chief Financial Officers
[5] Gartner 2017 CIO Agenda Survey

6 Implement a cloud-based automation solution

For 83 percent of CFOs (compared to 31 percent in 2016), the Cloud has become inevitable in every area including document digitization, financial closing files, and cash management. Providers today are in a position to offer robust and secure environments that are ISO certified and accessible to all companies and organizations.[2]

Download the 2019 Payables Insight Report: Understanding the Value of Holistic Invoice-to-Payment Automation

7 Choose the right technology tools

There are now some very effective technology tools for supporting finance departments in their fight against fraudsters. But how to choose the right one?

Automation tools have become essential for financial decision-makers and are now more operational than ever.[6]

In addition to ensuring total traceability of all actions taken regarding documents, the most advanced tools also integrate algorithms capable of extracting all the data present in those documents in order to detect and prevent document fraud and trigger alerts if abnormal data is detected.

Tweet now!

For more than 60 percent of CFOs, automation is still one of the top three priorities, playing a central role in the digital transformation process

[2] PwC, 2019 Priorities for Chief Financial Officers
[6] Euler Hermes Blog, 2019

PART 6

How to combine performance and security

The conclusion is clear: Digital transformation has considerably expanded the CFO's to-do list. Having to oversee accounting and finance operations, the growing risk of fraud, and the company's ongoing quest to improve performance by optimizing processes, the CFO's role no longer really involves managing priorities but also requires being able to address all issues coherently with a single and global strategic response.

Automation solutions enable CFOs to optimize finance and accounting processes from purchasing cycles through invoice payment, while enhancing security along the way.

Why is digitizing Purchase-to-Pay (P2P) processes the ideal solution for managing CFO priorities?

1 Digitization: A direct solution for CFO performance issues

The benefits derived from automating P2P processes have already been demonstrated. The main benefits include: Validation cycles five to 20 times faster; total traceability of all operations; elimination of risks related to document loss; two-fold increase in productivity; reduced administrative costs; access to all digital documents in real-time, and more.

Download the IOFM Report: The Future of Accounts Payable: Digitable, Profitable and Strategic

2 Po aud

These expert systems are involved from the very first step in the document automation process—capture—to detect fraudulent types of behavior. Examples include detecting modified information on an invoice by tracking down any changes made in the image, such as bank details, which is one of the leading sources of invoice fraud.

The technologies integrate powerful artificial intelligence algorithms that can not only adapt to all types of documents —even those with variable structure—but also learn from examples and create their own knowledge base. For example, statistical analysis can detect unusual monetary amounts with respect to data on supplier history. Users are then alerted in case amounts higher than usual are found. This type of technology also detects suspected duplicates, that is, invoices with the same numbers and supplier names.

Thanks to total traceability of all interventions, including dates, modified values and identification of people making changes, companies are in a better position than ever for identifying fraudsters.

Conclusion

Judging by the many articles in business publications, it is clear that fraud represents a major preoccupation for Chief Financial Officers.

We wrote this white paper to share some applicable and realistic tools for understanding and fighting fraud. Truly the driving force in the battle, CFOs must nonetheless adhere to a global strategy that combines human factors, technology, and organizational considerations.

When faced with several safes, a thief will always choose the one that's easiest to open.

yooz

Cloud P2P Automation. Easy. Powerful. Smart.

Yooz provides the smartest, most powerful and easiest-to-use cloud-based Purchase-to-Pay (P2P) automation solution. It delivers unmatched savings, speed and security with affordable zero-risk subscriptions to more than 3,000 customers and 200,000 users worldwide.

Yooz's unique solution leverages Artificial Intelligence and RPA technologies to deliver an amazing level of automation with extreme simplicity, traceability and end-to-end customizable features. It integrates seamlessly with more than 200 financial systems, exceeding any other solution on the market.

Yooz is a fast-growing, award-winning company that perfectly fits the expectations of mid-size organizations across all sectors.It has been recognized as a SaaS innovator, recently named as a 10 Best Cloud Solution Provider by Industry Era, Best of SaaS Showplace (BoSS) by THINKstrategies, Top 10 Accounting Solution Provider by CFO Tech Outlook; and Top 50 Company to Watch by Spend Matters.

Yooz North America is headquartered in the Dallas, Texas metropolitan area with global offices in Europe.

Find out more:

www.GetYooz.com

Contact us

United States, Canada,
Latin America, Asia Pacific

@ contact@us.getyooz.com

☎ 832-384-9669

Europe, Middle East, Africa

@ contact@uk.getyooz.com

☎ +44 1252 741 517

France

@ contact@fr.getyooz.com

☎ +33 (0)1 73 60 9669

This document is provided only as a source of general information and is not intended to replace professional guidance regarding accountancy, tax issues, computer science, project management or anything else. For all specific questions, please reach out to your regular contacts or contact Yooz directly. Photos: Adobe Stock