ilce - institut de lutte contre
la criminalité économique
heg - haute école de gestion
arc

I^{2}FC

Interdisciplinary Insights on Fraud and Corruption

Red flags and publicly available information: an effective combination for reducing the costs of fraud

Isabelle Augsburger-Bucheli

Doctor in Law, Professor of Law, Dean of Institut de lutte contre la criminalité économique (ILCE - Institute of Economic Crime Investigation), Deputy Director of the Haute école de gestion Arc (HEG Arc – Business School), University of Applied Sciences and Arts Western Switzerland HES-SO

Espace de l'Europe 21, CH-2000 Neuchâtel (Switzerland)

isabelle.augsburger@he-arc.ch

Abstract

Recent developments in the field of the fight against economic crime have shown a focus on developing detection tools based on companies' internal data. Our project explores other sources in order to establish to which extent the risk of fraud in a Swiss company can be assessed using publicly accessible data. We have also analyzed and classified a large number of fraud red flags, exogenous as well as endogenous, deriving from both financial and extra-financial information. This process has allowed us to develop several copyrighted lists and spreadsheets that could be extremely helpful in fraud assessment. Publicly accessible data still represents an untapped source in the fight against such crimes: if used the right way, it could become an asset for businesses, investors, and public authorities alike. Several obstacles, however, must be overcome in order to achieve this goal: first and foremost, non-financial red flags are rarely referenced - and while they sometimes highlight interesting tendencies, they are not guaranteed to reveal actual fraud cases. Secondly, the validity of results obtained when using such red flags necessarily depends on the reliability of the sources. Such issues naturally call for further research work.

Keywords: occupational fraud, red flags, fraud prevention, fraud detection, economic crime, Switzerland.

JEL codes: K14 Criminal Law, K 42 Illegal Behaviour and the Enforcement of Law, K22 Business and Securities Law, L53 Enterprise Policy

1. Introduction

Studies by advisory firms and professional associations indicate that economic crime is on the rise, due in particular to the development of financial engineering, the use of new technologies and the globalization of economy (see for example: KPMG 2009, 2013a;PwC 2011a, 2011b, 2014a, 2014b). Occupational fraud is at the heart of this problem; it can be defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE, 2014: 6). Occupational fraud generates enormous costs for employers: ACFE 2014 reports that typical organizations lose a medial of 5% to all types of fraud. As a result, the implementation of efficient strategies allowing to prevent and detect fraud is a priority for many of them.

Most of the strategies in place today involve the monitoring and surveillance of employees, internal control, and the detection of red flags through the analysis of internal information (such as accounting data). Red flags are defined as situations or transactions that reveal or are susceptible to reveal a fraud, or that are typical of an environment where fraudulent behaviors can arise and proliferate (see, Hounnongandji, 2010: 251). While fraud, like most forms of economic crime, does not manifest itself in a direct or immediate way (like street crime usually does), it still leaves traces.

Red flags are based on information and situations that typically show up in connection with fraud. Therefore, in a context of prevention or investigation, they can be read as pieces of evidence that such a crime has occurred, is about to be committed, or is likely to take place in the analyzed environment. They are powerful weapons, alongside internal control and whistleblowing, in the fight against fraud. They can be particularly useful in the prevention phase, as they can help reduce the number and impact of fraud cases together with the related costs.

Those in use today, however, depend almost exclusively on internal information, which is often kept private. This has two consequences: because of the focus on internal data, the possible role of publicly available information (any data originating from public or private sources that is available to anyone, without restrictions, free of charge or otherwise) in fraud detection has been overlooked. The second consequence is that a serious assessment of fraud risk can be conducted exclusively by the company itself. Third parties such as business partners or investors, which may have a legitimate interest in assessing such risks, do not have access to necessary information, and cannot use it to identify possible red flags.

Our project was meant as a first step in an attempt to fill these gaps. We explored other possible sources of information in order to establish to which extent the risk of fraud in a Swiss company could be assessed using red flags based on public information. At the same time, we created a series of risk assessment tools that work with red flags suitable to facilitate the tasks of those having access to both internal and external information, but also useful to interested third parties. We also endeavored to create a functional red flags database that integrates public information as a possible source of detection.

2. Literature review

Although the idea of using public information for the purpose of assessment has already been implemented in other sectors, it has not yet been extended to fraud and economic crime in general. The *Fondation Ibrahim* has established a collection of quantitative data leading to a yearly evaluation of the performances, in terms of governance, within African countries. Similarly, the *Basel Institute on Governance* (a non-profit organization tightly associated with the Law Faculty of the University of Basel) has developed an index that uses red flags (developed based on public reports by GAFI and by the Wolfsberg Group) to classify countries based on the risk level in relation with money laundering, terrorism financing, and corruption.

While the above projects showcase the potential of public information-derived red flags, they do so in a context far removed from business and occupational fraud. When it comes to the latter, the available literature focuses, as expected, on red flags that depend on internal information (e.g. information related to internal service compliance, etc.), and which is therefore suitable for internal use only (Pons, 2006; Gallet, 2010). Several authors have developed charts containing red flags that can be detected and evaluated based on such data (see: Cauvin & Bescos, 2005; Ouaniche, 2009; Pons & Berche, 2009). The forensic services of the Big Four (Deloitte, EY, KPMG, and PricewaterhouseCoopers), who assist companies in internal investigations, do employ red flags as part of their process, but their tools - besides being shred in secrecy - also require access to internal data.

Part of our project involved the identification of types of public information that can lead to the detection of fraud red flags. As purely financial information is typically kept private, the data available to the public is largely of a non-financial nature. Studies conducted in the auditing field, where financial information is paramount, have showed that non-financial information - such as the number of employees, consumer satisfaction, and the number of open accounts (Ames et al., 2012) - should also be taken into consideration (American Institute of Certified Public Accountant (AICPA), 2002; Cohen et al., 2000), as it helps to generate a more trustworthy assessment of a company, unveil irregularities, verify the validity of financial performances, and sometimes even predict the latter. The importance of non-financial information has been also highlighted by a number of other studies focusing on corporate governance and social and environmental responsibility (e.g. Mauléon, 2007; Peter & Jaquemet, 2014.).

Despite this, and despite the fact that companies' communications are becoming more focused on extra-financial information (Mauléon, 2007), few authors have explored the question of its role and importance in fraud detection (e.g. Ittner & Larcker, 1998). The studies conducted so far, however, have the merit of showing that extra-financial information can indeed prove useful. Brazel et al. (2009) have shown a correlation between financial results and extra-financial information, and argue that variations within this correlation can suggest that financial results have been manipulated. Extra-financial information, while harder to be tampered with than its financial counterpart (Cohen et al., 2011), can still be falsified by the management, but the risk factor becomes higher: this is because its veracity is more easily verifiable (Bell et al., 2005), and also because the circle of people involved in the fraud is likely to be extended by such maneuvers. Finally, Grove & Basilico (2008; 11) “demonstrate the usefulness of both types of red flags - quantitative fraud ratios and qualitative corporate governance factors - for detecting fraudulent financial reporting. The qualitative corporate governance red flags are just as, or even more, important than the quantitative ones for both detecting and preventing fraudulent financial reporting, according to many fund managers, short sellers, financial analysts, and financial press writers".

In conclusion, extra-financial data that is publicly available represents a valid source of information that - while often overlooked - can play an important role not only in fraud detection, but also in fraud prevention. Indeed, according to KPMG (2013b), "failure to adequately assess clients, agents and business partners, and to know how they operate, can expose organizations to reputational damage, operational risk and government investigations, as well as monetary penalties and potential criminal liability".

3. Methodology

Red flags are powerful tools in the fight against fraud. They are particularly important because they can allow to prevent fraud and assess the risk thereof, thus helping companies to drastically reduce the costs linked with the phenomenon. Today, as we have seen, red flags are detected using almost exclusively private information, especially of a financial nature. Our project aimed to evaluate whether the use of publicly available information could lead to a more efficient detection of red flags and at the same time widen the circle of people that are susceptible to use such red flags, ultimately transforming the latter into a more complete and universal tool of fraud prevention.

We have structured our project in four phases. The first phase consisted in establishing a general inventory of reliable fraud red flags. In the second phase we identified types of publicly available information that could, realistically, lead to the detection of the listed red flags (for practical reasons, we limited ourselves to information available in Switzerland and pertaining to Swiss companies). The third phase consisted in cross-referencing each red flag with the information found in phase two; it allowed us to determine which red flags could theoretically be detected using the latter, and in which cases such information could contribute to a more efficient detection. Phase four is currently in progress: we are testing the red flags identified in phase three, with the objective of evaluating to which extent they could be used to assess the risk of fraud within a Swiss company.

3.1 Establishing a catalogue of occupational fraud red flags

We achieved this through a three steps process, which is described below.

3.1.1 Identification of fraud typologies

As a starting point, we have based ourselves on the three main categories of occupational fraud established by the Association of Certified Fraud Examiners (ACFE & Peltier-Rivest, 2007: 8):

- Asset misappropriation: "Any scheme that involves the theft or misuse of an organization's assets, such as skimming sales, fraudulent billing, payroll fraud, or expense reimbursement fraud."
- Corruption: "Any scheme in which a perpetrator uses his or her influence in a business or official transaction to obtain an unauthorized benefit contrary to that person's duty to his or her employer. Common examples include paying or accepting bribes or illegal gratuities, engaging in self-dealing transactions or engaging in conflicts of interests."

- Fraudulent financial statements: “Any scheme that involves the deliberate falsification of an organization’s financial statements to make the organization appear more or less profitable. Examples include recording fictitious sales and concealing liabilities or expenses.”

We have then selected a series of crimes and situations within such categories; we have based our choices especially on surveys by ACFE and the Big Four, both of which have a long-standing expertise in financial investigation and advisory services (see for example: ACFE 2012; ACFE & Peltier-Rivest, 2007; KPMG 2009, 2013a; Isenring & al., 2014; PwC 2011a, 2011b, 2014a, 2014b). Having observed that several frauds that occur frequently (such as e-mail scams) have little financial consequences, and that rarer typologies (such as fraudulent financial statements) can have an enormous impact, we have decided to take both categories into account.

3.1.2 Red flags collection

Through a literature search in which we have consulted multiple sources (such as Brown & DLA Piper LLP, 2012; Colby, 2004a, 2004b, 2004c; DiNapoli, 2010; Gallet, 2010; Golden et al., 2011; KPMG, 2012a, 2012b; Ouaniche, 2009; Pons & Berche, 2009; Singleton & Singleton, 2006; Zimbelman & Albrecht, 2011) we have gathered a large collection of red flags lists and tables, as well as articles and papers discussing one or more red flags. We have retained and listed those that are applicable to occupational fraud.

We have then conducted an empirical research in which we have studied well-documented fraud cases and analyzed the relevant jurisprudence from the Swiss Federal Supreme Court (*Tribunal fédéral*). We have also conducted interviews with several forensic accounting experts, with the objective of listing the techniques used by fraudsters as well as the evidence they leave behind. Through this process we have confirmed some of the red flags collected during our literature search and also established new red flags, which have been added to the list.

3.1.3 Red flag indexing

The large amount of information collected in 3.1.2 was taken from several different sources, and as such it needed to be organized and homogenized before it could prove useful. We have therefore placed the retained red flags (around a thousand) in a spreadsheet and applied filters (with the objective of merging similar items and eliminating duplicates), thus generating a catalogue consisting of 403 red flags. For these we have developed an ad hoc classification inspired by the works of Zimbelman and Albrecht (2011), by the Swiss SME chart of account (*Plan comptable suisse PME*), and by the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework. Every red flag included in the final list has been tagged with the fraud category(ies) it pertains to and placed, based on its impact and its nature, in one of the tiers described below. The categorization according to fraud type was made with the goal of obtaining a clearer overview of the catalogue and to render the search of specific red flags easier. It is not intended to be final nor completely accurate, as it involved several decisions which were made according to our project's needs.

Endogenous red flags

Endogenous red flags are those that are detectable using companies' internal information. They can be further classified in four sub-categories:

- Organisation: includes red flags linked with a company's functioning, structure, management, and performance, as well as with its employees' behaviors and issues.
- Internal Control System (ICS). In order to decide which red flags to list under this category, we have drawn inspiration from the COSO framework, which provides a benchmark for internal control standards and “helps organizations design and implement internal control in light of many changes in business and operating environments” (COSO, 2013). One of the functions of internal control is to allow companies to identify and eliminate fraud opportunities, thus drastically reducing the chances that such a crime will occur. According to Cressey' fraud triangle theory, all frauds are characterized by the simultaneous occurrence of three elements: motivation, opportunity, and rationalization. As Chapuis et al. (2016) point out, the discovery of gaps and weaknesses in the controls in place, or of a certain lack of discipline in their application, can be perceived as opportunities and encourage fraudsters to act. Since in the majority of cases individuals do not actively look for breaches, but are willing to take the opportunities that arise, eliminating such opportunities is particularly effective when trying to limit fraud cases.
- Accounting: companies' activities generate a large number of transactions, entries, movements, and ratio calculations: anomalies within such data might indicate that a fraud has been committed. In order to identify which data could be helpful in fraud detection, we have studied the structure of the Swiss SME chart of account (Plan comptable suisse PME; Sterchi et al., 2014)).

- Documents: this last category concerns all information originating from company documents such as bills, contracts, etc.

Exogenous red flags

Exogenous red flags, which are detectable through information originating from sources that are external to the company, have been classified in three categories.

- *Internal control and surveillance:* includes red flags connected with the company's relations with its auditors.
- *Environment and business sectors:* includes red flags connected with the conditions and the changes within companies' external environment (political, social, etc.), and with problems linked to companies' business sectors.
- *Third parties: business partners, suppliers, and service providers:* this category concerns people and organizations that do business with the assessed company, such as business partners, suppliers, and service providers. It includes red flags connected with their behaviors and business activities, as well as with eventual complaints, lawsuits, and denunciations.

3.2 Identifying publicly available information relating to Swiss companies

In order to determine which of the red flags included in our list could be detected using publicly available information, we first had to establish which information of this kind is available in our country. As a reminder, we define publicly available information as any data or information originating from public or private sources that is available to anyone, without restrictions, free of charge or otherwise. This concept must be differentiated from that of open data, which includes any "data and content that can be freely used, modified, and shared by anyone for any purpose" (opendefinition.org). We achieved this by analyzing the Swiss legal framework and conducting semi-structured interviews with investigation and financial investigation experts working for law enforcement agencies as well as for private entities.

3.2.1 The legal framework in Switzerland

Few laws, in Switzerland, establish the obligation to publish company information. With regard to financial information, the Swiss Code of Obligations (CO) sets forth that "Following their approval by the competent management body, the annual accounts and consolidated accounts together with the audit reports must either be published in the Swiss Official Gazette of Commerce or sent as an official copy to any person who requests the same within one year of their approval" (Art. 958e CO). Annual accounts include the balance sheet, the profit and loss account and the notes to the accounts (art. 958 al. 2 CO and 959ff. CO). Other laws establish special duties with regard to publication of information: these apply for example to listed companies, (see for example the Federal law on stock exchanges and the commerce of securities (Loi sur les bourses, RS 954.1), to establishments subject to the Federal Law on Banks (Loi sur les banques, RS 952.0) and to the Swiss National Bank (Loi sur la Banque nationale, RS 951.11).

According to researchers (e.g. Del Bosco & Misani ; 2011) as well as to human rights, environmental, and anti-corruption organizations, published extra-financial information represents an important asset in the context of fraud detection. However, there is no legislation related to such publishing, and the Swiss government shows no intention of taking steps in this direction (Rapport de droit comparé, 2014), like the European Union has recently done (Directive 2014/95/EU).

3.2.2 Classification

Having established the legal framework, we searched for possible sources of publicly available information related to Swiss companies. We have identified 352 types of information, which can be classified in five categories:

- *Official documents* (as defined by art. 5 and 6 of the Federal Act on Freedom of Information in the Administration (Freedom of Information Act, FoIA, RS 152.3), such as documents issued by public authorities (residents' registration offices, debt collection and insolvency offices, commercial registers, land registers, chancelleries, etc.);
- *Reports established by companies and services that provide business, economic, and solvency information*. Such information is made available to the public in various forms (reports, ad hoc reports, by telephone, automatically, etc.), free of charge or for a fee. Swiss law (art. 13.2 of the Federal Act on Data Protection, FADP, RS 235.1) states that it is legal to process personal data for the purpose of evaluating another person's creditworthiness, under the condition that such data “is neither sensitive personal data nor a personality profile”, and that it is “disclosed to third parties only if the data is required for the conclusion or the performance of a contract with the data subject”;
- *Directories* that provide unrestricted access to information on people and corporations that have a telephone subscription;
- *Internet, social media and blogs*: these sources can provide an enormous amount of useful (though not always reliable) information on people and companies;

- *Official company websites and other official documents* such as brochures, yearly reports, management reports, etc. These sources provide information about companies' profiles, their structure, sectors of activity, financial health, etc. Availability and quality of such information varies highly between companies.

3.2.3 Determining which red flags can be detected using publicly available information

We have placed the 403 red flags in three categories, depending on the level of accessibility of the information that can lead to their detection: 1) Red flag detectable through private internal information; 2) Red flags detectable through publicly accessible internal information, 3) Red flags detectable through publicly accessible information. The majority of red flags have been, as expected, classified in the first category. We have however identified a satisfying numbers of red flags (67) that depend on publicly accessible information. We have then cross-referenced the latter with our publicly available information index, and determined that 43 red flags can be, in theory, detected by using exclusively such data (e.g. profits that are systematically lower than the business sector average, information that diverge from the financial performance, and presence of shell companies).

3.3.4 Testing

This phase of the project is currently in progress. We have conducted a preliminary test, which consisted in assessing the risk of fraud within a Swiss organization suspected of widespread corruption practices using the 43 red flags discussed above. Further, intensive tests will be conducted in 2015-16 by students of ILCE's Master of Advanced Studies in Economic Crime Investigation (MAS ECI), as well as by several Swiss experts and entrepreneurs, in order to determine to witch extent the results generated by its application can be considered accurate and reliable.

4. Results and discussion

The main output of the project consists in two unique red flag databases. The first includes our 403 hand-picked red flags pertaining to occupational fraud. It is available in two formats: a protected Excel spreadsheet, complete with filters that allow to quickly access the desired information, and a simplified printed version. This database has the potential of empowering any person having access to internal and/or external information regarding a company to rapidly foresee or detect and prevent potential fraud situations. Experts who have already been given access to the database agree that a tool grouping reliable occupational fraud red flags in one place is a highly valuable asset; they also lauded its flexibility and potential for customization, which will allow professionals to adapt it to their needs and to the situations they wish to analyze. They believe that the database will prove useful at an internal level (in particular to audit committees, internal auditors, management, risk committees, compliance bodies, ICS surveillance bodies, quality control bodies, and process managers), but also state that third parties (such as the business partners, competitors, and investors) could also benefit from its use. Finally, the experts suggest that the database could be used for education purposes, in the context of specialized training for professionals in the fight against economic crime.

The second database includes the 43 fraud red flags that could possibly be evaluated using only publicly available information. As mentioned above, these have been tested in the last phase of our project. While this first test has generated positive results, they are by no means conclusive. Further testing will take place in 2015-16. We will however not be able to corroborate our results with reliable statistical elements, as the latter are, at the moment, insufficient. Finally, the validation of several sources of information on which the red flags are based could prove to be problematic, because of the high volume of data, the lack of uniformity of such sources, and of the absence of evaluation standards in the field.

5. Conclusion

As of today, publicly available information cannot, by themselves, allow the detection of sufficient red flags to be considered a reliable source for the assessment of fraud risk within Swiss companies. This due to the legal framework in Switzerland and to the fact that most financial information, on which many proven red flags depend, is kept private. Publicly available information does fulfil, however, an important function in the fight against fraud. While not permitting a complete assessment, it can in some cases provide a general, preliminary evaluation of a company, and can lead to the spotting of problems (or problem areas) that deserve further investigation. As such they can prove useful to people who have access to both private and public information as well as to people external to the company. Those in the first category can also combine the two sources in order to achieve a more complete and efficient red flag-based assessment.

Public available information has the potential to play an even bigger role in the context of fraud detection and prevention. Further research, in particular with regard to the reliability and quality of the data (source validation) and to the corroboration of the results with reliable statistical data, will be needed in order to determine under which conditions this potential could be exploited. The volume of publicly available information is constantly growing, thanks also to media platforms such as Twitter and Facebook - which are used by countless companies and organizations. The identification of potentially useful information within this ocean of data will be one of the main challenges for the future.

References

ACFE. 2014. Report to the nations on occupational fraud and abuse. http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

ACFE. 2012. Report to the nations on occupational fraud and abuse. http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf, October 28, 2015.

ACFE, & Peltier-Rivest, D. 2007. La détection des fraudes commises en entreprise au Canada: une étude de ses victimes et de ses malfaiteurs. http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-french-canadian.pdf, October 28, 2015.

American Institute of Certified Public Accountant (AICPA). 2002. Consideration of Fraud in a Financial Statement Audit. Statement on Auditing Standards No. 99. http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf, October 28, 2015, AICPA.

Ames, D., Brazel, J. F., Jones, K. L., Rich, J. S., & Zimbelman, M. F. 2012. Using Nonfinancial Measures to Improve Fraud Risk Assessments. Current Issues in Auditing, 6(1): C28–C34.

Bell, T. B., Peecher, M. E., Solomon, I., & KPMG International. 2005. The 21st century public company audit: conceptual elements of KPMG’s global audit methodology. [S.l.]: KPMG International.

Brazel, J. F., Jones, K. L., & Zimbelman, M. F. 2009. Using Nonfinancial Measures to Assess Fraud Risk. Journal of Accounting Research, 47(5): 1135–1166.

Brown, S. A., & DLA Piper LLP. 2012. Identification of “Red Flags” for possible violations of key US laws for companies operating overseas. Stranger in a Strange Land:

Ethical and Compliance Challenges in International Disputes. Presented at the ABA Section of Litigation 2012 Section Annual Conference, Miami, Florida, http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/12-1_identification_red_flags.authcheckdam.pdf, September 5, 2014.

Cauvin, E., & Bescos, P. 2005. Les déterminants du choix des indicateurs dans les tableaux de bord des entreprises françaises : une étude empirique. Finance Contrôle Stratégie, 8(1): 5–25.

Chapuis, B., Granito, D., Jaquier, S., & Lavanchy, P.-Y. 2016. Investigation comptable. Précis d'investigation financière. Lausanne: Presses polytechniques et universitaires romandes.

Cohen, J., Holder-Webb, L., Nath, L., & Wood, D. 2011. Retail Investors' Perceptions of the Decision-Usefulness of Economic Performance, Governance, and Corporate Social Responsibility Disclosures. Behavioral Research in Accounting, 23(1): 109–129.

Cohen, J. R., Krishnamoorthy, G., & Wright, A. M. 2000. Evidence on the effect of financial and nonfinancial trends on analytical review. Auditing, 19(1): 27–48.

Colby, E. 2004a. La fraude et le contrôle interne, Première partie : l'importance des contrôles. https://www.cga-pdnet.org/Non_VerifiableProducts/ArticlePublication/FraudInternalControls_F/FraudInternalControls_p1_F.pdf, August 5, 2014.

Colby, E. 2004b. La fraude et le contrôle interne, Deuxième partie : concevoir des contrôles pour enrayer les menaces. https://www.cga-pdnet.org/Non_VerifiableProducts/ArticlePublication/FraudInternalControls_F/FraudInternalControls_p2_F.pdf, August 5, 2014.

Colby, E. 2004c. La fraude et le contrôle interne, Troisième partie : les stratagèmes de fraude interne. https://www.cga-pdnet.org/Non_VerifiableProducts/ArticlePublication/FraudInternalControls_F/FraudInternalControls_p3_F.pdf, August 5, 2014.

COSO. 2013. http://www.cpa2biz.com/AST/PricingStructureAssortments/Section_Credentials/Pricing_Tax_Section_Member/PRDOVR~PC-990025/PC-990025.jsp?selectedFormat=Paperback, October 28, 2015.

Del Bosco, B., & Misani, N. 2011. Keeping the enemies close: The contribution of corporate social responsibility to reducing crime against the firm. Scandinavian Journal of Management, 27(1): 87–98.

DiNapoli, T. P. 2010. Red Flags for Fraud: 14. http://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf, August 5, 2014, State of New York, Office of the State Comptroller.

Directive 2014/95/EU of the European Parliament And of the Council of 22 October 2014, amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups.

Gallet, O. 2010. Halte aux fraudes, Guide pour auditeurs et dirigeants. Paris: Dunod.

Golden, T. W., Skalak, S. L., Clayton, M. M., & Pill, J. S. 2011. A guide to forensic accounting investigation (2nd ed.). Hoboken, NJ: Wiley.

Isenring, G. L., Mugellini, G., & Killias, M. 2013. Survey to assess the level and impact of crimes against businesses in Switzerland. http://www.unisg.ch/~/media/internet/content/dateien/unisg/schools/ls/lehrstuhl%20killias/final%20report_swiss%20business%20crime%20survey_2013.pdf, August 5, 2014, University of Zurich.

Ittner, C. D., & Larcker, D. F. 1998. Are Nonfinancial Measures Leading Indicators of Financial Performance? An Analysis of Customer Satisfaction. Journal of Accounting Research, 36: 1–35.

KPMG. 2009. Enquête sur la criminalité économique 2009, Global Economic Crime Survey. https://www.pwc.ch/user_content/editor/files/publ_adv/pwc_global_economic_crime_survey_09_ch_f.pdf, August 5, 2014.

KPMG. 2012a. Audit Committee Institute, Outil 11: indicateurs d'alerte. https://www.kpmg.com/FR/fr/AuditCommitteeInstitute/Documents/Fiches_Outils_ACI_11.pdf, August 5, 2014.

KPMG. 2012b. La fraude dans le processus d'approvisionnement. http://www.kpmg.com/ca/fr/topics/at-risk-magazine/pages/procurement-fraud-are-you-prepared.aspx, August 5, 2014.

KPMG. 2013a. Wirtschaftskriminalität: Deutschland, Österreich, Schweiz im Vergleich. http://www.kpmg.com/CH/de/Library/Articles-Publications/Documents/Advisory/ch-pub-20130313-wirtschaftskriminalitaet-de.pdf, October 28, 2015.

KPMG. 2013b. Astrus insights. KPMG's analysis of third-party integrity risks. https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/astrus-insights.pdf, October 28, 2015.

Mauléon, F. 2007. La communication extra financière comme nouvelle forme de l'éthique de l'entreprise. http://quoniam.info/competitive-intelligence/PDF/PhDs_Guidance/PhD_Fabrice_Mauleon.pdf

Ouaniche, M. 2009. La fraude en entreprise : Comment la prévenir, la détecter, la combattre. Paris: Maxima.

Peter, H., & Jaquemet, G., 2014. Corporate Social Responsibility, Analyse des rapports 2013 des dix plus grandes sociétés du SMI. L'Expert-Comptable suisse, 2014|11: 1027-1037.

Pons, N. 2006. Cols blancs et mains sales. Economie criminelle, mode d'emploi. Paris: Odile Jacob.

Pons, N., & Berche, V. 2009. Arnaques: le manuel anti-fraude. Paris: CNRS.

PwC. 2011a. Cybercrime in the spotlight, Swiss Economic Crime Survey 2011. http://www.pwc.ch/user_content/editor/files/publ_adv/pwc_global_economic_crime_survey_11_CH_e.pdf, August 5, 2014.

PwC. 2011b. La fraude en entreprise : tendances et risques émergents, 6e édition Global Economic Crime Survey 2011. https://form.pwc.fr/dev/formulaire_pwc_publication/formulaire_pwc_publication_1.0.0/index.php?id=3932, August 5, 2014.

PwC. 2014a. Economic crime: A threat to business globally, Global Economic Crime Survey 2014. https://www.pwc.com/gx/en/economic-crime-survey/downloads.jhtml, July 28, 2014.

PWC. 2014b. La fraude continue à être une vraie menace pour les entreprises. http://www.pwc.fr//assets/files/pdf/2014/02/pwc_etude_fraude2014_fr.pdf

Rapport de droit comparé. Mécanismes de diligence en matière de droits de l'homme et d'environnement en rapport avec les activités d'entreprises suisses à l'étranger. Rapport rédigé en exécution du postulat 12.3980. 2 mai 2014. http://www.ejpd.admin.ch/content/dam/data/bj/aktuell/news/2014/2014-05-28/ber-apk-nr-f.pdf, October 29, 2015.

Singleton, T. W., & Singleton, A. J. 2006. Fraud auditing and forensic accounting (3rd ed.). Hoboken, NJ: Wiley.

Sterchi, W., Mattle, H., & Helbling, M. 2014. Plan comptable suisse PME. Lausanne: LEP, Loisirs et Mont-sur-Lausanne.

Zimbelman, M. F., & Albrecht, C. C. 2011. Forensic accounting (4th ed., International ed.). Mason, OH, etc.: South-Western/Cengage Learning.