IT-based Fraud Management Approaches in Small and Medium Enterprises – A Multivocal Literature Review

Michaela Karin Trierweiler
Johannes Kepler University, Austria, MKT.JKU@gmail.com

IT-based Fraud Management Approaches in Small and Medium Enterprises – A Multivocal Literature Review

Michaela K. Trierweiler[1]

[1] Johannes Kepler University, Department of Information Engineering, Linz, Austria
mkt.jku@gmail.com

Abstract. Fraud, particularly cybercrime, is an emerging worldwide risk. Despite this, the risk of fraud appears underestimated in discussions of fraud mitigation and risk management in the context of SMEs. This multivocal literature review discusses ways of minimizing fraud for SMEs and IT-supported concepts that are currently proposed in literature. The present review shows that existing concepts often focus on specific or internal fraud risks and organizational countermeasures, but rarely cover newer fraud risks or suggest IT-supported measures to reduce the risk of fraud for SMEs. However, some IT security approaches have been proposed to mitigate fraud, but the area of internal control concepts of compliance and governance appears unconnected to IS approaches. This review identifies a lack of integrated fraud-management concepts, which is surprising due to the omnipresence of ICT, it found limitations in existing concepts and suggests areas for future IS research and academic discussion.

Keywords: fraud management, framework, SME, IT security, literature review.

1 Introduction

The ACFE *Report to Nations* characterizes fraud as an existing and emerging risk to economies worldwide. Small and medium enterprises (SMEs) are considered the engine of many economies. In the European Union, nine out of 10 enterprises are SMEs, and these organizations generate two-thirds of all jobs [1]. SMEs drive innovation and are crucial for competitiveness and employment; for this reason, they are attractive targets for criminals [2–6]. ACFE statistics [4, 7, 8] show that small organizations (defined as organizations with fewer than 100 employees) are with approximately 30% the most common victims of fraud. Median losses of up to USD 200,000 indicates greater negative impacts for SMEs compared with larger companies [8]. SMEs tend to have fewer anti-fraud controls in place [9], leaving them more vulnerable to fraud. However, consultancy or audit service providers are conscious of fraud as business risks, particularly for big businesses. Accounting is arguably the best-protected area legally because it is a lucrative sector and, therefore, attracts risk.

In addition to accounting fraud other forms of occupational fraud include identity theft, bribery, asset misappropriation, and corruption [10],[11] exist. New forms of work collaboration, digitalization, and the use of more information and

17th International Conference on Wirtschaftsinformatik,
February 2022, Nürnberg, Germany

communications technology (ICT) tools present new forms of risk. In addition, the Covid-19 crisis has led to a shift to more but often quickly implemented ICTs in home-office environments, which often do not comply with corporate IT rules. This "shadow IT" makes it easier for fraudsters to attack [12],[13], and a significant increase in cyber fraud, payment fraud, or identity theft ("CxO-fraud") [14–18] is expected as fraudsters seize the opportunity to exploit the ongoing uncertainty and rapidly adapted work processes [12], [19]. Micro enterprises and SMEs [20] with flat organizational structures and combined functions in one head are particularly likely to lack internal controls [4] and a proper risk or fraud prevention, detection or response management.

Growing digitalization and the omnipresence of simple-looking IT tools, such as email programs, result in a reciprocal relationship between IT and fraud management. IT tools are considered vectors for fraud attacks [21] (e.g., email phishing attempts), though specific software, hardware tools, real-time and big data analytics [22], [23], and even AI [24] can help prevent or detect fraud. However, highly technological or ERP-based measures are rarely used in SME contexts. This invites the following questions: What technical measures for managing the emerging risk of fraud and cybercrime are suitable for SMEs? Are IT-supported concepts or frameworks in place? Further, what fraud types do they consider, and is cyber fraud one of them? What are the likely limitations?

The present study was designed as a multivocal literature review to follow an outcome perspective [25]: First, the current state of academic research was ascertained, and potential existing frameworks dedicated to fraud risk management for SMEs were identified. Second, this review verified the types of fraud risks these frameworks cover and examined potential limitations of these concepts.

In the following, this article provides an overview of existing fraud management principles, explains the methodological approach for the present study, presents and discusses the results, and concludes with ideas for future IS-related research.

2 State of the Field: Fraud Management Principles in Brief

In legal terms, fraud falls under the umbrella of white-collar crime. The main elements of fraud are intention, deception, and damage to another party in terms of financial loss (see for example §146 of the Austrian criminal law [26]). The types of activities classed as white-collar crime are extensive and include delicts that harm a company directly, such as paying a too high salary, as well as delicts that appear to benefit a company at first glance, such as corruption to gain a large profitable deal [27]. To differentiate the different kinds of fraud, in 2007, Joseph T. Wells developed a classification system for occupational fraud and abuse known as the "fraud tree" [10] and covers types of misconduct that can be committed by executives, managers, and employees [28]. This tree model has been refined over the years and is now considered a state-of-the-art definition concept. It splits fraud into three main types: corruption, asset misappropriation, and financial statement fraud (also known as accounting fraud). These types of fraud can all be summarized as non-compliance and engaging in undesired behavior that harms an organization [27] or individual.

In the literature, several concepts have been proposed in the context of discussions about the facilitators of fraud. Although a range of different fraud models has been developed in recent decades [29], the most widely accepted model follows Cressey's approach from the 1950s. Here, three critical elements must apply for fraud to take place: incentive/pressure, opportunity, and attitude/rationalization [28]. This approach, known as the "fraud triangle," was further developed by Wolfe and Hermanson [30] and supplemented with a fourth dimension and is now commonly known as the "fraud diamond." This added fourth dimension of capability, defined as intelligence, creativity, and experience [28], [30], can be interpreted in the sense of technical and computational skills and is relevant when considering cybercrime and IT-based fraud. In recent research [e.g., 31–35], a fifth dimension of arrogance and its impacts on fraud management have been discussed, leading to the "fraud pentagon" approach.

The interaction and relation of these dimensions indicate the complexity and interdisciplinary of fraud management. This complexity confirms the need for collaboration between different departments within enterprises and the need to use different types of mechanisms to establish effective working fraud-management systems [36]. Successful fraud management systems are a combination of people-related, technology-related, and organization-related measures in the sense of sociotechnical systems [37],[38]. A comprehensive fraud management concept combines measures for prevention (e.g., training, red-flags systems), detection (e.g. audit, monitoring, forensic), and response (e.g., reaction chains) and is embedded into the organization's overall governance and risk management framework [11],[39]. But all means must also be tailored to a company's risk, size, structure, and industry sector.

3 Methodological Approach – Multivocal Literature Review

In addition to classical mapping studies or structured literature reviews (LRs), other approaches to conducting scientific literature studies include both academic works and practitioners' views and could incorporate "grey literature". Synder [40] defined this as an "integrative LR," while Garousi et al. [41] termed such approaches "multivocal LRs." Both authors argued in favor of including different types of literature, particularly when the LR aims to provide an overview of existing knowledge on a broader topic, to critically review or potentially reconceptualize [40]. In situations where the subject is complex, and the formal literature output is small, it may be beneficial to combine insights and evidence from the industry and academic community [41]. All approaches to academic LRs plan and properly document the search process, define the search terms and databases (libraries), set clear including–excluding criteria for the selection of a source, and use a structured form to extract and compile data.

The present LR was performed in two stages as an iterative process with the intertwined activities of searching and reading literature [25]. This review started in June 2020 and applied the structured LR principles suggested by Kitchenham [42], Massaro et al. [43], and Fink [44], combining this with the use of strict search strings containing "fraud prevention | framework | SME" in three scientific databases (Compliance Digital, EBSCOhost, and SCOPUS) to identify peer-reviewed research

papers. As this initial search result delivered only five items, a second systematic search was performed in December 2020; here, the search strings were more generic, synonyms and free search were used, and additional databases (IEEE, ResearchGate, Academia) with snowballing and recommender searches were consulted. German- and English-language literatures were only included when they were in accordance with at least two of the three main search terms (fraud | framework | SME). After this second search, the LR still suggested a gap in the academic research on fraud-management frameworks for SMEs and revealed mostly case descriptive literature. Search strings shown in Table 1 generated 736 hits in total. These were narrowed down to 528 after keyword and title-reading and were further narrowed down to 65 after reading the abstracts. Of these 65 papers, five were unavailable, although the authors were contacted. The final selection of 33 scientific papers was made after a second round of abstract or cross reading of the articles to better understand their approaches.

Table 1. Scientific search engine yield and reason for selecting the database

Result items per database (total 33)		Reason for use of database	Overview of search strings and terms
Compliance Digital (German)	2	nearest to research field	• (Betrug*) AND (Rahmenwerk) AND (KMU)
EBSCO (Meta Search)	9	high academic, peer reviewed	• 'Fraud Prevention' AND (sme OR 'small and medium sized enterprises') • fraud AND (framework OR model OR theory) AND (SMEs OR 'small and medium sized enterprises') • 'nist cybersecurity framework' AND ('SMEs' OR 'small and medium sized enterprises' OR 'small businesses' OR 'small companies)
SCOPUS (Meta Search)	10	high academic, peer reviewed	• *Same terms as in EBSCO*
Research Gate (Meta Search)	9	recommendation search	• fraud AND (SME OR 'small and medium sized enterprises' OR 'small businesses' OR 'small companies')
Academia (Meta Search)	2	recommendation search	• *Free Search only*
IEEE	1	relevant for IS research	• fraud AND (SME OR 'small and medium sized enterprises' OR 'small businesses' OR 'small companies')

Garousi et al. [41] found that numerous practitioner sources have been ignored in IS research projects and argued that the lack of such information can have a significant impact on steering the research direction. In this sense, the simple question of whether literature on fraud-fighting frameworks for SMEs exists or not was too narrow-minded. A broader perspective was needed to be able to integrate different dimensions of classical (i.e., organizational) and newer (i.e., technical-based) fraud-management concepts to serve as a base for future academic discussions and research. Therefore, 28 additional sources - mainly textbooks, reports with practitioners' views or concepts

from related areas of fraud forensics or governance, risk and compliance (GRC) - were considered. These sources were found by free or recommender searches or coming from own previous research.

Sixty-one items were evaluated until June 2021, and Excel spreadsheets were used as the LR protocol to document the performed steps and log decisions for inclusion or exclusion. This helped maintain oversight via an index system of how and where each source was found and in assessing each item for extracting data. All 61 sources were assessed following Garousi et al.'s [41] guidelines. To ensure quality and rigor, published journal papers, conference proceedings, and textbooks from graduated publishing houses were classified as "white literature," ending in 50 items. The other 11 items, classed as "grey literature," were subsequently classified, and grey-literature sources were ranked according to their authority and credibility: eight were from academic researchers, and three were attributed to well-established business or trade associations. The latter were selected on the basis that they contained relevant domain knowledge on fraud management in certain contexts [Guideline 6+9+10].

Table 2 shows the statistical count after this assessment. Seven items were subsequently excluded for quality reasons [Guideline 11]: three papers were excluded due to poor methodology and weak empirical base, one journal article from 2001 was considered too old, two publications were doublets based on the same research and hence lacked novelty, and one of the grey literature items was excluded due to missing contribution to the present research.

Table 2. Statistical count of sample, exclusions, and grey literature

	No. of Sources	Excluded	Final	Grey
Books	22	0	22	1
Journals and conference papers	29	6	23	0
Thesis/scholarly work	7	1	6	6
Other (e.g., reports)	3	0	3	3
Total	61	7	54	10

The final literature sample consisted of 54 items from the years 2003 to 2021 and included 10 items identified as grey-literature sources. All items were indexed by type and a counter (e.g., B-001, J-001) and were screened and classified according to the following criteria:

- Schematic allocation of relevant keywords: define scoping and relevance per source
- Geographic coverage: check transferability to the European economy
- Empirical method: decide about meaningfulness
- Qualifiers for content: e.g., discusses whether the source has a framework—if yes, which one, and is it related to IT?
- Classification of perceived usefulness for future IS research

4 Results of the Multivocal Literature Review

The results of this paper are based on a multivocal review of sources from the different areas of fraud management, compliance, risk management, auditing, and IT security.

4.1 Findings from the Literature Review

This section presents the results of the LR according to the sources' relevance (keyword ranking), geographic coverage, scientific methods, perceived usefulness for potential future IS research with some qualifiers of the content.

Schematic allocation of relevant keywords. The main search terms, "fraud | framework | SME," were used to ascertain how narrowly each source dealt with the question of fraud in SME contexts and whether they provided concrete guidelines, frameworks, or road books for risk management. Sources that incorporated all three terms were considered the most valuable for examining in depth, as shown in Section 4.2. The label "Other" in Table 3 was applied to literature covering only a specific aspect of fraud, such as the psychology of fraud, GRC, IT security, fraud detection with data-analytical approaches, or forensic accounting.

Table 3. Keyword allocation on type of source and reference

		Keyword ranking - classification and allocated sources				
Source Type	No. items	Fraud +SME +Framework	Fraud +SME	Fraud +Framework	GRC +SME	Other
Book	22	2:[9, 45]	0	7:[39, 46–51]	1:[52]	12:[28, 53–63]
Paper	23	3:[64–66]	12:[67–78]	1:[79]	3:[80–82]	4:[83–86]
Thesis	6	1:[87]	3:[88–90]	0	2:[91, 92]	0
Other	3	0	1:[4]	1:[93]	0	1:[94]
Total	54	6	16	9	6	17

This approach was chosen because fraud management as a broad and interdisciplinary area is related to enterprise risk management, audit, and compliance. Integrating these items could provide a comprehensive knowledge base. In total, 28 sources focused on the SME context. Only five of the 23 academic journals and conferences papers [64], [86], [65], [66], [79] were from IS-related conferences. The majority were published in the areas of accounting, general management, criminology, and other social sciences.

Geographical Reach. The geographical coverage was set according to what was stipulated in the source. As shown in Table 4, most sources were focused on North America (N.A.) and Australia economic situations, which suggests a need for adaptation to European requirements if the results are to be used for future research. If no country was mentioned, the code "generic" was applied.

Table 4. Geographical reach of sources

Regional Focus	Items	Fraud +SME +Framework	Fraud +SME	Fraud +Framework	GRC +SME	Other
Generic	21	1	3	4	2	11
N.A. + Australia	17	3	6	2	1	5
Europe	8	0	2	2	3	1
Asia	5	2	2	1	0	0
Africa	3	0	3	0	0	0
Total	54	6	16	9	6	17

Methodology used by authors. The scientific methods used were assessed according to the described methodology or when the method could be derived from the given explanations. As shown in Table 5, only four sources adopted a design science approach, which suggested a lack of concrete frameworks. The same was true of the seven paper-based compilations of LRs and content synthesis. In contrast, there was extensive descriptive research with 12 case-studies or use-case descriptions, 13 quantitative, and nine qualitative research designs. The quantitative analyses were often based on only a small number of valid answers (N ranges from 37 to 250). This low level of empirical evidence must be considered when using this research as a basis for further study.

Table 5. Scientific methods used to discuss fraud in SME contexts (multiple allocations)

Method used by author	Items	Fraud +SME +Framework	Fraud +SME	Fraud +Framework	GRC +SME	Other
Design science	4	3	0	0	1	0
Literature review	2	0	0	0	1	1
Content synthesis	5	1	2	0	0	2
Case study / use case	12	1	1	1	0	9
Quantitative	13	0	9	1	3	0
Qualitative	9	1	5	0	3	0
Expert knowledge	25	2	2	8	0	13
Total	70	8	19	10	8	25

Potential use in future IS research. Table 6 shows the perceived usefulness of a literature source in terms of future IS research projects that might aim to close the identified lack of suitable fraud management framework for SMEs. The coding was done while reading the papers fully or cross reading the books. Remarkable is that most papers related to “fraud + SME” used descriptive statistics in certain countries or industries but did not provide advice in terms of a holistic approach that included IT-supported fraud management measures. This makes these sources suitable to problem statements, introductions, and basic considerations about fraud management. This assumption also applies to those sources that dealt with fraud management in a generic

manner. However, these generic sources often contained concrete advice in the form of checklists, framework structures, suggested fraud prevention, detection, or response measures, or even showed use cases for a better understanding; here, it is striking that these sources came mostly from items labeled "other" and were not necessarily scientific papers, but for example training material.

Table 6. Perceived usefulness for potential use in future IS research (multiple allocations)

Usefulness	Items	Fraud +SME +Framework	Fraud +SME	Fraud +Framework	GRC +SME	Other
Fraud management	22	3	9	4	0	6
Introduction	37	3	15	5	5	9
Contains checklists	15	3	3	6	1	2
Framework structure	14	4	1	5	2	2
Framework content	33	4	9	8	2	10
MTO dimension	22	2	5	4	2	9
Other	24	2	4	3	3	12
Total	167	21	46	35	15	50

Qualifiers for Content. To obtain a better understanding of the areas of focus, the sources were coded whether they suggested frameworks, provided some guidelines, discussed fraud types, proposed countermeasures, or covered specific industries, as well as how they used IT or analytical approaches. Most papers related to "fraud and SME" used descriptive statistics to examine fraud in certain countries or business areas but did not provide a prevention or detection approach. Only seven items [47, 61, 64, 82, 86, 91, 92] considered aspects of IS or IT security. More than half of all sources dealt with a particular fraud risk (and 13 of these had an accounting focus). The concentration on accounting fraud or other internal-fraud types, such as payroll fraud or employee fraud [45, 70–73, 75, 77, 78, 84], indicated a lack of research on handling certain fraud types, particularly IT- and cybersecurity-related ones, which are likely to take place from the outside. The concentration on specific industry sectors (banking [48], construction [79], healthcare [64], steel logistics [66], mobile-phone sector [73], and automotive [65]) also signaled a missing holistic or universal approach.

Use of Referenced Frameworks. Existing frameworks or concepts were used in 28 different sources of this sample as listed in Table 7: here, it was interesting to note whether the frameworks were used passively—meaning they were only mentioned in the introduction or theoretical section—or whether they were actively used as a base for defining the research questions, building design approaches, or define survey questions. The result shows there was a clear trend to refer to the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) "internal control framework" [95] in problem statements. Ten academic journals or thesis referenced the Fraud Triangle or Diamond in theory sections only. In contrast, IT security–related research, particularly items classified as grey literature, used the National Institute of

Standards and Technology (NIST) cybersecurity framework [96] for evaluation or to propose fraud-management measures.

Table 7. Referenced framework in publication (multiple allocations)

Framework	Passive use	Active use
A.B.C. Theory		[53]
CIA concept		[87]
CIMA Fraud Cycle	[51]	
COBIT	[64]	[86]
CORAS		[92]
COSO	[65], [74], [76], [78], [81], [63]	[45]
Ethics Barometer		[28]
Fraud Free Company		[9]
ISO norms		[59], [85]
MTO concept		[90]
NIST		[87], [92], [82], [91], [86]
Self-Control Theory	[68]	
SOX	[39]	
Triangle/Diamond	[83], [79], [71], [64], [72], [73], [65], [78], [89], [90]	

4.2 In-depth Analysis of Fraud-Management Frameworks in SME Contexts

When considering the six sources that included all three keywords ("fraud," "framework," "SME"), some remarkable differences were found between the approaches. In 2012, Lincke and Green [64] developed a web-based learning tool for teaching fraud management principles in the context of healthcare in a small practice environment. They provided six teaching case studies to familiarize students with concepts such as social engineering, codes of ethics, and designing information security. Although this approach is not a framework in a classical sense, it provides useful insights, and a transfer to other contexts is possible.

In contrast, Phuttima et al. (2014) [66] explored steel logistics fraud in Thailand, and Aris et al. (2013) [65] focused on procurement fraud in small and medium automotive firms in Malaysia. Therefore, these authors discussed fraud mitigation concepts in a very specific industry and under a specific set of circumstances that makes the transfer of these concepts to other industries or economic environments challenging.

Although Çalıyurt (2012) [9] followed a generic approach by defining three stages of fraud-free company levels and suggesting different measures in terms of organizational and corporate governance structures, the fraud-free company model concentrated mainly on reporting internal fraud, while no link to technical fraud risks was made. Dawson (2015) [45] used also a generic approach by providing recommendations and a roadbook for establishing an internal control and fraud-

prevention program for SMEs. The author focused on the use of the COSO internal control framework and did not consider technical measures or IT security–related risks, as he concentrated on employee fraud in the American economy.

Yearwood (2011) [87] developed the most general approach to reducing fraud risk in the SME context. The author suggested a conceptual framework that concentrates on a company's risk of fraud and protects this risk target by considering processes, technology, and organizational factors. The author also used concepts from IS, such as NIST, as well as the CIA principles of preserving confidentiality, integrity, and the availability of information.

All six approaches did not evaluate the proposed guidelines in practice or provide any other kind of proof of concept.

5 Discussion of the Results of the Literature Review

Looking in the "state of the field" fraud-management concepts that were discussed in Section 2, it is notable that concepts like the fraud diamond are on such an abstract level that they do not provide concrete advice and cannot serve as a roadbook or framework for SME practitioners wishing to establish a fraud risk–management system in their organization. An evaluation of other concepts was necessary.

The present study was designed as a multivocal review to answer questions like: What technical measures for managing the emerging risk of fraud and cybercrime are suitable for SMEs? Are IT-supported concepts or frameworks in place? Further, what fraud types do they consider, and is cyber fraud one of them? What are the likely limitations? Incorporating practitioners' views, as stipulated in textbooks, reports, and other examples of grey literature, allowed for different, interdisciplinary perceptions of fraud risk management to be compiled.

As shown in Table 4, many sources focused on Anglo-American economies, which suggests a need for adaptation to European requirements if the results are to be used for future research. To illustrate this, according to ACFE figures, cheque and payment tampering [4] is nearly four times more common in SMEs compared with large companies and represents 14% of fraud schemes in the U.S. and Canada. However, cheque tampering is less likely to occur in Western Europe because cheques are now rarely used as a payment method. Practitioners' works that contained anecdotal descriptions or practical use cases provide insights and serve as an entry point to the area of fraud risk management (see Table 6). Along with the scientific literature, such sources can serve as a foundation for future IS research, like design science research projects that aim to identify IT solutions for fraud as an emerging risk. Another example for the need of a careful transfer of results are those sources concentrating on employee fraud: they often suggest conducting background checks on employees to figure out whether they were living beyond their means or could be prone to unethical behavior. This is critical in terms of European regulations for employee protection and the GDPR standard. However, use cases or analyses of case studies can yield ideas for fraud-protection measures in certain contexts. Prenzler [84], for example, analyzed 19 real-

world projects and identified successful measures based on diagnostics about the opportunity factors in fraud and victims' characteristics.

A gap in the scientific research for SME-tailored fraud risk–management concepts could be derived from Tables 3 and 5. They show that little academic research has been conducted on fraud-management concepts and frameworks in the SME context. This outcome is in line with the results of a previous structured LR conducted by Behringer et al. [80], who examined the academic literature on compliance and corruption in family-owned companies. They found that only one-third of all articles reviewed came from VHB-ranked journals and focused mainly on comparing companies that adopted corporate governance rules with companies lacking such compliance structures.

The lack of a holistic approach and the failure to consider newer fraud risks, such as cybercrime**,** is visible by the many sources that just concentrated on describing fraud situations in certain industries or countries or because they made only suggestions for internal control mechanisms for fraud management in particular SME contexts. In many cases, research in this area did not relate to IS or consider fraud risk a problem for enterprises with an ICT landscape embedded within a sociotechnical environment. This finding is illuminated by considering the referenced frameworks (see Table 7): there was a clear either-or in favor of using classical organizational control frameworks like COSO or IT-supported frameworks, such as NIST. Only seven items at all considered IT-security aspects; this could be interpreted as a missing bridge between the wide area of IT security and fraud mitigation as a compliance risk. Both fields appear to coexist but are not integrated, although some transferable information seems promising. For instance, the IT governance framework COBIT-2019 allows different perspectives and focus areas, of which one is related to SMEs [97]. The NIST Cybersecurity Framework allows SME specific security approaches [98] and the five stages of NIST cybersecurity framework (identify, protect, detect, respond, recover) [99] could be applied to fraud prevention measures, as well.

Opportunities and challenges for IT and IS regarding fraud mitigation arise by the low usage of such measures**.** According to the ACFE, in 2020, only 2% of occupational fraud was initially detected by IT controls [4], whereas with 43%, giving a hint on a suspicious case was the most common type of fraud detection. Unfortunately, the ACFE reports offer no explanation for the low detection rate of IT controls and the preference for behavioral detection. But a similar picture is given when comparing answers of different experts groups: Two interviewees from compliance departments of medium-sized enterprises who were surveyed during a previous research [90] argued that ethical behavior is more important, while an IT security specialist interviewed highlighted the efficacy of IT security in preventing fraud intrusion by phishing or hacking attacks within his company. However, existing approaches from SAP [23], analytical methods for detecting credit card fraud, and even simple anti-virus and malware-detection software show that information technology is already an active player in minimizing losses caused by fraud attacks. Remarkably, fraud attempts can be detected four times quicker using IT tools as an active detection measure [4]. This suggests that a greater focus should be placed on IT-related fraud controls because the effectivity and opportunity for avoiding financial losses appear high.

6 Conclusion

Only a limited number of scientific papers and sources reviewed in this study dealt with all three scope-criteria of "fraud, framework, and SME" which suggests a gap in scientific research. Most sources of the sample focused on internal control and organizational measures but did not offer comprehensive guidelines or pursue a generalized fraud management approach. In many cases, research in this area is neither related to IS research nor considered fraud risk as a problem for enterprises that have an ICT landscape embedded within a sociotechnical environment. The sources rarely covered newer fraud risks or suggested concrete IT-support measures to reduce fraud.

One limitation of the present study is that this LR was not conducted as a team. This made additional efforts necessary in the form of several iterations when classifying the sources to reduce bias. Second, the question regarding existing technical measures for managing the emerging risk of fraud and cybercrime could not be answered based on the sources reviewed in this LR. A different research setup would be necessary to answer this topic.

This study identified the following limitations in existing fraud-management approaches in the selected sample, which could represent areas for future research:

- Fraud-management concepts, like the fraud-diamond, are not suitable as road book for practitioners, they are abstract and offer too little concrete advice and measures.
- There is a focus on employee fraud and a lack of representation of newer fraud types, such as cyber fraud committed by external parties.
- The quantitative research studies conducted by academic researchers were often based on only a small number of valid answers; this likely low level of empirical evidence must be considered when extrapolating these results.
- The specific geographical or regional context of a research must be considered before transferring the findings to other areas.
- Most academic papers related to fraud and SMEs used descriptive statistics to discuss fraud in certain countries or business areas but did not offer a holistic prevention approach, including IT-supported management measures.
- Only seven items considered IT-security aspects, which could be interpreted as a gap in the research between the wide area of IT security and fraud management.

Although, the negative impact of the Covid-19 crises was already notified by some reports, the focus of this paper was not to discuss these effects on the fraud risk situation. Nevertheless, this could open another interesting area for IS research. The present review aimed to provide an overview of existing fraud-management concepts focused on the specific needs of SMEs to serve as a foundation for future academic discussion. Existing internal control-based fraud-mitigation concepts should be combined with IT-supported approaches and incorporated into future research to draw a link between IT security and conventional fraud prevention, detection, and response measures for SMEs. These areas appear unconnected and are yet to be integrated into a holistic fraud-management approach, which meet the challenges of the omnipresence of ICT and the steady increase in fraud related to cybersecurity breaches.

References

1. European Commission: User guide to the SME Definition. Publications Office of the European Union, Luxembourg (2020).
2. Kempf, D.: Ohne Schutzschild, (2015).
3. Ponemon: 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB). Ponemon Institute LLC (2017).
4. ACFE: Report to the Nations - 2020 Global Fraud Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners Inc., Austin - Texas - USA (2020).
5. Barth, M., Hellemann, N., Kob, T., Krösmann, C., Morgenstern, U., Tschersich, T., Ritter, T., Shulman, H., Trapp, D., Wintergerst, R.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt. Bitkom e.V., Berlin (2020).
6. Ernst & Young Fraud Investigation & Dispute Services: Global Forensic Data Analytics Survey 2018: How can you disrupt risk in an era of digital transformation? (2018).
7. ACFE: Report to the Nations on Occupational Fraud and Abuse - 2016 Global Fraud Study. Association of Certified Fraud Examiners, Austin - Texas - USA (2016).
8. ACFE: Report to the Nations - 2018 Global Fraud Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners, Austin - Texas - USA (2018).
9. Çalıyurt, K.T.: Reporting Fraud Using the Fraud-Free Company Model: A Case for the SMEs in Emerging Economies? In: Çaliyurt, K. and Idowu, S.O. (eds.) Emerging Fraud. pp. 3–18. Springer Berlin Heidelberg, Berlin, Heidelberg (2012).
10. Association of Certified Fraud Examiners: The Fraud Tree - occupational fraud and abuse classification systems, https://www.acfe.com/rttn2016/images/fraud-tree.jpg, last accessed 2019/03/07.
11. Girgenti, R.H., Hedley, T.P. eds: Managing the risk of fraud and misconduct: meeting the challenges of a global regulated, and digital environment. McGraw-Hill, New York (2011).
12. Schöber, P., Schmitz, P.: Hochkonjunktur für die Schatten-IT, https://www.it-business.de/hochkonjunktur-fuer-die-schatten-it-a-973554, last accessed 2020/10/23.
13. Schuster, H.: Schatten-IT im Homeoffice gefährdet Unternehmens-IT, https://www.it-business.de/schatten-it-im-homeoffice-gefaehrdet-unternehmens-it-a-1010689, last accessed 2021/03/29.
14. ACFE: Fraud in the Wake of COVID-19: Benchmarking Report, https://www.acfe.com/covidreport.aspx, last accessed 2020/06/18.
15. ACFE: Fraud in the Wake of COVID-19: Benchmarking Report December Edition, https://www.acfe.com/covidreport.aspx, last accessed 2021/03/14.
16. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N.: Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies. 1–13 (2020). https://doi.org/10.1080/14616696.2020.1804973.
17. Deloitte Poland: The impact of COVID-19 on the fraud risks faced by organisations, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl_COVID_19_Fraud%20Risks_EN_newApril2020.pdf, (2020).
18. Pasculli, L.: COVID19-related fraud risks and possible anti-fraud measures (Written evidence submitted to the Treasury Committee on the Economic Impact of Coronavirus). Coventry University (2020).

19. Al-Khalidi, B.: Remote Workforce Security Survey shows the human problems behind cybersecurity, https://www.axiad.com/blog/remote-work-report, last accessed 2021/08/11.
20. European Commission: SME definition, https://ec.europa.eu/growth/smes/sme-definition_en, last accessed 2021/02/12.
21. KPMG: Global profiles of the fraudster: Technology enables and weak controls fuel the fraud. KPMG international (2016).
22. Holzenthal, F.: IT-gestützte Geldwäsche- und Betrugsbekämpfung in Banken und Versicherungen Mehrwert durch einen holistischen GRC-Ansatz. ZRFC. 3/14, 140–143 (2014).
23. Derksen, O.: Fraud Analyse von Massendaten in Echtzeit. In: Deggendorfer Forum zur digitalen Datenanalyse (ed.) Big Data - Systeme und Prüfung. pp. 45–59. Schmidt, Berlin (2013).
24. Spindler, M., Kögel, H.: Erkennung von Versicherungsbetrug mit künstlicher Intelligenz. Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Berlin (2020).
25. vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. CAIS. 37, (2015). https://doi.org/10.17705/1CAIS.03709.
26. jusline.at: § 146 StGB (Strafgesetzbuch), Betrug - JUSLINE Österreich, https://www.jusline.at/gesetz/stgb/paragraf/146, last accessed 2019/03/07.
27. Heißner, S.: Täter und Delikte. In: Erfolgsfaktor Integrität. pp. 37–70. Springer Fachmedien Wiesbaden, Wiesbaden (2014). https://doi.org/10.1007/978-3-658-05608-7_2.
28. Henselmann, K., Hofmann, S.: Accounting fraud: case studies and practical implications. Erich Schmidt, Berlin (2010).
29. Marks, J.: Fraud Pentagon - Enhancements to the Three Conditions Under Which Fraud May Occur, https://boardandfraud.com/2020/05/21/fraud-pentagon-enhancements-to-the-fraud-triangle-and-under-which-fraud-may-occur/, last accessed 2021/01/05.
30. Wolfe, D.T., Hermanson, D.R.: The Fraud Diamond: Considering the Four Elements of Fraud. CPA Journal. 74.12, 38–42 (2004).
31. Christian, N., Basri, Y.Z., Arafah, W.: Analysis of Fraud Triangle, Fraud Diamond and Fraud Pentagon Theory to Detecting Corporate Fraud in Indonesia. The International Journal of Business Management and Technology. 3, 73–78 (2019).
32. Fuad, K., Lestari, A.B., Handayani, R.T.: Fraud Pentagon as a Measurement Tool for Detecting Financial Statements Fraud. In: Proceedings of the 17th International Symposium on Management (INSYMA 2020). Atlantis Press, Vung Tau City, Vietnam (2020). https://doi.org/10.2991/aebmr.k.200127.017.
33. Maulidiana, S., Triandi, T.: Analysis of Fraudulent Financial Reporting Through the Fraud Pentagon Theory. In: Proceedings of the 2nd International Seminar on Business, Economics, Social Science and Technology (ISBEST 2019). Atlantis Press, South Tangerang, Indonesia (2020). https://doi.org/10.2991/aebmr.k.200522.042.
34. Muhsin, Kardoyo, Nurkhin, A.: What Determinants of Academic Fraud Behavior? From Fraud Triangle to Fraud Pentagon Perspective. KSS. 3, 154 (2018).

https://doi.org/10.18502/kss.v3i10.3126.
35. Nindito, M.: Financial Statement Fraud: Perspective of the Pentagon Fraud Model in Indonesia. Academy of Accounting and Financial Studies Journal. (2018).
36. Rupietta, W.: Datenanalysen als Erweiterung der Revisionsmethodik. ZIR. 06.15, 273–282 (2015).
37. Ulich, E.: Arbeitssysteme als Soziotechnische Systeme – eine Erinnerung. Journal Psychologie des Alltagshandelns. 6, (2013).
38. Bostrom, R.P., Gupta, S., Thomas, D.: A Meta-Theory for Understanding Information Systems Within Sociotechnical Systems. Journal of Management Information Systems. 26, 17–48 (2009). https://doi.org/10.2753/MIS0742-1222260102.
39. Hofmann, S.: Handbuch Anti-Fraud-Management: Bilanzbetrug erkennen - vorbeugen - bekämpfen. Erich Schmidt Verlag, Berlin (2009).
40. Snyder, H.: Literature review as a research methodology: An overview and guidelines. Journal of Business Research. 104, 333–339 (2019). https://doi.org/10.1016/j.jbusres.2019.07.039.
41. Garousi, V., Felderer, M., Mäntylä, M.V.: Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology. 106, 101–121 (2019).
42. Kitchenham, B.: Guidelines for performing systematic literature reviews in software engineering. EBSE, Technical Report (2007).
43. Massaro, M., Dumay, J., Guthrie, J.: On the shoulders of giants: undertaking a structured literature review in accounting. Accounting, Auditing & Accountability Journal. 29, 767–801 (2016). https://doi.org/10.1108/AAAJ-01-2015-1939.
44. Fink, A.: Conducting research literature reviews: from the internet to paper. Sage, Los Angeles (2020).
45. Dawson, S.: Internal control/anti-fraud program design for the small business: a guide for companies not subject to the Sarbanes-Oxley Act. Wiley, Hoboken (2015).
46. Biegelman, M.T., Bartow, J.T.: Executive roadmap to fraud prevention and internal control: creating a culture of compliance. Wiley, Hoboken, N.J (2012).
47. Baker, H.K., Saadi, S., Purda, L.: Corporate Fraud Exposed A Comprehensive and Holistic Approach. Emerald Publishing Limited, Bingley (2020).
48. Quedenfeld, R., Beuther, L., Ganguli, I., Mühlroth, U., Studer, M.: Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität. Erich Schmidt Verlag, Berlin (2017).
49. Vona, L.W.: Fraud risk assessment: building a fraud audit program. J. Wiley & Sons, Hoboken, NJ (2008).
50. Koletar, J.W.: Fraud exposed: what you don't know could cost your company millions. John Wiley & Sons, Hoboken, N.J (2003).
51. CIMA: Fraud risk management: a guide to good practice. CIMA, Chartered Institute of Management Accountants, London, UK (2009).
52. Montag, P.: Risikomanagement und Compliance im Mittelstand: Status quo und Erfolgsfaktoren der Implementierung. Erich Schmidt Verlag, Berlin (2016).
53. Ramamoorti, S., Morrison III, D.E., Koletar, J.W., Pope, K.R.: A.B.C.'s of behavioral forensics: applying psychology to financial fraud prevention and detection. Wiley, Hoboken, New Jersey (2013).

54. Dove, M.: The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable. Routledge, Abingdon, Oxon ; New York, NY (2021).
55. Baesens, B., Van Vlasselaer, V., Verbeke, W.: Fraud analytics using descriptive, predictive, and social network techniques: a guide to data science for fraud detection. Wiley, Hoboken, New Jersey (2015).
56. Gee, S.: Fraud and fraud detection: a data analytics approach. Wiley, Hoboken, New Jersey (2015).
57. Siegel, E.: Predictive analytics: the power to predict who will click, buy, lie, or die. Wiley, Hoboken, New Jersey (2016).
58. Finlay, S.: Predictive analytics, data mining and big data myths, misconceptions and methods. Palgrave Macmillan, Houndmills, Basingstoke, Hampshire (2014).
59. Gleißner, W., Romeike, F. eds: Praxishandbuch Risikomanagement: Konzepte - Methoden - Umsetzung. Erich Schmidt Verlag, Berlin (2015).
60. Silverstone, H., Sheetz, M.: Forensic accounting and fraud investigation for non-experts. Wiley, Hoboken, N.J (2007).
61. Singleton, T., Singleton, A.J.: Fraud auditing and forensic accounting. John Wiley & Sons, Hoboken, N.J (2010).
62. Kratcoski, P.C., Edelbacher, M. eds: Fraud and Corruption: Major Types, Prevention, and Control. Springer International Publishing, Cham (2018).
63. Bungartz, O.: Effiziente und effektive Interne Kontrollsysteme. In: Bassen, A. and Wagenhofer, A. (eds.) Controlling und Corporate-Governance-Anforderungen Verbindungen, Maßnahmen, Umsetzung. pp. 131–157. Erich Schmidt Verlag, Berlin (2010).
64. Lincke, S., Green, D.: Combating IS fraud: A teaching case study. In: AMCIS 2012 Proceedings. pp. 578–584. , Seattle, Washington (2012).
65. Aris, N.A., Arif, S.M.M., Othman, R., Chantrathevi, T., Tapsir, R.: Internal Control Mechanism Framework for Fraud Prevention in Small Medium Automotive Industry. In: 2013 IEEE Symposium on Humannities, Science and Engineering Research (SHUSER). pp. 594–598. , Malaysia (2013).
66. Phuttima, S., Rueangsirasak, W., Chaisricharoen, R.: Fraud Detection System for Steel Logistic SME Business on Cloud Services Model. In: The 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE). pp. 1–7. IEEE, Chiang Rai, Thailand (2014). https://doi.org/10.1109/JICTEE.2014.6804088.
67. Schaper, M.T., Weber, P.: UNDERSTANDING SMALL BUSINESS SCAMS. J. Enterprising Culture. 20, 333–356 (2012). https://doi.org/10.1142/S0218495812500148.
68. Geneste, L.A., Weber, P.C., Schaper, M.T.: SCAMS AND THEIR SMALL BUSINESS VICTIMS: PRELIMINARY FINDINGS FROM AN ONLINE SURVEY. Presented at the International Council for Small Business. World Conference Proceedings. , Washington, GWU School of Business June 1 (2012).
69. N'Guilla Sow, A., Basiruddin, R., Mohammad, J., Abdul Rasid, S.Z.: Fraud prevention in Malaysian small and medium enterprises (SMEs). Journal of Financial Crime. Vol. 25, 499–517 (2018). https://doi.org/10.1108/JFC-05-2017-0049.
70. Hess, M.F., Cottrell Jr., J.H.: Fraud risk management: A small business perspective. Business Horizons. 59, 13–18 (2016). https://doi.org/10.1016/j.bushor.2015.09.005.

71. Kramer, B.: Trust, but verify: fraud in small businesses. Jrnl of Small Bus Ente Dev. 22, 4–20 (2015). https://doi.org/10.1108/JSBED-08-2012-0097.
72. Andoh, C., Quaye, D., Akomea-Frimpong, I.: Impact of fraud on Ghanaian SMEs and coping mechanisms. JFC. 25, 400–418 (2018). https://doi.org/10.1108/JFC-05-2017-0050.
73. Yekini, K., Ohalehi, P., Oguchi, I., Abiola, J.: Workplace fraud and theft in SMEs: Evidence from the mobile telephone sector in Nigeria. JFC. 25, 969–983 (2018). https://doi.org/10.1108/JFC-03-2017-0025.
74. Mohd Danial Afiq Bin Khamar Tazilah, Norhusnaida Binti Che Hussain: The Importance of Internal Control in SMEs: Fraud Prevention & Detection. Presented at the International Conference on Business, Accounting, Finance, and Economics (BAFE 2015) , Malaysia October 9 (2015).
75. Agbaje, W.H., Igbekoyi, O.E.: Payroll Fraud and Profit Performance: An Assessment of Small and Medium Enterprises (SME's) in Nigeria. Research Journal of Finance and Accounting. 10 (2018).
76. Dimitrijević, D., Karapavlović, N., Milutinović, S.: Fraud prevention measures in Serbian small and medium-sized enterprises: Existence and effectiveness. Ekonomika preduzeća. 68, 369–382 (2020). https://doi.org/10.5937/EKOPRE2006369D.
77. Smith Stevenson, G., Hrncir, T., Metts, S.: Small Business Fraud and the Trusted Employee, (2013).
78. Lachney, K.: An Exploration of Internal Controls and Their Impact on Employee Fraud in Small Businesses. Journal of Forensic and Investigative Accounting. 12, 21–44 (2020).
79. Meiryani, Fitriani, A., Habib, Md.M.: Can Information Technology and Good Corporate Governance Be Used by Internal Control For Fraud Prevention? IJRTE. 8, 5556–5567 (2019). https://doi.org/10.35940/ijrte.C5503.098319.
80. Behringer, S., Ulrich, P., Barth, J., Unruh, A.: Compliance und Korruption in Familienunternehmen: Eine systematische Literaturanalyse. Journal "Risk, Fraud & Compliance." 65–72 (2019).
81. Cika, N.: An Analysis of Practices of Internal Controls in Small and Medium Enterprises in Albania. Journal of Accounting & Management (2284-9459). 7, 87–97 (2017).
82. Benz, M., Chatterjee, D.: Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons. 63, 531–540 (2020). https://doi.org/10.1016/j.bushor.2020.03.010.
83. Kranacher, M.-J., Morris, B.W., Pearson, T.A., Riley Jr, R.A.: A model curriculum for education in fraud and forensic accounting. Issues in Accounting Education. 23, 505–519 (2008).
84. Prenzler, T.: What works in fraud prevention: a review of real-world intervention projects. JCRPP. 6, 83–96 (2020). https://doi.org/10.1108/JCRPP-04-2019-0026.
85. Krause, L., Borens, D.: Strategisches Risikomanagement nach ISO 31000 – Teil 1. ZRFC. 180–186 (2009). https://doi.org/10.37307/j.1867-8394.2009.04.08.
86. Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., Ruhl, R.: The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches. In: 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing. pp. 734–741. IEEE, Amsterdam, Netherlands (2012). https://doi.org/10.1109/SocialCom-PASSAT.2012.109.
87. Yearwood, L.D.A.: A Conceptual Framework for the Prevention and Detection of

Occupational Fraud in Small Businesses, (2011).
88. Davis, M.V.: Strategies to Prevent and Detect Occupational Fraud in Small Retail Businesses, https://pdfs.semanticscholar.org/bea2/b0f8302e0345fb7e30a348b642cafc34e4d4.pdf, (2019).
89. Shao, S.: What are Some Best Practices for Internal Controls to Prevent Occupational Fraud in Small Businesses?, http://archives.pdx.edu/ds/psu/17410, (2016).
90. Trierweiler, M.K.: Evaluation the use of big data analytics to facilitate compliance and fraud prevention: an empirical study about usefulness and usage of big data analytics to prevent occupational fraud in German speaking companies, (2019).
91. Eilts, D.: An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses, https://nsuworks.nova.edu/gscis_etd/1106, (2020).
92. Koeze, R.: Designing a cyber risk assessment tool for Small to medium enterprises, (2017).
93. Dubis, G.S., Akresh, A.D., Jain, P., Morley, L., Phipps, T.M., Schmidt, R.A.: INTERNAL AUDITING AND FRAUD. The Institute of Internal Auditors (2009).
94. Lincke, S.: CIS 779 Information Systems Security, https://www.cs.uwp.edu/staff/lincke/infosec/, last accessed 2021/01/14.
95. The Committee of Sponsoring Organizations of the Treadway Commission: Welcome to COSO, https://www.coso.org/Pages/default.aspx, last accessed 2021/08/19.
96. Keller, N.: Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2020/06/19.
97. Andenmatten, M.: COBIT 2019 – Das neue Enterprise Governance Modell für Informationen und Technologien, https://blog.itil.org/2018/11/cobit-2019-das-neue-enterprise-governance-modell-fuer-informationen-und-technologien/, last accessed 2020/06/19.
98. Johnson, C.: Sizing Up the NIST Cybersecurity Framework, https://www.nist.gov/blogs/taking-measure/sizing-nist-cybersecurity-framework, last accessed 2020/06/19.
99. The MEP National Network: MANUFACTURERS GUIDE TO CYBERSECURITY - For Small and Medium-Sized Manufacturers. THE MEP NATIONAL NETWORK.