10-9-2023

Managing Cybersecurity and Other Fraud Risks in Small and Medium Enterprises – A Framework to Build a Fraud Management Program in Times of Digitalization

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

Barbara Krumay
Johannes Kepler University, Linz, Austria, barbara.krumay@jku.at

Managing Cybersecurity and Other Fraud Risks in Small and Medium Enterprises – A Framework to Build a Fraud Management Program in Times of Digitalization

Research Paper

Michaela K. Trierweiler[1], Barbara Krumay[1]

[1] Johannes Kepler University Linz – JKU Business School, Institute for Business Informatics - Information Engineering, Linz, Austria
mkt.jku@gmail.com; barbara.krumay@jku.at

Abstract. Fraud, particularly cybercrime, is an emerging worldwide risk that targets not only large but also small and medium enterprises (SME). SMEs are especially vulnerable because they often have limited resources in terms of money, staff, and IT knowledge. Because of the role SMEs play in the European economy, reducing their vulnerability has gained more importance. Therefore, this study considers the question of how to minimize fraud in SME-related digital and socio-technical work environments. Based on a design science research approach, we developed a fraud management framework to allow SMEs to identify individual fraud risks and establish an individual fraud management program based on the framework at hand. To be adaptable to different industries and sizes of SMEs, we propose a modular concept of documents and workshop material that includes occupational and cyber-fraud cases because previous fraud management concepts often handled only one of them.

Keywords: fraud management, framework, SME, IT security, GRC.

1 Introduction

Digitalization and digital transformation offer new opportunities for SMEs but also pose many challenges. Because 9 out of 10 enterprises in the European Union are SMEs -providing two-thirds of all jobs (European Commission, 2020)- they play an important role in the European economy (Lee et al., 2012; Li et al., 2016). Not only their importance and number but also their vulnerability make them lucrative targets for criminals (ACFE, 2020a; Barth et al., 2020; E&Y, 2018; Kempf, 2015; Ponemon, 2017). They were the most common victims of fraud (approx. 30%), suffering the highest financial losses and experiencing significant negative impacts compared to bigger companies (ACFE, 2020a, 2018, 2016). SMEs face specific occupational fraud risks (ACFE, 2018) but are also vulnerable to cyber-fraud (Ritchie, 2021). These risks evolve from the limited resources in terms of money, staff, and IT knowledge of SMEs. Fur-

18th International Conference on Wirtschaftsinformatik,
September 2023, Paderborn, Germany

ther, they are more likely to lack internal controls (ACFE, 2020a) and proper risk management, since they focus on operations but fail to invest into IT security staff or even staff trained in regulatory compliance (Asti, 2021). Fraud and cybersecurity breaches thus tend to go undetected in SMEs since identifying such events and formal documentation methods to report or learn are missing. Especially micro-SMEs (European Commission, 2016), having fewer than 10 employees, show a flat organizational structure and combine different functions in one role. This makes active fraud prevention, often requiring segregation of duties, difficult to establish. A compliant corporate culture is rarely established in a structured way. Fraudsters often target accounting, although it is a well-protected and legally regulated area. Besides this target, identity theft, bribery, asset misappropriation, and corruption are other common frauds (ACFE, 2022). Due to rapidly implemented information and communication technology (ICT) during the COVID-19 crisis, the number of threats even increased, as weaknesses in the implantation made attacks easier (Schöber and Schmitz, 2020). This situation led to a significant increase in cyber-fraud, payment fraud, or identity theft (ACFE, 2020b; Buil-Gil et al., 2020; Deloitte Poland, 2020; Pasculli, 2020). Risks also evolve from the use of shadow IT (Schuster, 2021), i.e., unregulated, and unsupervised ICT (Ritchie, 2021).

However, besides shadow IT, the increasing digitalization challenges companies. The omnipresence of widely used IT tools makes them vectors for fraud attacks (e.g., email phishing attempts). To detect and prevent from attacks and fraud, specific software and hardware tools enable real-time or big data analytics (Derksen, 2013; Holzenthal, 2014), and even AI (Spindler and Kögel, 2020) can be used. However, in SMEs, highly technological measures are rarely used, and IT-related fraud management measures are rarely discussed in SME contexts (Trierweiler, 2022). Current research focuses mainly on organizational measures without providing comprehensive guidelines. Research in this context is -to the best of our knowledge- neither related to information systems (IS) research nor considers cyber-fraud risk. However, the main source of risk and fraud is not the technology per se but the people handling it (Jeong et al., 2019). For example, phishing attacks happen often beyond technology and are connected to people's risk taking and decision making (Abroshan et al., 2021). Because companies operate in an ICT landscape embedded within a socio-technical business environment where people and technology work jointly, both must be considered.

Existing fraud management concepts, such as the BSI Grundschutz (BSI, 2022) or the NIST Cybersecurity Framework (NIST, 2013) are mainly addressing bigger companies. Even large auditing firms offer services targeted to bigger corporations. However, these approaches do not fit SMEs' situation because they rely on trained staff and established structures in a company. Since SMEs have lately become targets of attacks and fraud, concepts suited to the personnel resources, organizational situation, and technical possibilities of SMEs (Bada and Nurse, 2019) are necessary. This research aims to fill this gap by developing a fraud management framework (FMF) for SMEs that overcomes potential limitations (e.g., very complex to understand and handle; no holistic view). Therefore, we ask how a fraud management framework should look to fit into different SME contexts and cover company-specific fraud risks of occupational and cyber-fraud while considering given resources. To answer this question, a multivocal literature review was conducted (Trierweiler, 2022) to gain insights and build a

knowledge base for a better artifact (Peffers et al., 2007). We apply a design science research (DSR) approach to create an FMF as an ensemble artifact (Sein et al., 2011) that fits different SME contexts. The ensemble artifact is modular and combines documents (templates, such as FCM-03_FraudPolicyTemplate) and workshops (development and evaluation, such as FCM-02_CounterMeasureSelection&KPI) to support the creation of a fraud management program within a relatively short time frame of just a few months.

This research contributes to the existing field in two ways: first, it bridges epistemic research and applied sciences by creating a new artifact; second, this artifact supports practitioners in SMEs to minimize fraud risks in their individual contexts. This new approach uses the man-technology-organization (MTO) concept (Ulich, 2013), since current work situations are mainly socio-technical (Bostrom et al., 2009). Therefore, an effective fraud management system requires collaboration among technology (e.g., IT security aspects), organizational procedures (e.g., four-eyes principle), and workers (e.g., awareness training and ethical culture). Accordingly, the new framework shows characteristics like comprehensiveness, but also needs to be research-based, compatible with SMEs' fraud risk needs, and easy to understand. The last condition clearly influences the design and notation used to build the artifact. Our approach was piloted with an SME for evaluation as a proof of concept and to refine the design and details of the presented FMF in the sense of an action design research approach (Sein et al., 2011).

The remainder of this paper is structured as follows: Section 2 describes the state of the field regarding fraud management. Section 3 depicts the methodological approach, including the considerations for the real-world application of the artifact and the evaluation procedure. Section 4 explains the design considerations and components of the framework artifact, followed by an in-depth discussion related to the current literature. Finally, a conclusion, limitations, and future work are described.

2 State of Field

Compared to other criminal activities, fraud is often seen as a white-collar crime, i.e., a crime targeting financial or property loss (Braithwaite, 1985). White collar crime covers not only delicts directly harming an organization (e.g., asset misappropriation), but also crimes (e.g., corruption, money laundering) committed for the benefit of the company (Heißner, 2014). The main elements that constitute fraud are the harm done to a party resulting from action by another party (Bologna and Lindquist, 1995). So far, fraud has been mainly discussed from a legal point of view as well as in accounting and auditing literature. Legal entities define fraud based on characteristics such as intention, deception, and damage to a third party. For example, the European Parliament names Articles 310(6) and 325 of the Treaty on the Functioning of the European Union (Pouwels, 2022), the German criminal law in §263 and §263a (Bundesamt für Justiz, n.d.), Austrian criminal law §146 (jusline.at, 1975), to name just some legal foundations. Occupational fraud, i.e., fraud committed by an employee within the organization, covers three main categories: asset misappropriation (e.g., theft of cash, misuse of inventory), corruption (e.g., bribery, economic extortion), and financial statement fraud

(e.g., net income understatements) (ACFE, 2022). This scheme for occupational fraud, often referred to as the fraud tree (ACFE, 2022; Wells, 2001), addresses misconduct on different levels of an organization, from higher-level management to employees on the operational level (Henselmann and Hofmann, 2010). Overall, misconducts addressed in the fraud tree cover undesired and non-compliant behavior (Heißner, 2014).

Reasons for committing fraud are various, yet they follow a general scheme (Dorminey et al., 2012). The recently developed fraud models (Marks, 2020) are mainly based on the so-called fraud triangle (Cressey, 1952), a work done by Donald Cressy in the 1950s. In its very basic form, the fraud triangle addresses three conditions: pressure, opportunity, and attitude or rationalization (Kassem and Higson, 2012; Wells, 2014). Furthermore, it has been stated that fraud is related to the level of trust a person enjoys (Kassem and Higson, 2012). The fraud triangle, however, was the starting point for other fraud models, such as the fraud diamond, adding capability as the fourth dimension (Wolfe and Hermanson, 2004). Capability in this context includes the intelligence, creativity, and experience of the fraudster (Henselmann and Hofmann, 2010), which may also include technical and computational skills as preconditions to committing IT-based fraud. Lately, academic research has identified another dimension: arrogance (e.g., Christian et al., 2019; Fuad et al., 2020; Maulidiana and Triandi, 2020; Muhsin et al., 2018; Nindito, 2018), making the fraud pentagon.

Thus, the relevance of fraud management has gained some attention, especially in the financial management and auditing literature (e.g., Amasiatu and Shah, 2018; Cortesão et al., 2005; Soomro et al., 2019). Although research on fraud management focuses on schemes and frameworks, it also addresses the involved parties: fraud managers and offenders (Gill, 2011). It has been shown that fraud managers recognize changes in the way frauds are committed relative to technology (Gill, 2011), resulting in a "fraudogenic" environment (Button and Cross, 2017). Fraud management is widely based on the above-mentioned fraud models (i.e., fraud triangle, fraud diamond, fraud pentagon) to detect fraudulent activities (Indarto and Ghozali, 2016; Kassem and Higson, 2012; Roden et al., 2016; Umar et al., 2020).

However, fraud management extends beyond pure detection and encompasses prevention and response to fraud, including mitigation and remediation (Cappelli et al., 2012; Girgenti and Hedley, 2011). Fraud management frameworks exist at the governmental (e.g., U.S. Government Accountability Office, 2015) and organizational levels, e.g., the COSO framework (COSO, 2013). Existing fraud framework approaches related to SMEs mainly address occupational fraud but lack a clear position toward IT-related issues and do not adopt a holistic view (Trierweiler, 2022). Six lately analyzed approaches (Trierweiler, 2022) focus on employee fraud (Dawson, 2015; Yearwood, 2011), a specific industry (steel logistics in Thailand; Phuttima et al., 2014), or a business situation (internal controls for purchasing in the automotive sector in Malaysia; Aris et al., 2013). Or they focused on fraud reporting (Çalıyurt, 2012) and the development of a fraud policy (Lincke and Green, 2012). Common to all identified approaches is their conceptual nature, lacking evidence for applicability in the real world.

In addition, other disciplines offer frameworks that are transferable to fraud management, such as COBIT-2019 (ISACA, 2019) or the NIST Cybersecurity Framework (NIST, 2013). Both have been addressed in the context of SMEs (Andenmatten, 2018;

Asprion and Burda, 2019; Johnson, 2016; The MEP National Network, 2020) but with a different focus on security. An effective fraud management approach comprises measures for prevention, detection, and response (Girgenti and Hedley, 2011), which also apply to cybersecurity risks. Nowadays, IT security breaches and occupational fraud are intertwined: occupational fraud is often conducted within (e.g., changing a financial record) or via an information system (e.g., a phishing attack).

3 Methodology

The goal of this study is to develop a fraud management framework (FMF) for SMEs that overcomes potential limitations found in existing concepts. We adopt a DSR approach (Gregor and Hevner, 2013; Hevner et al., 2004; Iivari, 2015; Peffers et al., 2007) to develop an alternative FMF based on a recently published multivocal literature review identifying six SME-related fraud management approaches (Trierweiler, 2022). Because of the scarce IT-related measures in the academic literature, we used grey literature to fill the gap. Therefore, the research entry point related to an objective-centered solution (Peffers et al., 2007) relies on the idea of an existing knowledge base (Hevner, 2007). To safeguard consistency and integrate empirical sources, we further relied on domain-specific notation principles (e.g., Frank, 2013) for explanation and description as well as action design research (ADR) for evaluation (Maccani et al., 2015; Sein et al., 2011) and refinement of the framework. From a methodical perspective, incremental artifact evaluation with incremental delivery of features is also a characteristic of ADR (Haj-Bolouri et al., 2018; Sein et al., 2011). Therefore, this FMF artifact was developed using an agile sprint approach.

To achieve a proof-of-concept state, a naturalistic evaluation (Iivari and Venable, 2009) in a real-world SME was conducted, involving a second researcher creating and leading the feedback interviews to minimize bias. The piloting SME company has 10 employees with different levels of experience, from software developers to administrative staff. Security and fraud management are the responsibility of the CEO. The evaluation occurred from September until November 2022, involving the CEO of the company as well as people from the administrative staff to ensure validity, applicability (i.e., ease of use, understandability), and utility (e.g., Peffers et al., 2012; Prat et al., 2014). The pilot study was following the intended routine that a SME needs to apply to build its own fraud management program from this framework: The process starts with a briefing of the management and building a small ADR team of practitioners from the SME and the two researchers. To gain firsthand insights into the fraud management of the SME, a self-assessment questionnaire is filled out by SME management aiming at the identification of the fraud risk areas. Information from this self-assessment form is incorporated into a workshop with all SME project members to ensure the same knowledge base about fraud and the project in general. After this kickoff, a second workshop is conducted to perform the fraud risk analysis that is based on a comprehensive fraud glossary, consisting of over 120 fraud risks from different categories. At least the main areas of occupational and cyber-fraud need to be assessed by the SME. The results are then summarized and prepared for further use to define MTO-based fraud

countermeasures. Their definition is typically finalized in another workshop to be SME bespoke as possible. After this definition phase, the implementation in the SME's context is necessary, which can be completed as a workshop (our case) or as a pure planning activity. The stages and workshops are supported by different documents constituting the ensemble artifacts of the FMF at hand.

After each workshop sessions, expert interviews (Atteslander et al., 2010; Döring and Bortz, 2016) comprising 14 questions for aspects of utility (length, language, applicability, prerequisite of knowledge, needed time to work with), validity (scope and completeness perception), and efficacy (perceived impact and usefulness to the SME and to other SME contexts) were conducted to further evaluated the artefact. Answers were recorded and noted in form of a 5-point Likert scale (Brown, 2010). The analysis of the answers was used to refine the components of the FMF for SMEs. In total, 21 documents were evaluated, and 16 documents were applied by the piloting SME. This extended evaluation was applied to gain feedback as comprehensive as possible.

Because of the complex nature of the matter to be addressed by the DSR project (e.g., Venable et al., 2012), the development of the artifact was done in different design cycles (Sein et al., 2011; vom Brocke and Buddendick, 2006). An architectural construct (Trierweiler, 2021), which is a meta-artifact (Iivari, 2015) and developed in a first design cycle, was used to further design and build the content, sub-components, and their connections as well as the appropriate granularity of the information we show in this paper. This second design cycle was split into alpha and beta phases (see Sein et al., 2011) and connected to the evaluation as described above.

4 Results

Based on the DSR approach, we created an artifact that exists in two expressions: First, a meta-artifact, which comprises an architecture (Trierweiler, 2021). It holds five connected dimensions (called "tiers"), with processes and sub-processes on a generic level. Second, a generalized artifact was produced to address a class of problems (Wieringa, 2014). This artifact, further referred to as FMF for SMEs, contains self-explanatory information, template documents and workshop supporting material. However, it might require some external accompaniment and consultancy as well as project management and change management skills depending on the individual SME's knowledge.

4.1 Prerequisites and Design Considerations

Fraud prevention in an organization can best be achieved by having an effective and visible antifraud program (Vona, 2008) embedded in a corporate culture of ethical standards and the organization's governance and risk considerations. From the existing literature and based on the evaluation, we identified certain requirements and design considerations related to the SME context, i.e., scope and completeness; usability and handling; modularity; limitations of staff; cost efficiency; comprehensiveness; data protection and topic sensitivity. Table 1 represents some findings from the evaluation.

Table 1. Evaluation findings

Topic	Findings	Implications
FMF overall	Works well; positive evaluation results in general	Keep approach
Dual language	Applying German and English in the same document reduced the understandability	Split documents to single language
Modular concept	Worked well; SME could use only the relevant documents	Keep approach
Usage for different SME contexts	Documents are perceived to work universally; split into a golden-rule version and a more comprehensive one suggested	Rework and split document
Transfer/reusage FRA results into the next stages	Transfer of documents that are not directly connected made usage and transfer of results a bit cumbersome	Idea to support it by an IS in future
Sequencing of documents	During application, we found that they should be applied in another area (tier)	Move documents to correct tier
Redundancies, text length, style	Redundancies were spotted; repetition allows a document to stand independently; some explanations could be more to the point	Check and rework documents

We identified scope and completeness, referring to the extension of the scope beyond existing framework as well as achieving completeness of aspects as requirements. Many authors (e.g., Aris et al., 2013; Bungartz, 2010; Cika, 2017; Dawson, 2015; Dimitrijević et al., 2020; Lachney, 2020; Tazilah and Hussain, 2015), refer to existing models to address prerequisites and design, such as the COSO model. It describes the components of an antifraud program as a process consisting of the following steps (Vona, 2008): performing fraud risk assessments, building a control environment adverse to fraud, designing, and implementing fraud controls and countermeasures, sharing and training the fraud program, establishing monitoring activities, and responding to fraudulent activities. However, we identified the need to further extend the scope: from internal, staff-, and organizational-related controls responding mainly to classical occupational fraud risks (ACFE, 2022) to IT-related fraud situations, addressing current threats resulting from today's digital world and socio-technical work environments. In addition, the framework was further extended, integrating information about fraud incident response activities and possibilities to find additional support in case an SME lacks the knowledge in-house. Therefore, the FMF for SMEs considers more and different aspects of content than previous approaches. In the evaluation, two additional aspects were identified and added to the FMF for SMEs, resulting in the documents FCM-08_ConflictOfInterestForm, and FMF-02_DocumentsExplanation.

Furthermore, SMEs need a framework that is easy to use (usability) and does not require additional training (handling), allowing them to concentrate on the content. Therefore, the FMF for SMEs uses standard office products that are widespread and well-known. To address an international context, the framework allows a multi-language approach. However, based on the evaluation, the documents need to be separated

for not confusing the employees. To fit different sizes and industries of SMEs, a modular design (modularity) was identified as a design consideration. The FMF for SMEs compiles of best practices, domain knowledge, and additional information. It is organized in form of well-structured multiple documents. Drawing from the example of other frameworks (BSI, 2022; NIST, 2013), documents were indexed in relation to the main components. The documents can be used stand-alone or in combination according to the needs for building the SME specific fraud management program. The documents are either templates and forms, that are instantiated on use (e.g., in workshops) or information documents. The piloting SME, for example, did not instantiate a new IT security policy based on the proposed template (FCM-03), but used their existing one.

SMEs are clearly challenged by the number of people they employ. Role-based access to systems or segregation of duties, particularly in finance and accounting, therefore is hard to achieve. Consequently, not all fraud countermeasures, such as establishing a four-eyes principle when releasing money in an investment situation, are feasible. Since there is no clear-cut recommendation on measures, the FMF for SMEs considers workshops to discuss measures and build individual solutions. In the same manor, the limited financial resources of SMEs need to be considered. Accordingly, cost-efficiency of solutions is vital, making the use of existing tools (e.g., standard office products) more feasible rather than developing or buying a specific information system that also requires costly training.

SMEs have specific characteristics independent from the industry they operate in, but do not have the resources to implement different, industry-specific frameworks. Therefore, comprehensiveness as well as to encompass all risk areas is vital. Thus, a fraud glossary was compiled to build the baseline for the fraud risk analysis. It is used for the risk assessment and to contribute to the awareness for specific risks. It also influences subsequent documents of the framework.

Due to the need to protect internal data and the topic sensitivity, an SME might hesitate to integrate external players. To overcome these issues, documents in the FMF for SMEs foresee non-disclosure agreements. Internally, documents related to the fraud management program holding sensitive data need to be maintained and controlled in an archive within the SME with a confidentiality clause to safeguard data protection.

4.2 The FMF for SMEs

The FMF for SMEs (Figure 1) consists of five major interconnected components ("tiers"): Risk assessment (FRA), incident responses / forensics (FIR), fraud countermeasures (FCM), external support (FES), and implementation (FMFI). The FMF for SMEs addresses *risk assessment* to identify the individual fraud risk. It touches on *incident responses and forensics* because the need for risk management is often realized after an incident has occurred. The core part of the framework uses *fraud countermeasures* related to fraud types along the MTO concept (Ulich, 2013) to enable the selection of suitable measures. In addition, the proposed framework suggests where to find *external support* and suggests a roadmap for *implementation*. A *continuous improvement cycle* follows the implementation to keep the measures current. The framework provides a series of documents related to each tier, marked with an abbreviation for the tier (e.g.,

FRA) and a consecutive number. The documents are either templates, that need to be instantiated or hold necessary information. Workshops are directly related to some documents, as in the workshops these documents are used as the basis for instantiated documents (fitting the SME) or discussed to gain a common understanding. To reflect the process related to the FMF for SMEs, a sequence for use and run through is proposed in four stages (see section 4.3).

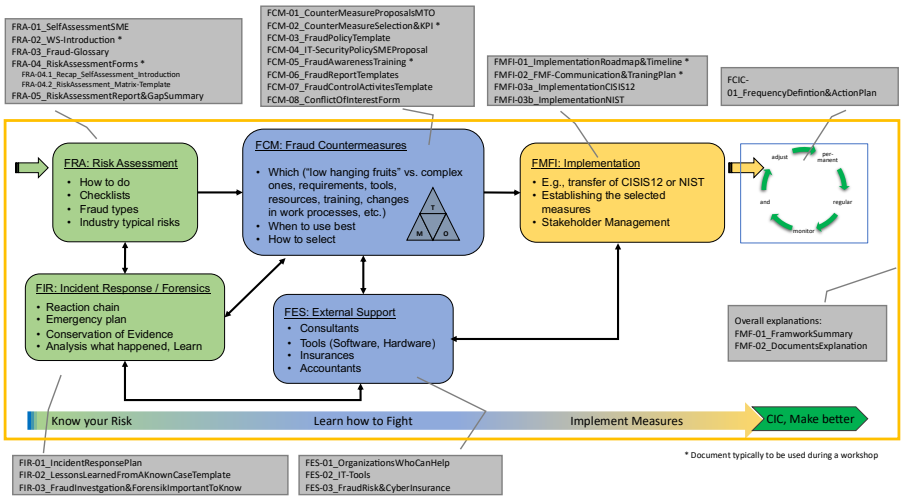

Figure 1. FMF for SMEs

4.3 Sequence of Use and Run Through

Although the FMF for SMEs is modular and offers the possibility to use the documents independently, they follow a process, based on a logical and chronological sequence. The sequence is divided in four stages: (1) know your risk, (2) learn how to fight, (3) implement measures, and (4) CIC, make better.

Stage 1: Know Your Risk. This stage allows to identify, learn about, and prioritize individual fraud risks. It includes a fraud risk self-assessment as well as workshops with relevant stakeholders to identify the risk, its impact, and prioritization, based on documents indexed with FRA (fraud risk assessment). If the need to create a fraud management program is caused by a recent incident, the assessment could also start by analyzing the incident based on documents indexed with FIR (incident responses / forensics).

Stage 2: Learn How to Fight. This second stage focuses on learning, i.e., how the fraud schemes are conducted, what are most common warning signals and what collusion strategies are. The SME shall understand what countermeasures could be suitable in the specific context, considering the SME's resources, balancing people (employee-related), technology, and organizational (processes) means. A workshop with relevant stakeholders of the SME is proposed to cover the learning process. Documents indexed with FCM (fraud countermeasures) support this stage. They provide support to capture

the decisions for certain measures, but also templates to create a fraud and an IT-security policy, forms to design internal controls and to establish a fraud reporting process. Depending on the SME's situation of resources and know-how, external tools or support might be required at this stage. Documents dealing with outside-resources and information like IT tools or cyber-security insurance to carry-over the burden, are indexed with FES (fraud external support).

Stage 3: Implement Measures. In the third stage the implementation of measures applies. Within the identified countermeasures, there might be quick wins, i.e., measures that could be installed easily without consuming significant time or money. Other measures might require more investigation or planning as well as some investments because other external resources, such as IT security experts or technical equipment or software must be paid. Considering this, a plan for implementation and a kind of rollout strategy that includes some budgeting must be developed. The FMF for SMEs proposes a training and communication plan. When an SME has no procedures for such change management or rollouts, this FMF offers implementation strategies derived from established IT security frameworks and adapted to fraud management needs; see documents indexed with FMFI (fraud management framework implementation).

Stage 4: CIC, Make better. Stage 4 calls for the establishment of continuous improvement cycle (indexed FCIC) of the implemented fraud management program. It is necessary to keep it current and to adapt it to organizational changes, new fraud schemes, and technological developments. Determining an appropriate frequency to reassess fraud risks and to adapt the countermeasures to the changed needs is proposed.

5 Discussion

The goal of this study was to develop a FMF for SMEs that overcomes potential limitations found in existing frameworks, such as non-comprehensiveness and lack of implementation in a real SME situation to proof applicability. Specific conditions found in SMEs (e.g., scarce financial and human resources; segregation of duties) hinder SMEs from using existing frameworks -such as COSO, COBIT, or NIST- that focus mainly on larger companies and often not directly on fraud management. In addition, fraud management seems to be successful only when it considers people, technology, and the organization. Therefore, in the FMF for SMEs, we combine measures targeting the specific SME aspects while integrating prevention, detection, and response tailored to an SME's needs. Following the man-technology-organization (MTO) concept (Ulich, 2013) in the FCM tier the sociotechnical nature is considered (Bostrom et al., 2009).

To mitigate fraud and cybersecurity risks, it is relevant to understand "why" to mitigate the risk by ensuring a good security and awareness program by building or verifying organic policies and procedures (Asti, 2021). To understand the "why" is part of the risk assessment and helps the SME to understand the individual fraud risks and how to prioritize them in accordance with given resources. The FMF for SMEs considers this point of "vulnerability management" (Ritchie, 2021) by starting with the tier of the

fraud risk assessment. What is different compared to other approaches is the comprehensive fraud glossary, fostering as the basis of the fraud risk assessment. The glossary incorporates different areas of fraud from which the SME can select during the assessment (occupational fraud, cyber-fraud, bid manipulation, and insurance fraud as well as other industry-specific areas). By evaluating these fraud areas, an SME can narrow the types of fraud; assess the impact in terms of reputation, financial loss, and business continuity; and prioritize. In addition, some summary documentation is needed to enable the SME to properly communicate the results of the fraud risk assessment within the organization. Although it seems obvious to start with a risk assessment, fraud management literature or conceptions often neglect this aspect; they assume that the fraud risk is known. However, research showed (Asti, 2021) that SMEs tend to be less aware of their risks. With respect to SMEs' limited resources, a fraud training program is a measure of low cost and effort and a "must-have" and should comprise all different kinds of identified fraud. Building a "human firewall" is a key element addressing cybersecurity (Jeong et al., 2019) even when an SME has no dedicated IT knowledge. The FMF at hand provides preset training material that can be tailored with guidance to an SME situation. To complete the understanding of one's fraud vulnerability and to build a response plan to a suspected fraud case or a cybersecurity breach, the risk assessment is supported by the fraud incident response section to extend our fraud management approach compared to other approaches.

Although anti-fraud training is a key element, education is not sufficient as a standalone measure The awareness and willingness of an organization must be documented and enforced by dedicated policies—such as a fraud and IT security policy—which should also consider teleworking from home. A lack of these basic concepts (Ritchie, 2021) is still common. The FMF at hand provides policy templates compiled from literature as best practices. In any case, an SME should have a legal consultation and review before handing out the policies to the organization.

A fraud management program is not valid if it is not launched. Therefore, the tier of fraud management implementation uses classical project management tools and makes proposals for an implementation roadmap and a communication plan. If an SME wants to use the given FMF as a blueprint and develop the fraud management program without external consultancy, we propose two adaptations from cybersecurity frameworks to allow an application of the framework in a self-management approach (FMFI-3a,b). One is based on the CISIS12® approach, a compliance information security management system in 12 steps (IT-Sicherheitscluster e.V., 2022; ISIS12-Netzwerk, 2020). The second proposal focuses on the five stages of the NIST cybersecurity framework (identify, protect, detect, respond, recover; The MEP National Network, 2020) applying them to fraud management, including a classification of measures as man-, technology-, or organization-related.

Shortcomings that emerged from the small set of academic literature used were considered. First, the approaches found in academic literature lack comprehensiveness in terms of the industries and types of fraud they cover. Therefore, the FMF at hand uses a modular document concept and a comprehensive fraud glossary as baselines. Second, the current literature has not shown evaluation or proof-of-concept. This issue was addressed by implementing the FMF in a real-world SME context, considering that this

fraud management framework will be easily understood by SME stakeholders. Therefore, the documents must be provided in the local language.

6 Conclusion, Limitations, and Future Research

Because of their importance and number, SMEs play a significant role in the European economy. At the same time, they are impacted by the effects of digital transformation in a positive as well as negative way. To address occupational fraud and IT security (cyber-fraud) risks, we provide a comprehensive fraud management framework for SMEs that overcomes potential limitations found in existing concepts of addressing only specific industries or fraud types or by being too big and complex for SMEs. In addition to a clear structure and process for implementation, we also provide information in the form of documents specifically designed for SMEs. We developed the artifact in two design cycles. The first cycle was an architectural design to determine the structure and content of a framework that would be applicable in real-world contexts. The second designed artifact was built with all the details and applied in a real-world SME context to demonstrate its proof of concept and to evaluate the artifact. Based on insights captured during this pilot study through interviews conducted by another researcher to minimize bias, the framework was refined to its current state. The framework consists of different documents that could be used in a modular concept, which allows a holistic approach but also flexible use and adaptations to the individual SME situation—such as size, industry, and resources. Further, it gives a structure to manage fraud rather than react on occasion and allows creation of awareness of the risk of fraud—because people are key to fraud management.

This research has some limitations. First, it has been applied to only one piloting company because fraud management is a sensitive topic that requires the establishment of trust between the researchers and the company beforehand. However, during evaluation, we assessed more components (documents) than used by the piloting SME and asked questions about perception of usability in other SME contexts. Therefore, we believe that the FMF for SMEs is generic enough to be applied in different contexts. Second, the scarce academic literature used as the basis may be an issue. By adding grey literature, we aimed to control this issue and build a broad base for designing each component of our framework. However, further research can be derived from these two limitations. Not only should the framework be tested and evaluated in additional SMEs from various industries, but also the study should be replicated after some time when the state of the field and the literature might be broader. Third, the transfer of results from the risk assessment to the next stages to select countermeasures was a bit cumbersome because this was a manual procedure prompted by the given document's approach. Here, one can think of an IS-supported version of the framework to be developed. However, such an application must consider the data protection statements and topic sensitivity of fraud by limiting accesses.

References

Abroshan, H., Devos, J., Poels, G., Laermans, E., 2021. Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. IEEE Access 9, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

ACFE, 2022. The Fraud Tree - occupational fraud and abuse classification systems.

ACFE, 2020a. Report to the Nations - 2020 Global Fraud Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners Inc., Austin - Texas - USA.

ACFE, 2020b. Fraud in the Wake of COVID-19: Benchmarking Report [WWW Document]. URL https://www.acfe.com/covidreport.aspx (accessed 6.18.20).

ACFE, 2018. Report to the Nations - 2018 Global Fraud Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners, Austin - Texas - USA.

ACFE, 2016. Report to the Nations on Occupational Fraud and Abuse - 2016 Global Fraud Study. Association of Certified Fraud Examiners, Austin - Texas - USA.

Amasiatu, C.V., Shah, M.H., 2018. First party fraud management: framework for the retail industry. IJRDM 46, 350–363. https://doi.org/10.1108/IJRDM-10-2016-0185

Andenmatten, M., 2018. COBIT 2019 – Das neue Enterprise Governance Modell für Informationen und Technologien. Disruptive agile Service Management. URL https://blog.itil.org/2018/11/cobit-2019-das-neue-enterprise-governance-modell-fuer-informationen-und-technologien/ (accessed 6.19.20).

Aris, N.A., Arif, S.M.M., Othman, R., Chantrathevi, T., Tapsir, R., 2013. Internal Control Mechanism Framework for Fraud Prevention in Small Medium Automotive Industry, in: 2013 IEEE Symposium on Humannities, Science and Engineering Research (SHUSER). Malaysia, pp. 594–598.

Asprion, P.M., Burda, D., 2019. COBIT — Enzyklopädie der Wirtschaftsinformatik [WWW Document]. Enzyklopädie der Wirtschaftsinformatik - Online Lexikon. URL https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/daten-wissen/Grundlagen-der-Informationsversorgung/COBIT (accessed 6.19.20).

Asti, A., 2021. Cyber Defense Challenges from the Small and Medium-Sized Business Perspective.

Atteslander, P., Cromm, J., Grabow, B., Klein, H., Maurer, A., Siegert, G., 2010. Methoden der empirischen Sozialforschung, 13., neu bearbeitete und erweiterte Auflage. ed, ESV basics. Erich Schmidt Verlag, Berlin.

Bada, M., Nurse, J.R.C., 2019. Developing cybersecurity education and awareness programmes for Small and medium-sized enterprises (SMEs). ICS 27, 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Barth, M., Hellemann, N., Kob, T., Krösmann, C., Morgenstern, U., Tschersich, T., Ritter, T., Shulman, H., Trapp, D., Wintergerst, R., 2020. Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt (No. Studienbericht 2020). Bitkom e.V., Berlin.

Bologna, J., Lindquist, R.J., 1995. Fraud auditing and forensic accounting: new tools and techniques, 2nd ed. ed. Wiley, New York.

Bostrom, R.P., Gupta, S., Thomas, D., 2009. A Meta-Theory for Understanding Information Systems Within Sociotechnical Systems. Journal of Management Information Systems 26, 17–48. https://doi.org/10.2753/MIS0742-1222260102

Braithwaite, J., 1985. White Collar Crime. Annu. Rev. Sociol. 11, 1–25. https://doi.org/10.1146/annurev.so.11.080185.000245

Brown, S., 2010. Likert Scale Examples for Surveys [WWW Document]. URL https://www.extension.iastate.edu/Documents/ANR/LikertScaleExamplesforSurveys.pdf

BSI, Bundesamt für Sicherheit in der Informationstechnik (Ed.), 2022. IT-Grundschutz-Kompendium, Edition 2022. ed, Unternehmen und Wirtschaft. Reguvis Fachmedien GmbH, Köln / Bonn.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N., 2020. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies 1–13. https://doi.org/10.1080/14616696.2020.1804973

Bundesamt für Justiz, n.d. § 263a StGB - Einzelnorm.

Bungartz, O., 2010. Effiziente und effektive Interne Kontrollsysteme, in: Bassen, A., Wagenhofer, A. (Eds.), Controlling und Corporate-Governance-Anforderungen Verbindungen, Maßnahmen, Umsetzung. Erich Schmidt Verlag, Berlin, pp. 131–157.

Button, M., Cross, C., 2017. Technology and Fraud: The 'Fraudogenic' Consequences of the Internet Revolution, in: McGuire, M.R., Holt, T.J. (Eds.), The Routledge Handbook of Technology, Crime and Justice. (Author version of this article).

Çalıyurt, K.T., 2012. Reporting Fraud Using the Fraud-Free Company Model: A Case for the SMEs in Emerging Economies?, in: Çaliyurt, K., Idowu, S.O. (Eds.), Emerging Fraud. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 3–18.

Cappelli, D., Moore, A., Trzeciak, R., 2012. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud), The Sei series in software engineering. Addison-Wesley, Upper Saddle River, NJ.

Christian, N., Basri, Y.Z., Arafah, W., 2019. 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.

Cika, N., 2017. An Analysis of Practices of Internal Controls in Small and Medium Enterprises in Albania. Journal of Accounting & Management (2284-9459) 7, 87–97.

Cortesão, L., Martins, F., Rosa, A., Carvalho, P., 2005. Fraud Management Systems in Telecommunications: a practical approach.

COSO, Committee of Sponsoring Organizations of the Treadway Commission, 2013. Guidance on Internal Control [WWW Document]. www.coso.org. URL https://www.coso.org/pages/ic.aspx (accessed 6.9.21).

Cressey, D.R., 1952. Application and Verification of the Differential Association Theory. The Journal of Criminal Law, Criminology, and Police Science 43, 43–52. https://doi.org/10.2307/1138991

Dawson, S., 2015. Internal control/anti-fraud program design for the small business: a guide for companies not subject to the Sarbanes-Oxley Act, Wiley corporate F&A series. Wiley, Hoboken.

Deloitte Poland, 2020. The impact of COVID-19 on the fraud risks faced by organisations

Derksen, O., 2013. Fraud Analyse von Massendaten in Echtzeit, in: Deggendorfer Forum zur digitalen Datenanalyse (Ed.), Big Data - Systeme und Prüfung. Schmidt, Berlin, pp. 45–59.

Dimitrijević, D., Karapavlović, N., Milutinović, S., 2020. Fraud prevention measures in Serbian small and medium-sized enterprises: Existence and effectiveness. Ekonomika preduzeća 68, 369–382. https://doi.org/10.5937/EKOPRE2006369D

Döring, N., Bortz, J., 2016. Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften, 5. vollständig überarbeitete, aktualisierte und erweiterte Auflage. ed, Springer-Lehrbuch. Springer, Berlin Heidelberg.

Dorminey, J., Fleming, A.S., Kranacher, M.-J., Riley, R.A., 2012. The Evolution of Fraud Theory. Issues in Accounting Education 27, 555–579. https://doi.org/10.2308/iace-50131

European Commission, 2020. User guide to the SME Definition. Publications Office of the European Union, Luxembourg.

European Commission, 2016. SME definition.

E&Y, 2018. Global Forensic Data Analytics Survey 2018: How can you disrupt risk in an era of digital transformation? Ernst & Young Fraud Investigation & Dispute Services.

Frank, U., 2013. Domain-Specific Modeling Languages: Requirements Analysis and Design Guidelines, in: Reinhartz-Berger, I., Sturm, A., Clark, T., Cohen, S., Bettin, J. (Eds.), Domain Engineering. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 133–157. https://doi.org/10.1007/978-3-642-36654-3_6

Fuad, K., Lestari, A.B., Handayani, R.T., 2020. 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. https://doi.org/10.2991/aebmr.k.200127.017

Gill, M., 2011. Fraud and recessions: Views from fraudsters and fraud managers. International Journal of Law, Crime and Justice 39, 204–214. https://doi.org/10.1016/j.ijlcj.2011.05.008

Girgenti, R.H., Hedley, T.P. (Eds.), 2011. Managing the risk of fraud and misconduct: meeting the challenges of a global regulated, and digital environment. McGraw-Hill, New York.

Gregor, S., Hevner, A.R., 2013. Positioning and Presenting Design Science Research for Maximum Impact. MISQ 37, 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Haj-Bolouri, A., Purao, S., Rossi, M., Bernhardsson, L., 2018. Action Design Research in Practice: Lessons and Concerns. Presented at the Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK.

Heißner, S., 2014. Täter und Delikte, in: Erfolgsfaktor Integrität. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 37–70. https://doi.org/10.1007/978-3-658-05608-7_2

Henselmann, K., Hofmann, S., 2010. Accounting fraud: case studies and practical implications. Erich Schmidt, Berlin.
Hevner, A.R., 2007. A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems 19, 87–92.
Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design Science in Information Systems Research. MIS Quarterly 28, 75–105.
Holzenthal, F., 2014. IT-gestützte Geldwäsche- und Betrugsbekämpfung in Banken und Versicherungen Mehrwert durch einen holistischen GRC-Ansatz. ZRFC, GRC-Report 3/14, 140–143.
Iivari, J., 2015. Distinguishing and contrasting two strategies for design science research. European Journal of Information Systems 24, 107–115. https://doi.org/10.1057/ejis.2013.35
Iivari, J., Venable, J.R., 2009. Action research and design science research - Seemingly similar but decisively dissimilar, in: ECIS 2009 Proceeedings Presented at the 17th European Conference on Information Systems, Verona, Italy.
Indarto, S.L., Ghozali, I., 2016. Fraud diamond: Detection analysis on the fraudulent financial reporting. RGC 6, 116–123. https://doi.org/10.22495/rcgv6i4c1art1
ISACA, Information Systems Audit and Control Association, 2019. COBIT 2019 framework introduction and methodology.
ISIS12-Netzwerk, 2020. Handbuch zur effizienten Gestaltung von Informationssicherheit für Kleine und Mittlere Organisationen (KMO). IT-Sicherheitscluster e. V., 93053 Regensburg, Regensburg.
IT-Sicherheitscluster e.V., 2022. Was ist CISIS12®? CISIS12®. URL https://cisis12.de/was-ist-cisis12/ (accessed 3.5.23).
Jeong, J., Mihelcic, J., Oliver, G., Rudolph, C., 2019. Towards an Improved Understanding of Human Factors in Cybersecurity, in: 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC). Presented at the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), pp. 338–345. https://doi.org/10.1109/CIC48465.2019.00047
Johnson, C., 2016. Sizing Up the NIST Cybersecurity Framework. NIST Taking Measure. URL https://www.nist.gov/blogs/taking-measure/sizing-nist-cybersecurity-framework (accessed 6.19.20).
jusline.at, 1975. § 146 StGB (Strafgesetzbuch), Betrug - JUSLINE Österreich.
Kassem, R., Higson, A., 2012. The New Fraud Triangle Model. JETEMS 3, 191–195.
Kempf, D., 2015. Ohne Schutzschild. IT-Security Channel Compendium.
Lachney, K., 2020. An Exploration of Internal Controls and Their Impact on Employee Fraud in Small Businesses. Journal of Forensic and Investigative Accounting 12, 21–44.
Lee, Y., Shin, J., Park, Y., 2012. The changing pattern of SME's innovativeness through business model globalization. Technological Forecasting and Social Change 79, 832–842. https://doi.org/10.1016/j.techfore.2011.10.008
Li, W., Liu, K., Belitski, M., Ghobadian, A., O'Regan, N., 2016. E-Leadership through Strategic Alignment: An Empirical Study of Small- and Medium-sized Enterprises in the Digital Age. Journal of Information Technology 31, 185–206. https://doi.org/10.1057/jit.2016.10

Lincke, S., Green, D., 2012. Combating IS fraud: A teaching case study, in: AMCIS 2012 Proceedings. Presented at the Americas Conference on Information Systems (AMCIS), Seattle, Washington, pp. 578–584.

Maccani, G., Donnellan, B., Helfert, M., 2015. Action Design Research: A Comparison with Canonical Action Research and Design Science, in: At the Vanguard of Design Science: First Impressions and Early Findings from Ongoing Research Research-in-Progress Papers and Poster Presentations from the 10th International Conference. Presented at the DESRIST 2015, Dublin, Ireland.

Marks, J., 2020. Fraud Pentagon - Enhancements to the Three Conditions Under Which Fraud May Occur. BoardAndFraud. URL https://boardandfraud.com/2020/05/21/fraud-pentagon-enhancements-to-the-fraud-triangle-and-under-which-fraud-may-occur/ (accessed 1.5.21).

Maulidiana, S., Triandi, T., 2020. 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. https://doi.org/10.2991/aebmr.k.200522.042

Muhsin, Kardoyo, Nurkhin, A., 2018. What Determinants of Academic Fraud Behavior? From Fraud Triangle to Fraud Pentagon Perspective. KSS 3, 154. https://doi.org/10.18502/kss.v3i10.3126

Nindito, M., 2018. Financial Statement Fraud: Perspective of the Pentagon Fraud Model in Indonesia. Academy of Accounting and Financial Studies Journal.

NIST, National Institute of Standards and Technology, 2013. NIST Cybersecurity Framework [WWW Document]. www.nist.gov. URL https://www.nist.gov/cyberframework (accessed 3.11.23).

Pasculli, L., 2020. COVID19-related fraud risks and possible anti-fraud measures (Written evidence submitted to the Treasury Committee on the Economic Impact of Coronavirus) (No. EIC0792). Coventry University.

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems 24, 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peffers, K., Rothenberger, M., Tuunanen, T., Vaezi, R., 2012. Design Science Research Evaluation, in: Design Science Research in Information Systems. Advances in Theory and Practice. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 398–410. https://doi.org/10.1007/978-3-642-29863-9_29

Prat, N., Comyn-Wattiau, I., Akoka, J., 2014. Artifact Evaluation in Information Systems Design Science Research - A Holistic View. Presented at the Proceedings - Pacific Asia Conference on Information Systems, PACIS 2014, p. 16.

Phuttima, S., Rueangsirasak, W., Chaisricharoen, R., 2014. Fraud Detection System for Steel Logistic SME Business on Cloud Services Model. Presented at the 2014 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), IEEE, Chiang Rai, Thailand. https://doi.org/10.1109/JICTEE.2014.6804088

Ponemon, 2017. 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB). Ponemon Institute LLC.

Pouwels, A.C.J., 2022. Combating fraud and protecting the EU's financial interests | Fact Sheets on the European Union | European Parliament [WWW Document]. URL https://www.europarl.europa.eu/factsheets/en/sheet/32/combating-fraud-and-protecting-the-eu-s-financial-interests (accessed 3.10.23).

Ritchie, D., 2021. Cyber insecurity - Resliience for the new normal. CIR - Continuity Insurance & Risk 16–19.

Roden, D.M., Cox, S.R., Kim, Joung Yeon, 2016. THE FRAUD TRIANGLE AS APREDICTOR OF CORPORATE FRAUD. Academyof Accounting and Financial Studies Journal 20, 80–92.

Schöber, P., Schmitz, P., 2020. Hochkonjunktur für die Schatten-IT [WWW Document]. IT-Business. URL https://www.it-business.de/hochkonjunktur-fuer-die-schatten-it-a-973554 (accessed 10.23.20).

Schuster, H., 2021. Schatten-IT im Homeoffice gefährdet Unternehmens-IT [WWW Document]. IT-Business. URL https://www.it-business.de/schatten-it-im-homeoffice-gefaehrdet-unternehmens-it-a-1010689 (accessed 3.29.21).

Sein, Henfridsson, Purao, Rossi, Lindgren, 2011. Action Design Research. MIS Quarterly 35, 37–56. https://doi.org/10.2307/23043488

Soomro, Z.A., Ahmed, J., Shah, M.H., Khoumbati, K., 2019. Investigating identity fraud management practices in e-tail sector: a systematic review. JEIM 32, 301–324. https://doi.org/10.1108/JEIM-06-2018-0110

Spindler, M., Kögel, H., 2020. Erkennung von Versicherungsbetrug mit künstlicher Intelligenz (Faktenpapier No.9), AI: Science over Fiction. Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Berlin.

Tazilah, M.D.A.B.K., Hussain, N.B.C., 2015. The Importance of Internal Control in SMEs: Fraud Prevention & Detection. Presented at the International Conference on Business, Accounting, Finance, and Economics (BAFE 2015), Malaysia.

The MEP National Network, 2020. MANUFACTURERS GUIDE TO CYBERSECURITY - For Small and Medium-Sized Manufacturers.

Trierweiler, M.K., 2022. IT-based Fraud Management Approaches in Small and Medium Enterprises – A Multivocal Literature Review, in: Wirtschaftsinformatik 2022 Proceedings. Presented at the 17th International Conference on Wirtschaftsinformatik (WI22), Nürnberg, Germany.

Trierweiler, M.K., 2021. Development of an IT-supported Anti-Fraud-Framework for SMEs: An Architectural Concept for Risk Management Using the 'Man-Technology-Organization' Approach, in: CEUR Workshop Proceedings of 7th International Workshop on Socio-Technical Perspective in IS Development (STPIS'21). Presented at the 7th International Workshop on Socio-Technical Perspective in IS development (STPIS'21), Trento, Italy, pp. 204–215.

U. S. Government Accountability Office, 2015. A Framework for Managing Fraud Risks in Federal Programs | U.S. GAO [WWW Document]. URL https://www.gao.gov/products/gao-15-593sp (accessed 3.11.23).

Ulich, E., 2013. Arbeitssysteme als Soziotechnische Systeme – eine Erinnerung. Journal Psychologie des Alltagshandelns 6.

Umar, H., Partahi, D., Purba, R.B., 2020. Fraud Diamond Analysis In Detecting Fraudulent Financial Report. IJSTR 9, 6638–6646.

Venable, J., Pries-Heje, J., Baskerville, R., 2012. A Comprehensive Framework for Evaluation in Design Science Research, in: Peffers, K., Rothenberger, M., Kuechler, B. (Eds.), Design Science Research in Information Systems. Advances in Theory and Practice: 7th International Conference, DESRIST 2012. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 423–438. https://doi.org/10.1007/978-3-642-29863-9_31

vom Brocke, J., Buddendick, C., 2006. Reusable Conceptual Models-Requirements Based on the Design Science Research Paradigm. Presented at the DERIST 2006, Claremont, CA, USA.

Vona, L.W., 2008. Fraud risk assessment: building a fraud audit program. J. Wiley & Sons, Hoboken, NJ.

Wells, J.T., 2014. Principles of fraud examination, Fourth edition. ed. Wiley, Hoboken, NJ.

Wells, J.T., 2001. Enemies Within. Journal of Accountancy 192, 31–35.

Wieringa, R.J., 2014. Design science methodology for information systems and software engineering. Springer Berlin Heidelberg, New York, NY.

Wolfe, D.T., Hermanson, D.R., 2004. The Fraud Diamond: Considering the Four Elements of Fraud. CPA Journal 74.12, 38–42.

Yearwood, L.D.A., 2011. A Conceptual Framework for the Prevention and Detection of Occupational Fraud in Small Businesses (Master Thesis). Concordia University College of Alberta, Alberta Canada.