Development of an IT-supported Anti-Fraud-Framework for SMEs: An Architectural Concept for Risk Management Using the 'Man-Technology-Organization' Approach

Michaela K. Trierweiler [1]

[1] *Johannes Kepler University, Altenberger Straße 69, Linz, 4040, Austria*

Abstract

Small and medium enterprises (SMEs) are an important economic factor in many countries. In the European Union, they represent the majority of companies, provide two thirds of all jobs, and drive a lot of innovation. This makes them attractive for perpetrators of fraud; limited resources in terms of money, staff, and IT knowledge make them vulnerable. This research deals with the question of how to minimize fraud as a specific risk to SMEs. In concrete terms, it sets out how a framework should look and establishes the guidance that should be given in the context of fraud prevention. This study is set up as a design science research project with the aim of producing a concrete framework as a solution and contributing artifact. Previous research shows that there is a gap in academic research regarding fraud prevention concepts tailored to SMEs. This assumption seems valid as an integrative literature review revealed only a few appropriate papers plus a great deal of non-academic or semi-academic literature. In particular, information systems research is underrepresented in this area. Existing SME-related fraud prevention frameworks concentrate more on internal related fraud risks rather than on fraud committed by external parties, such as cybercrime. This suggests that a comprehensive fraud prevention concept is missing for SMEs and is worthy of being developed, especially considering that any enterprise is a socio-technical system. Keeping in mind that such a framework must be generic enough to cover different fraud risks and company situations while also giving concrete advice, this research applies domain-specific modeling principles to find the best notation and style of presentation. This work-in-progress paper proposes a preliminary architectural model for a new fraud prevention concept suitable for SMEs.

Keywords[1]

fraud prevention, framework, SME, MTO, risk management, socio-technical system, design science

1. Introduction and Research Scope

Small and medium enterprises (SMEs) are considered to be the engine of many economies. In the European Union, nine out of 10 enterprises are SMEs and they generate two thirds of all jobs [1]. SMEs drive innovation and are seen as a key factor in driving competitiveness and employment. Therefore, they are lucrative targets for criminals [2]–[6]. Analysis of the fraud situation in SMEs (as recorded by the Association of Certified Fraud Examiners in their bi-annual *Report to Nations*) proves the importance of fraud prevention for SMEs. Over the last several years, they were the most common victims of fraud with an approximately share of 30%. Since 2018, SMEs have suffered the highest financial losses and thus the biggest negative impacts compared to companies of other sizes [4], [7], [8]. In addition, SMEs face different fraud risks than those faced by larger companies [8]. Therefore,

P 7th International Workshop on Socio-Technical Perspective in IS development (STPIS'21), October 11th-12th, 2021, Trento, Italy
EMAIL: mkt.jku@gmail.com (Michaela K. Trierweiler)
ORCID: 0000-0003-3016-9889 (Michaela K. Trierweiler)

they need different fraud risk management concepts (or at least tailored countermeasures) that are suited to the personnel resources, organization and technical possibilities of SMEs.

In legal terms, fraud is part of the field of white-collar crime. The main elements are intention, deception, and damage to another party in the sense of financial loss (see, for example, §263 and §263a of the German criminal law [9] or §146 of the Austrian criminal law [10]). The bandwidth of white-collar crime is huge and includes both delicts that harm a company directly (such as paying too much salary) and delicts that may seem beneficial for a company at first glance, such as corruption to gain a large and profitable deal [11]. In 2007, Joseph T. Wells developed a classification system for occupational fraud and abuse in business contexts that is known as the *fraud tree* [12]. This system covers most kinds of misconduct by executives, managers, and employees [13]. The model has been refined over the years and is now considered to be one of the state-of-the-art fraud definition concepts. All types of fraud considered in this taxonomy could be summarized as non-compliant and as a undesired behavior because they harm either an organization [11] or an individual.

The existing literature discusses different fraud theories and concepts about the facilitators of fraud. Although very different fraud models have been developed in recent decades [14], the widely accepted perception follows the approach of Cressey, developed in the 1950s, where three critical elements must apply: incentive/pressure, opportunity, and attitude/rationalization [13]. This concept, known as the *fraud triangle*, was further developed by Wolfe and Hermanson [15] by supplementing a fourth dimension and is now commonly known as the *fraud diamond*. The added fourth dimension of capability (defined as intelligence, creativity, and experience [13], [15]) could be interpreted in the sense of technical and computational skills. It is therefore relevant when considering cybercrime and IT-based fraud. In recent research, such as [16]–[20], a fifth dimension of arrogance is discussed, along with its impact on fraud management. This leads to an approach named the *fraud pentagon*.

Fundamentally, small companies are more likely to lack internal controls [4], have no proper risk management systems in place, and lack staff in IT functions, because the focus of employment lies in staffing the core roles and functions that are critical for running and developing the business. Micro SMEs [21], defined as those that have fewer than ten employees, have a very flat organizational structure and often combine functions in one role. This makes active fraud prevention (or even a simple thing such as the four-eyes principle when signing documents or releasing payment requests) difficult to establish. In SMEs, a compliant corporate culture, including fraud prevention and detection, is usually practiced by example or just because it is seen as commonly accepted good manners. It is seldom methodically established as a part of enterprise risk management. The most well-protected and legally regulated area is accounting because this is the most lucrative part. Besides accounting fraud (e.g., fraudulent statements) there are many other forms of occupational fraud, such as identity theft, bribery, asset misappropriation, and corruption [12]. The existing fraud risk situation is currently fostered by the COVID-19 crisis: the sudden rise of rapidly implemented information and communication techniques (ICT) makes it easier for fraudsters to attack [22] and a significant increase in cyber fraud, payment fraud, or identity theft [23]–[27] is projected.

Increasing digitalization, and the omnipresence of apparently straightforward IT tools such as email programs in daily business transactions, results in a reciprocal relationship between IT and fraud prevention. IT tools often are vectors for fraud attacks (e.g., email phishing attempts); on the other hand, specific software and hardware tools, real-time or big data analytics [28], [29], or even AI [30] can help to prevent and detect fraud. However, highly technological or ERP-based measures are seldom used in SMEs. The literature review reveals a lack of discussion of IT-related fraud prevention measures, which is notable considering the importance of IT in today's business world. Many researchers focus on organizational measures and do not deliver comprehensive guidelines or pursue a generalized research approach. Furthermore, in many cases, research in this area is neither related to information systems (IS) research nor considers fraud risk as a problem in an enterprise that has an ICT landscape embedded within a socio-technical business environment where people and technology working jointly together.

This research aims to contribute to filling this gap through a design science research project. The project is setup in three major stages, starting with an integrative literature review to examine the state of existing research and to build a knowledge base. This is followed by designing an alternative fraud prevention concept as new artifact that overcomes potential limitations found in existing concepts. The research concludes with an evaluation based on piloting the new framework in some SMEs and gathering feedback in terms of understandability, complexity, and integration in order to refine the framework to its final state.

Based on the assumption that bigger companies have a greater need for fraud prevention than smaller companies (as well as more workers and resources with which to establish anti-fraud controls and countermeasures), the following research questions (RQs) have been defined:

RQ 1. What kinds of SME-tailored fraud management frameworks can be found in the existing literature? What fraud types do they consider and how are IT-related fraud risks discussed?

RQ 2. What does an IT-supported fraud prevention framework need to look like in order to fit into an SME to cover the individual fraud risk and consider given resources? What IT security concepts can be applied to such a new framework as an artifact to be created?

RQ 3. How does this newly developed IT-supported fraud prevention framework perform in different SME contexts? Where are the limitations of the framework and what adjustments are necessary?

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 is based on the man-technology-organization (MTO) concept of Strohm and Ulich [31]. An effective anti-fraud management system is a socio-technical system in the sense that it requires collaboration between technology (e.g., IT security aspects), organizational procedures (e.g., the four-eyes principle), and workers (e.g., awareness training and ethical culture). Therefore, a new framework must be comprehensive, science-based, compatible with SMEs' fraud risk needs, and understandable for non-academics.

This objective has a major influence on the design and notation used for describing the new framework model. The relevance and benefits of such a framework are based on the fact that SMEs have limited know-how on such controls; they could easily lose reputation and money in the event of fraud. Existing IT frameworks are often very complex and do not meet the requirements of SMEs or are beyond the knowledge base of SMEs. Therefore, a more practical and tailored guidance is required. The present work-in-progress paper describes the development and evaluation of a new concept and proposes a preliminary architectural draft for an SME-appropriate fraud prevention approach that includes IT-related risks and countermeasures.

2. Methodology and Research Design

This section describes the methodologies used in the present research.

2.1. Literature Review

The literature review in context of this research fulfilled three aims. The first aim was to establish the current state of academic research and to find potential existing frameworks. The second aim was to verify the gap-spotting approach in terms of clarifying the research focus and to define the research entry point for the design science procedure. The third aim was to find the best resources in order to design a new framework for a universal fraud prevention concept for SMEs.

An integrative literature review was performed in several stages, starting with the application of structured literature review principles as suggested by Kitchenham [32], Massaro et al. [33], and Fink [34] using three academic databases (Compliance Digital [German language], EBSCOhost, and Scopus). Strict search strings were used (containing "fraud | framework | SME") to find peer-reviewed research papers. The number of results was very small, which suggested a gap in research. To clarify this outcome and to obtain robust results for the definition of the academic resource pool, a second round of systematic searching was performed. In this round, the search strings were more generic and additional databases (IEEE, ResearchGate, Academia) were used along with snowballing and free searches. After this second round, the literature review showed a gap in terms of academic research in the field of fraud prevention frameworks for SMEs. It also revealed a large amount of case-descriptive or consultancy-related literature. Based on the used search strings,736 hits were found; after reading titles, abstracts, and skim-reading the text, only 33 items were found to be relevant. Especially the third target of building an adequate resource pool as baseline for the design phase required to include more practitioners' view (reflected in textbooks) and to add non-academic (so called *grey literature*) works as well. The final source pool consists of 61 items. These sources were assessed according to guidelines from Snyder [35] and Garousi et al. [36]. Four academic works were excluded because of their poor empirical base, one journal article was not available, one publication was a doublet based on same research, and one of the grey literature items was excluded due to missing contribution to my research. Consequently, the final core pool of literature consisted of 54 items that were screened and classified according to the following criteria:

- Schematic allocation of relevant keywords (define scoping and relevance of each source)
- Geographic coverage (check transferability to European economy)
- Empirical base (decide on the meaningfulness of the scientific work)
- Qualifiers for content (e.g., what the source discusses)
- Qualifiers for intended use during the further research steps.

The geographical coverage of the sources (generic, North America, and Asia) suggested the need for adaption before doing a transfer to European requirements because economical situations differ. The small number of design science approaches showed that there was a lack of concrete frameworks. The quantitative analyses carried out by some researchers were often based on a small number of valid answers (with N ranges from 37 to 250). This low empirical base and evidence needed to be considered when adapting information to the present research. In terms of content, most of the papers related to the search term "fraud and SME" contained descriptive statistics about the fraud situation in certain countries or business areas. However, they did not give a holistic prevention approach that included IT-supported prevention measures. Most of the sources concentrated on organizational or internal control aspects. These sources were used in the present research for problem statements or for explaining important background aspects. Sources that mention a concrete framework or guideline often referred to existing frameworks, such as *Internal Control – Integrated Framework*, published by Committee of Sponsoring Organizations of the Treadway Commission (COSO-2013) [35]. Many other authors have used the COSO-2013 as justification for their own introduction or problem statement. The concentration on accounting fraud (or other very specific fraud types such as payroll fraud or employee fraud) indicated a lack of research in handling certain fraud types (especially IT-related or cybersecurity-related fraud attempts). The concentration on specific industry sectors also suggested a missing holistic or universal approach.

To summarize, the fact that only a limited number of scientific papers and sources deal with all three scope-criteria (fraud, framework and SME) indicated a gap in the academic discourse in that area. Because of this small scientific base, grey-literature and textbooks from fraud prevention or auditing experts were added to the information pool for this research (always keeping in mind that such texts are often written in the context of the Anglo-American economic situation). In addition, established frameworks from other disciplines will be analyzed to find useful concepts to be transferred into the present approach during the design phase of this research.

2.2. Design Science Research Concept

In order to design a framework model in a structured way, this research project is conducted by following the design science principles of Hevner et al. [36] and the design science process model (DSPM) from Peffers et al. [37]. The final artifact will obtain proof-of-concept during the evaluation phase in a specific SME context that is yet to be defined. The socio-technical approach is in line with Hevner's [38] three-cycle view of design science as reflected in the *relevance cycle* connecting the environment with the designing phase.

Six fraud management frameworks dedicated to SME were found during the literature search. This information defined the entry point of this research as an *objective-centered solution*. This entry point enables the planning of a new (or improved) prevention framework. It was necessary to analyze and compare existing anti-fraud frameworks in order to identify gaps and add missing technology and aspects. Useful content could be found by evaluating well-established auditing frameworks such as the Sarbanes-Oxley Act (2002) or the US National Institute of Standards and Technology (NIST) cybersecurity framework (2014).

The framework developed in this way is the artifact in the sense of the design science approach. Regarding the nominal process sequence, Table 1 shows the six stages of the design science process model (DSPM) plus an iteration, and briefly declares the use respectively to the present research work.

Table 1

Relationship of the DSPM Sequence [37] to the Present Research

Stage of DSPM	Relationship to current research
Identify Problem/ Motivation	Fraud is a white-collar crime and entails the risk of losing money and reputation; thus, fraud prevention is relevant for enterprises of all sizes. SMEs are increasingly affected. Currently, there are only a few non-holistic fraud prevention frameworks that are dedicated to SMEs.
Define Objectives of the Solution	As part of enterprise risk management, fraud prevention measures could be transferred from existing fraud-fighting concepts and from other areas such as IT security or generic compliance recommendations. These must be tailored to the needs and resources of SMEs. Such a framework must contain concrete measures, checklists, and action plans outlining the steps an SME should take against different types of fraud within their industry. (This phase contributes to answering RQ-2).
Design and Development	The notation of this framework will apply domain-specific modeling principles. It must be understandable for scientists and practitioners. The architectural structure is presented with this paper. (This phase contributes to answering RQ-2).
Demonstration	A conceptual model and drafts will be presented at relevant conferences and in discussions with practitioners (e.g., compliance managers) from the business network (expert evaluation). (This phase contributes to answering RQ-3).
Evaluation	The core evaluation is planned as a pilot implementation with two SMEs of different sizes and from different industries. The aim is to get a real-life proof-of-concept for completeness, practicability, and understandability. Such an evaluation is an interactive method and requires collaboration between the researcher and the piloting company. Therefore, the method of action research seems to be the best approach. A second, more theoretical approach is to apply an SME-related IT security maturity model to evaluate the feasibility of an IT-supported fraud prevention framework. (This phase contributes to answering RQ-3).
Process Iteration	*The feedback from demonstrations and evaluation phases will be used to rework and refine the artifact.*
Communication	Communication is planned in the form of a scholarly publication and a professional publication (textbook). Parts of it will be written bi-lingually in German and English to allow access by a broader audience.

2.3. Evaluation of the New Framework in Certain SME Contexts

Once the new framework is created, an evaluation will be required to ensure utility, efficacy, understandability, and completeness. This evaluation will also identify potential limitations. Some literature [39]–[41] suggests different methods suitable for evaluation purposes in design science research contexts; these include benchmarking, expert evaluation, experiments, action research, prototyping, and case studies. Several strategies for selecting the appropriate method are proposed by IS researchers [42]–[44]. These take into consideration aspects of risk, effectiveness, efficacy, and technical aspects with the aim of evaluating how well the artifact performs. After comparing possible evaluation methods by their intended use, the concept of action research seems to be the best approach for this current research because it allows a practical problem to be solved through the joint cooperation of science and practice [45], [46]. The latter, in this context, would be a SME willing to pilot, implement, and utilize the new framework. In contrast, a case study approach [47] does not seem to be suitable in this research because no hypothesis with variables on an individual or single existing phenomenon shall be validated. The aim of this research is to test the artifact implementation in a real-world situation, which results in a concrete and tailored instance of the framework for the piloting SME. Action research can provide scientific knowledge but also improve organizational problems where some technology is adopted or even built from scratch, supported by state-of-the-art corresponding knowhow [48]. Action research is an interactive method that considers both the practical concerns of people working with the framework and the goals of the researcher in order to obtain feedback on how the artifact performs; it is set up as an iterative process [49]. The cyclic approach of action research was interpreted by Checkland as an approach where the researcher is interested in a certain research theme that is related to a real-world problem situation and where the researcher participates the situation (consultancy to the piloting SME during implementation) to enable reflections that will lead to findings related to the research theme [50]. This approach seems suitable for the present research because the framework of ideas (the new artifact), the methodology, and the area of concern are defined in advance.

Regarding the answer to RQ-3, proper planning and acquisition of piloting SMEs is necessary. The approach in this study is to present, discuss, and implement the new fraud prevention framework in two piloting SMEs of different sizes and in different industries. Potential partners will need to come from very different areas in order to obtain diverse feedback regarding understandability, comprehensiveness, and applicability (in the sense of implementation while running the daily work and not to interfere with current business processes). The intention is to pilot the framework with a small SME with less than 20 employees and a medium-sized SME with more than 100 employees [21]. The different numbers of employees impacted by the framework will allow conclusions to be drawn about the practicability of the framework and the impact on given resources. In terms of industry sectors, the aim is to run one pilot implementation in a more technology-oriented company (such as a software development company with a high level of digital maturity) and to perform a second evaluation in a more traditional industry. This will test the applicability of the prevention framework for different types of fraud risks. If the framework is suitable for very different company situations, this may indicate that it provides a generic prevention concept that could be applied to various SME situations. Feedback about applicability will be captured by interviewing the piloting companies about their experiences during the implementation phase and some month after in order to gather feedback about its usability during daily work.

Finding piloting partners may be difficult because the SME must see clear benefits in undertaking the effort of such a scheme. Therefore, this research will be supported by presentations and through discussion of the framework with experts from related domains (such as compliance, auditing, and IT security). In addition, a theoretical evaluation will be conducted by applying digital maturity models to the framework for the question about necessary IT prerequisites a SME must have to be able to implement such an IT-supported fraud prevention framework; especially if the SME might not have an own dedicated IT or security department but needs to implement dedicated software and other IT-related tools to better protected against fraud attempts.

2.4. Notation of Framework: Use of Domain-Specific Modeling Principles

After first drawings of the components, their interconnections, and related sub-process and possible content for the current fraud-prevention framework, it got clear to design and describe the framework in its own notation by applying principles for domain specific modelling suggested by Kelly and Tolvanen [51]. The framework will consist of several layers and types of information (such as flowcharts) to show dependencies, business workflows, checklists, step plans, and recommendations for software tools. It will also be necessary to include a glossary outlining the different types of fraud and the proven countermeasures that an SME could implement. This combination of graphical and textual content must find a form of notation that is both understandable and abstract enough to allow existential generalizations [52]. IT-specific notations such as Unified Modelling Languages (UML) or the concept of BPMN 2.0 would cover only parts of the framework; others, such as ArchiMate®, are too complex to be understood by those who are not IT experts.

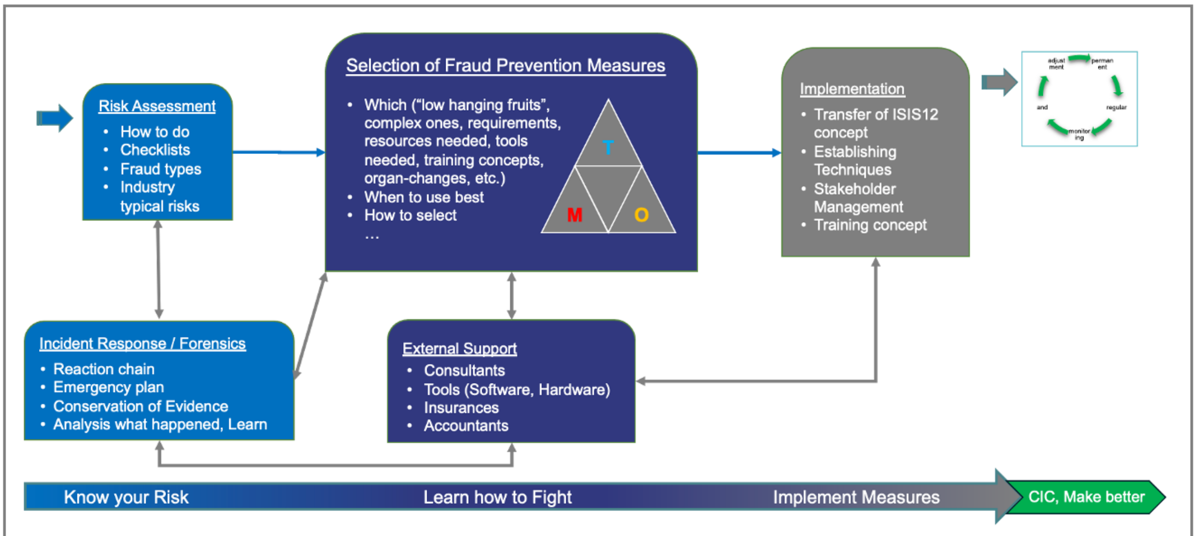
3. Summary of Findings to Date and Current State of Artifact Design

The first examination of the six fraud prevention frameworks dedicated to SMEs revealed that these concepts showed a narrow scope and offered little advice on prevention measures. These concepts either concentrated on a very specific context [53], [54], or only covered employee fraud [55], [56] and not external fraud risks. One case study [57] pursued a more behavioral approach by developing a code of conduct and incident response chains, while another study [58] concentrated on reporting options for fraud. An alternative prevention concept must also consider external fraud vectors. Internal control mechanisms must be supplemented by IT techniques to detect fraud at an early stage.

When looking into existing and well-established frameworks from other disciplines, some transferable information seems promising. For instance, the IT management and IT governance framework COBIT-2019 (Control Objectives for Information and Related Technologies) developed by the Information Systems Audit and Control Association allows different perspectives and focus areas, one of which is related to SMEs [59], [60]. The NIST Cybersecurity Framework [61], [62] allows SME specific security approaches. As an example, a transfer of the five stages of NIST cybersecurity framework (identify, protect, detect, respond, recover) [63] into fraud prevention measures including a classifying of these measures as man-, technology- or organization-related. The MTO classification allows the creation of different cluster for the implementation and makes it easier for SMEs to decide what prevention measure to be installed and in what order. With regard to the implementation itself, the use of the ISIS12 (Information Security Management System in 12 steps) concept [64] could be adapted to create a roadmap for implementing a fraud-prevention framework.

An in-depth analysis of the six concepts found during the literature review and a detailed review of established frameworks from other disciplines is currently in progress. Therefore, the present architectural fraud prevention framework (as visualized in Figure 1) is at a preliminary stage. It consists of five connected dimensions (Tier 1). The framework deals with risk management in order to allow the SME to identify the individual fraud risk. It touches on fraud forensics because the need for risk management is often realized after an incident has occurred. The core part of the framework discusses and describes the fraud types and their countermeasures along the MTO concept to enable the selection of suitable measures. In addition, the proposed framework gives ideas of where to find external support and suggests a roadmap for implementation. A continuous improvement cycle must follow the implementation in order to keep the implemented measures up to date.

Figure 1 illustrates the different components, connections, and interplay. But a second conceptualization is helpful to understand the layers of granularity in each tier. This information will be worked out in detail for the final publication and the concrete guideline for SME practitioners.



Explanation:

Box	*= Tier 1, main process step, containing sub-processes*
Bullet-Point in Box	*= Tier 2, sub-process or sub-information, high level of detail*
Pointers/Edges	*= connection/dependency/way-to-go between the (sub-)processes, sometimes bi-directional or resulting in loops to go*
CIC	*= continuous improvement cycle*
Big Arrow	*= idealistic starting/ending point and path through the model ('happy path` in case an organization has enough resources and can start without a fraud incident as trigger)*

Figure 1: Prelim. Fraud Prevention Framework for SMEs

Figure 2 shows the content-related structure consisting of six layers (I–VI) with an increase in granularity for each level. For example, Layer VI will contain concrete recommendations and references or weblinks, whereas Layers I and II are more introductory and will provide background overviews. Layers III–VI build the core of the framework and will offer a concrete toolbox for selecting and implementing the most suitable countermeasures for the individual fraud risk as identified during the risk assessment. Layers III – VI reflect the Tier 2 containing all sub-processes and a high level of content and detailed information.

Layer of content	Information included
I – High-level description	Textual introduction, high-level overview, and explanations of how the framework is organized.
II – Streams	Explanation of Tier 1 in a timely and logical order (incident response/forensics and external parties involved/support are left out for simplification reasons) and why things should be done in a specific sequence because the build upon each other. Individual fraud risk assessment Decide for measures along MTO Implementation Review/continuous improvment
III – How-to implement	Concentration on procedural aspects; explanation/suggestion of best practices for conducting the activities; fraud risk assessment; selection of appropriate fraud prevention measures; implementation strategies; and when forensics or external support is indicated.
IV – What to implement	Detailed explanation (glossary) of different fraud risks, how to identify the individual risk, and what countermeasures are commonly seen as effective for them.
V – What to implement (give more details)	Explanation of the details of each measure (categorization along MTO) and their interconnections (what they look like; providing concrete examples with prepared checklists, step plans and workflows; suggestions when external support and software/hardware may be useful; suggestion for variants for micro-SMEs with limited resources and potential upgrades for medium-sized SMEs).
VI - Supplements	Recommendations for concrete external support, software, hardware, and further literature.

--------- increasing level of detail --------->

Figure 2: Prelim. Architectural and Content-related Structure of Fraud Prevention Framework for SMEs

4. Conclusion, Limitations and Further Research

This research project concentrates on finding the best measures and activities for preventing or detecting fraud in small and medium organizations. It is supplemented with related aspects of IT security, risk management, and implementational aspects. The present work-in-progress paper gives an idea of why a comprehensive fraud-fighting framework is valuable for SMEs. It also shows why this framework must be created in a generalized and flexible manner to enable SMEs to choose the fraud prevention activities that are most suitable for their business model and resource situation. Therefore, the final framework might include advice for modifications of some suggested fraud prevention measures to make them applicable to micro-SMEs, as well.

Limitations might occur if a generic framework cannot be created, since different fraud types or industries would require very different prevention approaches. This would increase complexity and might reduce the applicability and understandability of the framework.

Upcoming steps during this design science research project will include an in-depth analysis of the six fraud prevention concepts found during the literature review and the evaluation of existing frameworks from other disciplines. These insights will be incorporated into the design and creation of the Tier 2 details for the above-mentioned five dimensions (Tier 1 boxes). The MTO approach will be used to enable manageable cluster for the implementation of different measures that will interplay and build a fraud prevention and detection framework for the SME. The SME context for the evaluation will be defined (e.g., the use of very different industry partners) and a roadmap for evaluation will be prepared according to the principles of action research in order to acquire piloting SME partners and to prepare for expert evaluation.

5. References

[1] European Commission, “User guide to the SME Definition,” Publications Office of the European Union, Luxembourg, Aug. 2020. Accessed: Feb. 12, 2021. [Online]. Available: https://ec.europa.eu/docsroom/documents/42921

[2] D. Kempf, “Ohne Schutzschild,” *IT-Security Channel Compendium*, Jun. 2015.

[3] Ponemon, “2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB),” Ponemon Institute LLC, Sep. 2017. Accessed: Nov. 28, 2020. [Online]. Available: https://www.csrps.com/wp-content/uploads/2019/03/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf

[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. Accessed: Dec. 01, 2020. [Online]. Available: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

[5] M. Barth *et al.*, “Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt,” Bitkom e.V., Berlin, Studienbericht 2020, 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. [Online]. Available: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-global-fda-survay.pdf

[7] ACFE, “Report to the Nations on Occupational Fraud and Abuse - 2016 Global Fraud Study,” Association of Certified Fraud Examiners, Austin - Texas - USA, 2016. Accessed: Apr. 07, 2018. [Online]. Available: https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

[8] ACFE, “Report to the Nations - 2018 Global Fraud Study on Occupational Fraud and Abuse,” Association of Certified Fraud Examiners, Austin - Texas - USA, 2018. Accessed: May 15, 2018. [Online]. Available: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

[9] Bundesamt für Justiz, “§ 263a StGB - Einzelnorm.” https://www.gesetze-im-internet.de/stgb/__263a.html (accessed Mar. 07, 2019).

[10] jusline.at, “§ 146 StGB (Strafgesetzbuch), Betrug - JUSLINE Österreich.” https://www.jusline.at/gesetz/stgb/paragraf/146 (accessed Mar. 07, 2019).

[11] S. Heißner, “Täter und Delikte,” in *Erfolgsfaktor Integrität*, Wiesbaden: Springer Fachmedien Wiesbaden, 2014, pp. 37–70. doi: 10.1007/978-3-658-05608-7_2.

[12] Association of Certified Fraud Examiners, “The Fraud Tree - occupational fraud and abuse classification systems,” *The Fraud Tree - Occupational Fraud and Abuse Classification System*, 2016. https://www.acfe.com/rttn2016/images/fraud-tree.jpg (accessed Mar. 07, 2019).

[13] K. Henselmann and S. Hofmann, *Accounting fraud: case studies and practical implications*. Berlin: Erich Schmidt, 2010.

[14] J. Marks, “Fraud Pentagon - Enhancements to the Three Conditions Under Which Fraud May Occur,” *BoardAndFraud*, May 21, 2020. https://boardandfraud.com/2020/05/21/fraud-pentagon-enhancements-to-the-fraud-triangle-and-under-which-fraud-may-occur/ (accessed Jan. 05, 2021).

[15] D. T. Wolfe and D. R. Hermanson, “The Fraud Diamond: Considering the Four Elements of Fraud,” *CPA Journal*, vol. 74.12, pp. 38–42, 2004, [Online]. Available: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs

[16] N. Christian, Y. Z. Basri, and W. Arafah, “Analysis of Fraud Triangle, Fraud Diamond and Fraud Pentagon Theory to Detecting Corporate Fraud in Indonesia,” *The International Journal of Business Management and Technology*, vol. 3, no. 4, pp. 73–78, Aug. 2019.

[17] K. Fuad, A. B. Lestari, and R. T. Handayani, “Fraud Pentagon as a Measurement Tool for Detecting Financial Statements Fraud,” Vung Tau City, Vietnam, 2020. doi: 10.2991/aebmr.k.200127.017.

[18] S. Maulidiana and T. Triandi, “Analysis of Fraudulent Financial Reporting Through the Fraud Pentagon Theory,” South Tangerang, Indonesia, 2020. doi: 10.2991/aebmr.k.200522.042.

[19] Muhsin, Kardoyo, and A. Nurkhin, “What Determinants of Academic Fraud Behavior? From Fraud Triangle to Fraud Pentagon Perspective,” *KSS*, vol. 3, no. 10, p. 154, Oct. 2018, doi: 10.18502/kss.v3i10.3126.

[20] M. Nindito, “Financial Statement Fraud: Perspective of the Pentagon Fraud Model in Indonesia,” *Academy of Accounting and Financial Studies Journal*, Jun. 2018, Accessed: Jan. 02, 2021. [Online]. Available: https://www.abacademies.org/abstract/financial-statement-fraud-perspective-of-the-pentagon-fraud-model-in-indonesia-7319.html

[21] European Commission, “SME definition,” *Internal Market, Industry, Entrepreneurship and SMEs - European Commission*, Jul. 05, 2016. https://ec.europa.eu/growth/smes/sme-definition_en (accessed Feb. 12, 2021).

[22] P. Schöber and P. Schmitz, “Hochkonjunktur für die Schatten-IT,” *IT-Business*, Oct. 23, 2020. https://www.it-business.de/hochkonjunktur-fuer-die-schatten-it-a-973554 (accessed Oct. 23, 2020).

[23] ACFE, “Fraud in the Wake of COVID-19: Benchmarking Report,” Jun. 2020. https://www.acfe.com/covidreport.aspx (accessed Jun. 18, 2020).

[24] ACFE, “Fraud in the Wake of COVID-19: Benchmarking Report December Edition,” Dec. 2020. https://www.acfe.com/covidreport.aspx (accessed Mar. 14, 2021).

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

[26] Deloitte Poland, “The impact of COVID-19 on the fraud risks faced by organisations.” Apr. 2020. Accessed: Mar. 14, 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl_COVID_19_Fraud%20Risks_EN_newApril2020.pdf

[27] L. Pasculli, “COVID19-related fraud risks and possible anti-fraud measures (Written evidence submitted to the Treasury Committee on the Economic Impact of Coronavirus),” Coventry University, EIC0792, Jun. 2020. [Online]. Available: https://www.researchgate.net/publication/345760552_COVID19-related_fraud_risks_and_possible_anti-fraud_measures_Written_evidence_submitted_to_the_Treasury_Committee_on_the_Economic_Impact_of_Coronavirus

[28] F. Holzenthal, “IT-gestützte Geldwäsche- und Betrugsbekämpfung in Banken und Versicherungen Mehrwert durch einen holistischen GRC-Ansatz,” *ZRFC*, vol. 3/14, pp. 140–143, 2014.

[29] O. Derksen, “Fraud Analyse von Massendaten in Echtzeit,” in *Big Data - Systeme und Prüfung*, Deggendorfer Forum zur digitalen Datenanalyse, Ed. Berlin: Schmidt, 2013, pp. 45–59.

[30] M. Spindler and H. Kögel, “Erkennung von Versicherungsbetrug mit künstlicher Intelligenz,” Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Berlin, Faktenpapier No.9, 2020.

[31] E. Ulich, “Arbeitssysteme als Soziotechnische Systeme – eine Erinnerung,” *Journal Psychologie des Alltagshandelns*, vol. 6, no. 1, 2013, [Online]. Available: http://www.allgemeine-psychologie.info/cms/images/stories/allgpsy_journal/Vol%206%20No%201/Arbeitssystem_Ulich.pdf

[32] B. Kitchenham, “Guidelines for performing systematic literature reviews in software engineering,” EBSE, Technical Report, Ver. 2.3, 2007. Accessed: Oct. 07, 2017. [Online]. Available: https://pdfs.semanticscholar.org/e62d/bbbbe70cabcde3335765009e94ed2b9883d5.pdf

[33] M. Massaro, J. Dumay, and J. Guthrie, “On the shoulders of giants: undertaking a structured literature review in accounting,” *Accounting, Auditing & Accountability Journal*, vol. 29, no. 5, pp. 767–801, Jan. 2016, doi: 10.1108/AAAJ-01-2015-1939.

[34] A. Fink, *Conducting research literature reviews: from the internet to paper*, Fifth edition. Los Angeles: Sage, 2020.

[35] Committee of Sponsoring Organizations of the Treadway Commission (COSO), “Guidance on Internal Control,” *www.coso.org*, 2013. https://www.coso.org/pages/ic.aspx (accessed Jun. 09, 2021).

[36] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, Mar. 2004.

[37] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[38] A. R. Hevner, “A Three Cycle View of Design Science Research,” *Scandinavian Journal of Information Systems*, vol. 19, no. 2, pp. 87–92, 2007.

[39] M. Shaw, “What Makes Good Research in Software Engineering?,” *STTT*, vol. 4, no. 1, pp. 1–7, 2002.

[40] A. Cleven, P. Gubler, and K. M. Hüner, “Design alternatives for the evaluation of design science research artifacts,” 2009, p. 1. doi: 10.1145/1555619.1555645.

[41] K. Peffers, M. Rothenberger, T. Tuunanen, and R. Vaezi, “Design Science Research Evaluation,” in *Design Science Research in Information Systems. Advances in Theory and Practice*, vol. 7286, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 398–410. doi: 10.1007/978-3-642-29863-9_29.

[42] N. Prat, I. Comyn-Wattiau, and J. Akoka, “Artifact Evaluation in Information Systems Design Science Research - A Holistic View,” Jun. 2014, p. 16.

[43] J. Pries-Heje, R. Baskerville, and J. R. Venable, “Strategies for Design Science Research Evaluation,” *ECIS 2008 Proceedings. 87*, p. 13, 2008.

[44] J. Venable, J. Pries-Heje, and R. Baskerville, “FEDS: a Framework for Evaluation in Design Science Research,” *European Journal of Information Systems*, vol. 25, no. 1, pp. 77–89, Jan. 2016, doi: 10.1057/ejis.2014.36.

[45] T. Wilde and T. Hess, “Forschungsmethoden der Wirtschaftsinformatik: Eine empirische Untersuchung,” *WIRTSCHAFTSINFORMATIK*, vol. 49, no. 4, pp. 280–287, Aug. 2007, doi: 10.1007/s11576-007-0064-z.

[46] K. C. Laudon, J. P. Laudon, and D. Schoder, *Wirtschaftsinformatik: eine Einführung*, 3., Vollständig überarbeitete Auflage. Hallbergmoos/Germany: Pearson, 2016.

[47] N. Döring and J. Bortz, *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*, 5. vollständig überarbeitete, Aktualisierte und erweiterte Auflage. Berlin Heidelberg: Springer, 2016.

[48] P. S. M. dos Santos and G. H. Travassos, “Action Research Can Swing the Balance in Experimental Software Engineering,” in *Advances in Computers*, vol. 83, Elsevier, 2011, pp. 205–276. doi: 10.1016/B978-0-12-385510-7.00005-9.

[49] J. Recker, *Scientific research in information systems: a beginner’s guide*. Heidelberg: Springer, 2013.

[50] N. F. Kock, Ed., *Information systems action research: an applied view of emerging concepts and methods*. New York, N.Y: Springer, 2007.

[51] S. Kelly and J.-P. Tolvanen, *Domain-specific modeling: enabling full code generation*. Hoboken, N.J: Wiley-Interscience : IEEE Computer Society, 2008.

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

[53] S. Phuttima, W. Rueangsirasak, and R. Chaisricharoen, "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)*, Chiang Rai, Thailand, Mar. 2014, pp. 1–7. doi: 10.1109/JICTEE.2014.6804088.

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

[55] S. Dawson, *Internal control/anti-fraud program design for the small business: a guide for companies not subject to the Sarbanes-Oxley Act*. Hoboken: Wiley, 2015.

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

[57] S. Lincke and D. Green, "Combating IS fraud: A teaching case study," in *AMCIS 2012 Proceedings*, Seattle, Washington, Aug. 2012, vol. 2, pp. 578–584. [Online]. Available: http://aisel.aisnet.org/amcis2012/proceedings/ISEducation/2

[58] K. T. Çalıyurt, "Reporting Fraud Using the Fraud-Free Company Model: A Case for the SMEs in Emerging Economies?," in *Emerging Fraud*, K. Çaliyurt and S. O. Idowu, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 3–18. Accessed: Dec. 01, 2020. [Online]. Available: http://link.springer.com/10.1007/978-3-642-20826-3_1

[59] M. Andenmatten, "COBIT 2019 – Das neue Enterprise Governance Modell für Informationen und Technologien," *Disruptive agile Service Management*, Nov. 26, 2018. https://blog.itil.org/2018/11/cobit-2019-das-neue-enterprise-governance-modell-fuer-informationen-und-technologien/ (accessed Jun. 19, 2020).

[60] P. M. Asprion and D. Burda, "COBIT — Enzyklopädie der Wirtschaftsinformatik," *Enzyklopädie der Wirtschaftsinformatik - Online Lexikon*, Feb. 27, 2019. https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/daten-wissen/Grundlagen-der-Informationsversorgung/COBIT (accessed Jun. 19, 2020).

[61] C. Johnson, "Sizing Up the NIST Cybersecurity Framework," *NIST Taking Measure*, Oct. 31, 2016. https://www.nist.gov/blogs/taking-measure/sizing-nist-cybersecurity-framework (accessed Jun. 19, 2020).

[62] N. Keller, "Small and Medium Business Perspectives," *NIST*, Feb. 01, 2018. https://www.nist.gov/cyberframework/small-and-medium-business-perspectives (accessed Jun. 19, 2020).

[63] The MEP National Network, "MANUFACTURERS GUIDE TO CYBERSECURITY - For Small and Medium-Sized Manufacturers," THE MEP NATIONAL NETWORK. Accessed: Nov. 08, 2020. [Online]. Available: https://www.nist.gov/system/files/documents/2019/11/14/mepnn_cybersecurity_guide_10919-508.pdf

[64] ISIS12-Netzwerk, "Handbuch zur effizienten Gestaltung von Informationssicherheit für Kleine und Mittlere Organisationen (KMO)." IT-Sicherheitscluster e. V., 93053 Regensburg, Apr. 27, 2020. [Online]. Available: https://www.isis12.de