IT-COMPLIANCE IN SME - A METHOD FOR THE ADAPTED USE OF FRAMEWORKS

Nico Deistler
KIPS, HTWG Konstanz, Konstanz, Germany
Alfred-Wachtel-Straße 8, 78462 Konstanz

ABSTRACT

The digital transformation of business processes and the integration of IT systems leads to opportunities and risks for small and medium-sized enterprises (SMEs). Risks that can result in a lack of IT Governance, Risk and Compliance (GRC). The purpose of this paper is to present the Design and Evaluation phase of creating an artefact, to reduce these risks. With this, the Design Science Research approach based on Hevner is using. The artefact will be developed by selecting relevant existing frameworks and the identification of SME-specific competencies. The method enables IT-GRC managers to transfer or adapt the frameworks to an SME organizational structure. The results from ten interviews and further three feedback loops showed that the method can be applied in practice and that a tailoring of established frameworks can take place. Contrary to the previous basic orientation of the research, this paper focuses on the concretization of approaches.

KEYWORDS

IT-Compliance, GRC, SME, Design-Science Research

1. INTRODUCTION

Small and medium-sized enterprises (SMEs) are known for their innovative strength and are increasingly confronted with the challenges of digitalization. In order to maintain or expand their competitive advantages, they are forced to actively address this development. The digital transformation of business processes and the greater integration of IT systems bring both, opportunities, and risks. Risks can lead to a lack of IT governance, Risk, and Compliance (GRC), for example with regard to information security and data protection.

A literature review conducted (Deistler and Rentrop 2020) found that existing best practice approaches and frameworks are largely not suitable for SMEs and are therefore not widespread among SMEs. The results of a survey of IT-GRC managers show that the reasons for this status quo are too high costs for IT, limited staff resources, lack of know-how and frameworks that do not fit SME structures. This leads to companies not implementing a holistic approach, but only individual technological measures. In addition, digitalization, cloud applications and cybersecurity already play a major role as drivers (Deistler and Rentrop 2022a). Due to the heterogeneity, it is not reasonable to adapt one of the common standards for all SMEs (Beißel 2017). Instead, general SME-relevant competencies should be abstracted, and a guideline for the selection of appropriate standards should be provided.

The aim of this paper is to develop an artefact for the selection of standards by adapting SME-relevant competencies and existing frameworks to the defined criteria.

In the following chapter, the status quo is presented, from which the problem is specified, and the research question is derived. Subsequently, the research approach with the applied design science methodology is discussed. Next, the case studies are discussed, and the steps and measures developed to design the artefact are outlined and the evaluation of the final methodology is shown. Finally, the results are discussed and implications for practice and research are presented with a summary.

2. STATUS QUO

First, a systematic review of previous research on IT-Compliance was conducted (Deistler and Rentrop 2020). Contributions focus on the topics of IT risk management, IT security, cloud computing, IT governance and the implementation of reference models. Particularly in the case of the contributions in connection with SMEs, it is apparent that these relate almost exclusively to the topics of digitalization and compliance management systems. However, the willingness in companies to actively address measures for IT-Compliance and IT security is low despite an increasing perception of risk (Hillebrand et al. 2017). The reasons and motives for this are, on the one hand, the perceived high costs of external expertise or building up in-house staff, who are also still scarce on the labor market (Deistler and Rentrop 2022a). In addition, the frameworks do not fit the structures in SMEs, which was also described by Johannsen and Kant (2020).

Barriers to implementation exist in small and medium-sized enterprises, especially with more complex frameworks such as COBIT. These lie in the fact that parts of the approach still have to be largely specified by SMEs, and comprehensive requirements and process recommendations have to be handled (Beißel 2017).

Recent empirics show different approaches for SMEs. Henschel and Heinze (2016) present a GRC approach for SMEs, but this largely ignores the specific requirements and the extent of digital transformation that has now also reached SMEs. Knoll and Strahringer (2017, p. 2) define IT-GRC as an integrated planning and control view of a company's opportunities and risks arising from the use of information as a production factor in the age of digitalization. Their approach provides a good orientation, but still requires "tailoring" for SMEs. Beißel (2017) uses the example of IT risk to show how existing frameworks can be meaningfully differentiated. Johannsen and Kant (2020) developed a competency-based approach to perceive, measure, and manage IT governance, risk, and compliance management in SMEs.

The goal of this paper is to develop an artefact for selecting appropriate standards by abstracting SME-relevant competencies and tailoring existing approaches and standards to the defined characteristics. Based on the problem definition and the state of research, the following research question can be derived: How can an IT GRC approach be designed to leverage existing frameworks and address specific needs of SMEs?

3. RESEARCH APPROACH

This chapter describes the methodological approach for developing and evaluating the artefact for selecting appropriate standards in SMEs.

The work has been conducted according to the design science research approach of Hevner (Hevner et al. 2004). The goal is to develop and evaluate an artefact in order to address the research question. First, in the Problem Identification & Objectives phase, a literature review and expert interviews were used to identify and clearly describe the relevant IT problem and to demonstrate the research gap. This is followed by the Design & Demonstration phase, in which an artefact, in this case a method, is developed to adequately implement IT-Compliance in SMEs. This initial approach was presented, discussed and adaptations directly incorporated. Further evaluation was conducted with the help of two case studies by practice partners, which are discussed in the next section. Here, the artefact was deployed and tested for functionality, quality, and effectiveness. The two phases of design & demonstration and evaluation run iteratively until the final artefact is developed.

3.1 Conducting the Case Studies

The ideal type of an evaluation of an artefact consists of its complete application in practice (Pries-Heje et al. 2008). However, this does not take place in the context of this work. For pure practicality reasons, the author lacks access to an IT organization with the authority necessary for an organizational design. The limited duration and resources of the work also stand in the way of such an ideal-typical approach to evaluation. Therefore, conducting comparative case studies according to Yin (2014) was chosen to evaluate the artefact. Accordingly, expert interviews are conducted, with the help of which a broad expertise, which the experts have acquired from their professional practice, is queried, and presented in a representative manner.

Furthermore, the instrument of triangulation was applied (Yin 2014). The interviews took place in the period from August to October 2022 and had different target groups and objectives as their purpose.

On the one hand, the methodological approach was to be evaluated. For this purpose, ten experts from compliance-relevant positions in small and medium-sized companies, scientists, and consultants from the field of business informatics were interviewed (see Chapter 4.5).

Second, the implemented design object was to be evaluated. In order to keep the number of cases manageable for the scope of the work, these were limited to four, one SME per archetype and one external consultant (see Chapter 4.6).

4. A METHOD FOR THE ADAPTED USE OF FRAMEWORKS IN SME

Starting from the Problem Identification & Objectives phase, this chapter presents the development and evaluation of the artefact. The methodological procedure is shown graphically in Figure 1. An essential component are the structural elements as well as SME relevant competencies. These were selected based on existing literature and serve as structure-giving elements for the artefact. The derivation and definition are explained in advance.

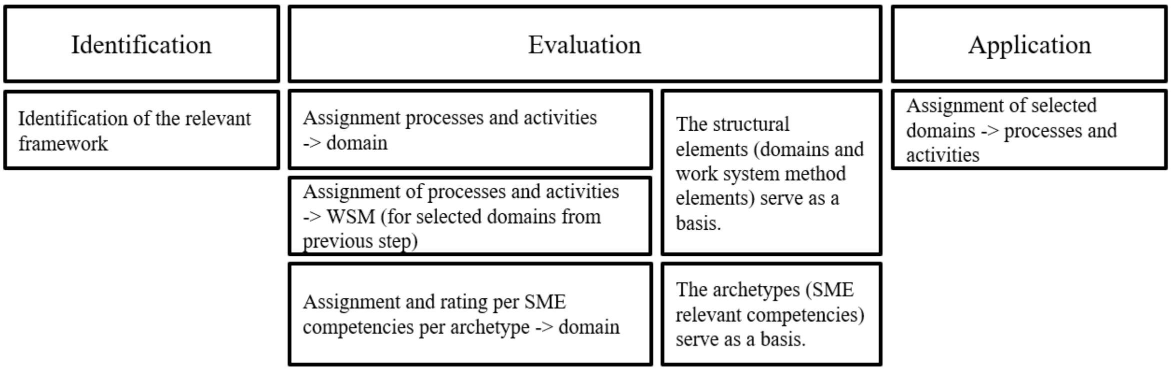

Identification
Evaluation
Application
Identification of the relevant framework
Assignment processes and activities -> domain
Assignment of processes and activities -> WSM (for selected domains from previous step)
Assignment and rating per SME competencies per archetype -> domain
The structural elements (domains and work system method elements) serve as a basis.
The archetypes (SME relevant competencies) serve as a basis.
Assignment of selected domains -> processes and activities

Figure 1. Methodical Approach

4.1 Definition of the Structural Elements

With the help of the structural elements, the individual processes and activities are to be brought into a uniform comparative structure, detached from the respective focus of a framework. In order to derive the appropriate elements, it is necessary to take a look at the strategic alignment of business and IT, which is regarded as an essential prerequisite for IT to contribute to business success. Henderson and Venkatraman have developed a model for this purpose to clarify how alignment works. This is divided into an external and internal perspective and contains, among other things, the positions Infrastructure, Processes, Capabilities, Competencies, Governance, and Scope (Henderson and Venkatraman 1989). Weill & Ross propose the differentiation into IT Principles, Architecture, Infrastructure, Business requirements, and Investments (Weill and Ross 2004). However, this proves to be not granular enough in practice, as the area of infrastructure is very comprehensive. Accordingly, Rentrop (Rentrop 2022) proposes a division into seven domains: IT Principles (subdomain: Stakeholders, Strategic Role, Fundamental Alignment of IT), Governance of IT (subdomain: Strategy, Budgeting, Investment Decisions, Cost Management), Architecture (subdomain: Design of the Development Plan, Standardization, Data Governance), Sourcing (subdomain: Sourcing Strategy, Supplier Selection, Relationship Design), Security, Risk & Compliance, Organization and Personnel (subdomain: IT in the Enterprise, IT within, Personnel Decisions) and IT Services.

The domains mentioned cover all areas and are therefore suitable as structure-giving elements for the further steps.

However, a further structural element is necessary, which takes into account in particular the aspect that SMEs have specific challenges, for example with regard to employees and costs. In addition, there are differences by industry and by small and medium-sized enterprises (Deistler and Rentrop 2022b).

For this reason, Alter's Work System Method (WSM) is suitable to differentiate and classify them. The Work System Method is an approach to analyzing systems in organizations, whether or not IT plays a significant role. This method is more broadly applicable than techniques designed to specify detailed software requirements, and it is more prescriptive and powerful than domain-independent system analysis methods such as the Soft System Method (Alter 2002). For this paper, we do not use all the elements Alter uses in his model but limit ourselves to the coherent elements of processes and activities, people, information, and technology that are relevant to us. These are explained below.

Processes and activities: Steps by which work is performed within a work system. In our case, these map to the relevant Objectives (COBIT 2019 and ISO/IEC 27001:2013) and Practices (ITIL4).

People (P): the people who perform at least some of the work in the business process are the people of the work system.

Information (I): Information includes codified and non-codified information that is used and created as people perform their work.

Technologies (T): Technologies include the tools and techniques used by the people of the work system as they perform their work (Alter 2002).

4.2 Definition of SME Relevant Competencies

In a next step, a further classification is made according to SME-relevant competencies. To this end, a classification of company sizes within SMEs must be made first, as this has a significant influence on the design of an IT GRC approach. This is based on a common understanding of the term. According to this, a company with fewer than 9 employees is defined as a micro enterprise, with 10 to 49 employees as a small enterprise, and with 50 to a maximum of 249 employees as a medium-sized enterprise (EU Commission 2005). However, this classification does not go far enough for an IT GRC approach. The presence of technology in the company also has a significant influence. It can be assumed that there is a correlation between the design or maturity of the technology and the number of stakeholders. In order to incorporate this into the model, three archetypes are developed based on Rohlfing and Funck (2002) and COBIT2019 Focus Area SMEs (ISACA 2018), according to which a differentiation within SMEs is possible and thus the different characteristics in SMEs are taken into account, as shown in Table 1.

Table 1. Archetypes

Archetype	Competencies
1	small enterprise, IT mainly outsourced, no clear responsibility for the IT, limited in-house IT skills/capacity, relative high-risk tolerance, because of their low-risk capacity, simple command structure and limited organizational structures in place
2	small enterprise, IT mainly in-house, IT department in place, outsource more complex tasks, limited in-house IT skills and/or capacity, relative high-risk tolerance, because of their low-risk capacity, simple command structure and limited organizational structures in place
3	medium-sized enterprise, heterogeneous IT-landscape, and IT department in place, aim more to buy (and potentially tailor) than to build themselves, outsource more complex tasks

Furthermore, current trends and developments are to be considered from the Problem Identification & Objectives phase. These are Information Security Awareness, Cybersecurity, Cloud Compliance and Data Protection (Deistler and Rentrop 2022a).

After describing the structure-giving elements that serve as a basis, the next step is the identification, evaluation, and application phases. It should be added at the outset that in this work, not one framework but three widely used frameworks were selected and evaluated due to their greater informative value (Deistler and Rentrop 2022a). Therefore, the next step, the mapping of the selected frameworks can be seen as optional for the actual method.

4.3 Mapping of the Selected Frameworks

The established and continuously revised COBIT 2019 framework serves as a reference framework, which is used for structuring and mapping other standards. Mappings from COBIT 2019 to ITIL4 (Hartawan and Suroso 2017) and ISO/IEC 27001:2013 (Yasin et al 2020) have already been performed. This was done using the ArchiMate Language according to Lankhorst. ArchiMate is an open and independent modeling language for enterprise architecture that can represent the description, analysis, and visualization of architecture within and between business units in an unambiguous manner (Lankhorst 2009). Thus, a comparability of the different frameworks was worked out, which is shown in Figure 2 (part "Mapping COBIT2019, ITIL4, ISO/IEC 27001:2013" of the table).

4.4 Step 1: Identification of the Relevant Frameworks

For the identification of the relevant frameworks, the complete existence of the individual framework, in particular the respective requirements, which are also called objectives, practices, or scope, is relevant.

ISO/IEC 27001:2013 and COBIT 2019 are both frameworks that address how organizations manage and monitor their IT systems. COBIT has clearly defined objectives and governance structures, while ISO/IEC 27001:2013 requires that information security objectives related to confidentiality, integrity and availability be defined according to organizational context. The difference between these two standards is that ISO/IEC 27001:2013 focuses mainly on security, while COBIT 2019 looks at IT as a whole and takes a functional perspective. In ITIL4, the focus is on the operational view and assessment of the security process, with an emphasis on information security. ITIL4 and ISO 27001:2013 primarily define how requirements should be implemented, COBIT 2019 primarily defines what should be implemented. COBIT 2019 is therefore at a higher level. In highly simplified terms, ITIL4 and ISO/IEC 27001:2013 are operational and tactical, while COBIT 2019 is more strategic.

4.5 Step 2: Evaluation of the Relevant Frameworks

In the evaluation phase, the processes and activities are first assigned to domains and based on this, the selected domains are assigned to the WSM elements. In the last step, the assignment is made to the domains with the help of a rating of the SME competencies per archetype. These assignments and the procedure were evaluated in the case studies and are presented in detail below.

In order to perform an assignment of the processes and activities to the defined seven domains in the first step, techniques of the ArchiMate Language (Lankhorst 2009) and the evidence suggested from the case study research (Yin 2014), such as manuals, process models and service catalogs, were used. In detail, all processes and activities from the frameworks were individually sifted and assigned to the respective domain. Multiple assignments are possible (see marked green in Figure 2). The ten experts reviewed and supplemented the results of this preliminary stage. The data collection procedure used for each interview partner was based on the specific assignment of processes and activities to domains in the form of a matrix prepared in advance. Deviations were identified, re-evaluated, and adjusted.

On this basis, the next step was to assign the selected processes and activities and associated domains to the WSM elements of people, information, and technology. For a better understanding, for the activity and process EDM01 from COBIT 2019, a domain mapping to IT principles was developed. As a result, it must be evaluated for this domain whether people, information or/and technology are required to achieve the objective. Multiple assignments may occur. For example, a process, such as APO05 from COBIT 2019, may require multiple processes and activities, such as IT principles, management of IT, and architecture. This results in multiple people being required for these processes, and thus multiple assignments to people. The personal intensity to cover this process is thus reflected. The result of these assignments is shown with an "x" in Figure 2.

In the final step, the three archetypes were evaluated based on their proficiencies and assigned to the corresponding domains. A two-level scoring model was used: high (h; +1) for indicating that this domain is appropriate and important to express and should be mapped as a priority, and low (l; -1) for indicating that this domain should not be included. No rating means that the domains are neutral for these proficiencies and thus a rating of 0 is assigned. For example, for the expression "IT mainly outsourced" in archetype 1, the domain Sourcing was rated as high because it can be assumed that the topics such as strategies of IT (cloud application, integration) and selection of suppliers/vendors can be classified as an important characteristic for this. The IT services domain, however, can be considered irrelevant, as the operation of the IT systems (with its sub-areas such as: change management, software development) is primarily the responsibility of the service provider in the case of outsourcing. Due to these qualitative measurements, we have a subjective interpretation here. However, in order to achieve high validity, this was discussed and adjusted several times with all ten interviewees. The summarized result is shown in the following table for archetype 1 in full and the results for archetypes 2 and 3 in the bottom row.

Table 2. Assignment and Rating to Archetype 1 in Detail and Archetype 2 and 3 in Summary

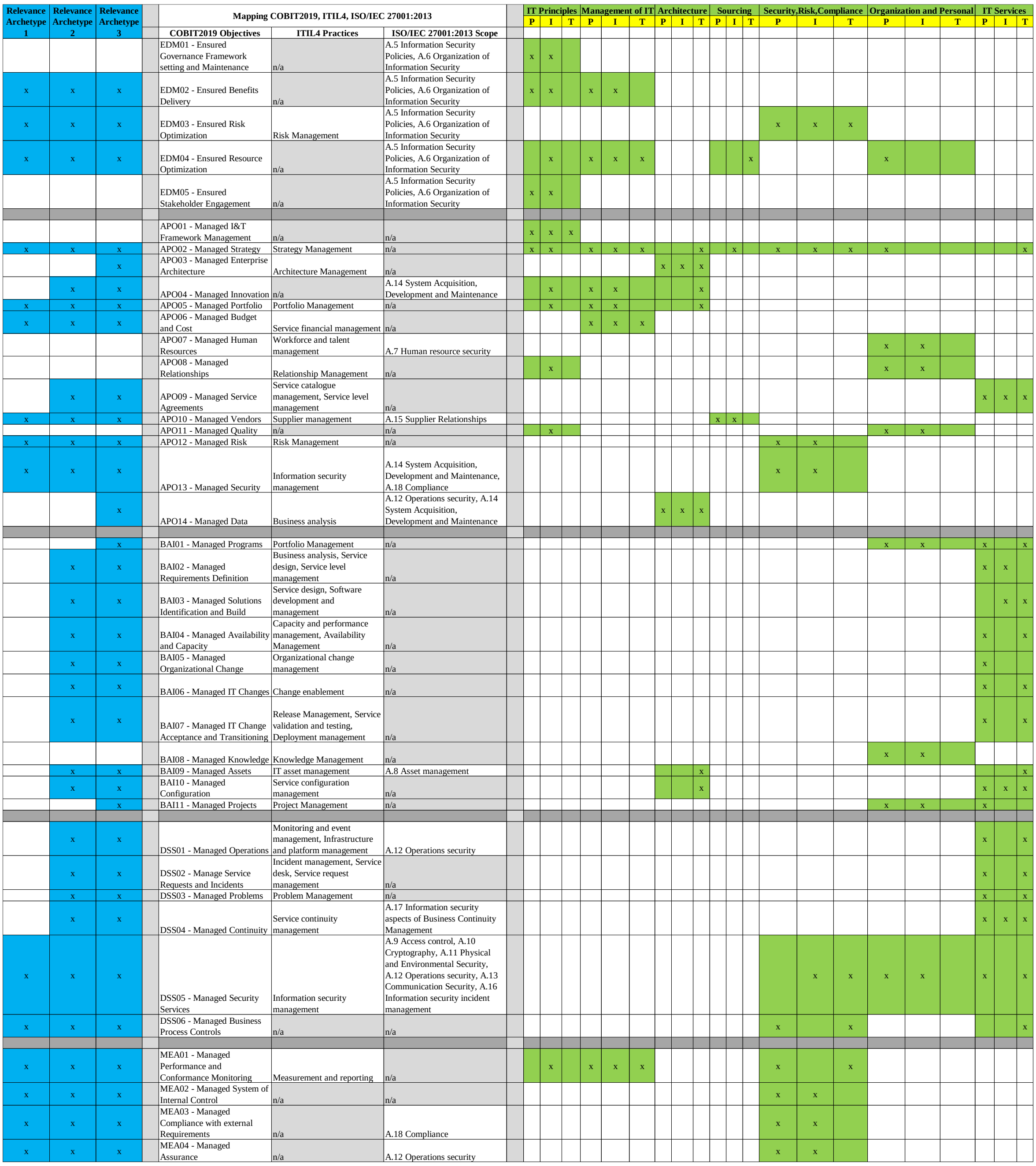
Archetype 1	**IT Principles**	**Management of IT**	**Architecture**	**Sourcing**	**Security, Risk & Compliance**	**Organization and Personal**	**IT Services**
small enterprise	l	h	l	h	h	l	l
IT mainly outsourced				h			l
no clear responsibility for the IT		h					
limited in-house IT skills/capacity						l	
relative high risk tolerance, because of their low-risk capacity					h		
simple command structure and limited organizational structures in place					h	l	
Information Security Awareness, Cyber Security, Cloud Compliance and Data protection					h		
Result Archetype 1	**-1**	**2**	**-1**	**3**	**4**	**-3**	**-2**
Result Archetype 2	**0**	**2**	**-1**	**3**	**4**	**-3**	**2**
Result Archetype 3	**0**	**2**	**1**	**4**	**3**	**-2**	**4**

Finally, each interviewee assigned the relevant processes and activities per archetype. The final step is the application of the relevant framework.

4.6 Step 3: Application of the Relevant Frameworks

In the further procedure, the final assignments were made based on the ratings from Table 1. Domains with a rating greater than 0 (see "Result" in Table 1) were classified as relevant and included in the target object (highlighted in blue in Figure 2), domains with a rating below 0 were considered as not relevant for this archetype. If a process such as EDM02 covers multiple domains, such as the domain IT Principles and Management of IT, which were rated -1 and +2, this business process was included because the relevance was clearly highlighted with +2. However, if a process such as BAI01 is assigned to two domains and one of them is Organization & Personal, which was rated -3 in archetype 2, this process has not been included because it is assumed that this is difficult to apply. This process was performed for all three archetypes.

Subsequently, three experts who had already been involved in the implementation, customization and operation related to COBIT2019/ITIL/ISO27001:2013 in their organization and could describe the operation and background based on their recollection and experience were interviewed. In doing so, each expert represented an archetype. The data collection procedure used for each case was based on a guideline. A pilot case study with a consultant was also incorporated to improve the data collection process. The entry point was formed by general questions about the framework of the organization and the project/implementation of the relevant framework. In this context, collected experiences of the respondents should be identified. In the next step, the target object (artefact per archetype) was mirrored to the experiences of the expert and feedback on feasibility was requested. A positive/negative test was also carried out, for example, it was checked whether the target object of archetype 1 was suitable, but it was also checked whether archetype 2 or 3 would also be suitable. Accompanying the expert interviews, a triangulation of the information thus collected was performed. At Expert A, for example, the documentation of an internal audit was inspected, and it was seen which processes and activities from the ISO standard were assessed as not effective. Likewise, project presentations were viewed at Expert C, which manifested the statement that personnel-intensive processes were minimized, and projects were set up to automate them with the help of IT applications. Each interviewee was interviewed a second time to confirm the results and to clarify the descriptions.



Relevance Archetype 1	Relevance Archetype 2	Relevance Archetype 3	Mapping COBIT2019, ITIL4, ISO/IEC 27001:2013			IT Principles			Management of IT			Architecture			Sourcing			Security,Risk,Compliance			Organization and Personal			IT Services		
			COBIT2019 Objectives	ITIL4 Practices	ISO/IEC 27001:2013 Scope	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T
			EDM01 - Ensured Governance Framework setting and Maintenance	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x	🟩																		
x	x	x	EDM02 - Ensured Benefits Delivery	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x	🟩	x	x	🟩															
x	x	x	EDM03 - Ensured Risk Optimization	Risk Management	A.5 Information Security Policies, A.6 Organization of Information Security													x	x	x						
x	x	x	EDM04 - Ensured Resource Optimization	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	🟩	x	🟩	x	x	x				🟩	🟩	x				x	🟩	🟩			
			EDM05 - Ensured Stakeholder Engagement	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x	🟩																		
			APO01 - Managed I&T Framework Management	n/a	n/a	x	x	x																		
x	x	x	APO02 - Managed Strategy	Strategy Management	n/a	x	x	🟩	x	x	x	🟩	🟩	x	🟩	x	🟩	x	x	x	x	🟩	🟩	🟩	🟩	x
		x	APO03 - Managed Enterprise Architecture	Architecture Management	n/a							x	x	x												
	x	x	APO04 - Managed Innovation	n/a	A.14 System Acquisition, Development and Maintenance	🟩	x	🟩	x	x	🟩	🟩	🟩	x												
x	x	x	APO05 - Managed Portfolio	Portfolio Management	n/a	🟩	x	🟩	x	x	🟩	🟩	🟩	x												
x	x	x	APO06 - Managed Budget and Cost	Service financial management	n/a				x	x	x															
			APO07 - Managed Human Resources	Workforce and talent management	A.7 Human resource security																x	x	🟩			
			APO08 - Managed Relationships	Relationship Management	n/a	🟩	x	🟩													x	x	🟩			
	x	x	APO09 - Managed Service Agreements	Service catalogue management, Service level management	n/a																			x	x	x
x	x	x	APO10 - Managed Vendors	Supplier management	A.15 Supplier Relationships										x	x	🟩									
			APO11 - Managed Quality	n/a	n/a	🟩	x	🟩													x	x	🟩			
x	x	x	APO12 - Managed Risk	Risk Management	n/a													x	x	🟩						
x	x	x	APO13 - Managed Security	Information security management	A.14 System Acquisition, Development and Maintenance, A.18 Compliance													x	x	🟩						
		x	APO14 - Managed Data	Business analysis	A.12 Operations security, A.14 System Acquisition, Development and Maintenance							x	x	x												
		x	BAI01 - Managed Programs	Portfolio Management	n/a																x	x	🟩	x	🟩	x
	x	x	BAI02 - Managed Requirements Definition	Business analysis, Service design, Service level management	n/a																			x	x	🟩
	x	x	BAI03 - Managed Solutions Identification and Build	Service design, Software development and management	n/a																			🟩	x	x
	x	x	BAI04 - Managed Availability and Capacity	Capacity and performance management, Availability Management	n/a																			x	🟩	x
	x	x	BAI05 - Managed Organizational Change	Organizational change management	n/a																			x	🟩	🟩
	x	x	BAI06 - Managed IT Changes	Change enablement	n/a																			x	🟩	x
	x	x	BAI07 - Managed IT Change Acceptance and Transitioning	Release Management, Service validation and testing, Deployment management	n/a																			x	🟩	x
			BAI08 - Managed Knowledge	Knowledge Management	n/a																x	x	🟩			
	x	x	BAI09 - Managed Assets	IT asset management	A.8 Asset management							🟩	🟩	x										🟩	🟩	x
	x	x	BAI10 - Managed Configuration	Service configuration management	n/a							🟩	🟩	x										x	x	x
		x	BAI11 - Managed Projects	Project Management	n/a																x	x	🟩	x	🟩	🟩
	x	x	DSS01 - Managed Operations	Monitoring and event management, Infrastructure and platform management	A.12 Operations security																			x	🟩	x
	x	x	DSS02 - Manage Service Requests and Incidents	Incident management, Service desk, Service request management	n/a																			x	🟩	x
	x	x	DSS03 - Managed Problems	Problem Management	n/a																			x	🟩	x
	x	x	DSS04 - Managed Continuity	Service continuity management	A.17 Information security aspects of Business Continuity Management																			x	x	x
x	x	x	DSS05 - Managed Security Services	Information security management	A.9 Access control, A.10 Cryptography, A.11 Physical and Environmental Security, A.12 Operations security, A.13 Communication Security, A.16 Information security incident management													🟩	x	x	x	x	🟩	x	🟩	x
x	x	x	DSS06 - Managed Business Process Controls	n/a	n/a													x	🟩	x				🟩	🟩	x
x	x	x	MEA01 - Managed Performance and Conformance Monitoring	Measurement and reporting	n/a	🟩	x	🟩	x	x	x							x	🟩	x						
x	x	x	MEA02 - Managed System of Internal Control	n/a	n/a													x	x	🟩						
x	x	x	MEA03 - Managed Compliance with external Requirements	n/a	A.18 Compliance													x	x	🟩						
x	x	x	MEA04 - Managed Assurance	n/a	A.12 Operations security													x	x	🟩						

Figure 2. Results per Archetype

5. DISCUSSION OF RESULTS

If the number of assignments of the WSM elements, personal (47), information (42) and technology (33) in the initial state of the framework are considered and these are compared with the assignments in the developed archetypes, the following results can be determined. For archetype 1, the result of assignments of people (22), information (22), and technology (15) that correspond to the characteristics of this archetype. The WSM assignments for archetype 2 and 3 also confirm a reduction in the human element relative to the baseline condition. This addresses the problem of lack of employee resources in SMEs. Furthermore, the element Technology (32) has the highest number of assignments in archetype 3, which correlates with the characteristics of this archetype. The same issue can be seen with the number of relevant processes and activities, so of the 40 relevant processes and activities in the baseline condition, 15 have been evaluated as relevant in archetype 1, 29 in archetype 2, and 33 in archetype 3.

The results are seen as consistently helpful among interviewees. The method enables those responsible for IT-GRC to transfer or adapt the frameworks to an SME organizational structure. By focusing on SME-relevant competencies in the developed method, processes and activities are prioritized. Risks can thus be reduced because the (missing) capacities are used in a more goal-oriented manner. Finally, the flexibility and innovative capacity for which SMEs are known should be maintained and not imposed on processes and activities that are easy to implement for large companies but bureaucratize SMEs.

The steps outlined examined the utility, quality, and effectiveness of the method developed (Hevner et al. 2004). The successful simulation in the three archetypes proves the usefulness of the method. This can be seen in the execution of each step (Peffers et al. 2008) and in the evaluation of each case by the experts involved. With the final design, the research question can be answered.

Contrary to the basic orientation of the research so far, this paper focuses on the concretization of approaches. Thus, the results contribute to the extension of the literature as it is based on basing approaches and generates a possibility to evaluate them. Moreover, the criteria of the evaluation are independent of technology and organizational structure.

6. CONCLUSION

The results of ten interviews and further three feedback loops showed that the method can be applied in practice, that established frameworks can be "tailored", and that it provides SMEs with recommendations for action to achieve a certain level of IT-Compliance. In addition, the method can be carried out with little effort.

However, the selection of cases could have limitations. Generalization could be improved by studying even more cases from other industries and with a different organizational structure. In addition, a full application could be tested in practice. It can also be assumed that there is a certain bias towards positive extreme cases, as it can be assumed that such companies agreed to participate where the projects are seen as successful. Moreover, our study is based exclusively on qualitative data, as allocations are difficult to quantify.

In addition to the described competencies, a company may need to consider other individual characteristics that may lead to a further archetype and thus change the result. Furthermore, the omission of processes and activities should be critically reviewed again by each company to see if they are really not necessary, as the frameworks usually represent a holistic approach. We are sure that this work will contribute to theory and practice in the field of IT-Compliance in SMEs.

In summary, the paper can be an impetus for SMEs to raise their awareness with regard to IT GRC and provides recommendations for action for an adapted minimum level of IT-Compliance.

REFERENCES

Alter, S. 2002. The Work System Method for Understanding Information Systems and Information Systems Research. In: *Communications of the Association for Information Systems*, Vol. 9, Article 6.

Beißel, S. 2017. Differenzierung von Rahmenwerken des IT-Risikomanagements. In: *HMD Praxis der Wirtschaftsinformatik*, Vol. 1, S. 54:37–54.

Deistler N., Rentrop C. 2020. IT-Compliance in KMU – State of the art. In *HMD Praxis der Wirtschaftsinformatik*, Vol. 57, pp 1047-1057.

Deistler, N., Rentrop, C. 2022a. IT-Compliance in KMU – Experteninterviews zum Status quo. In *Wirtsch Inform Management,* https://doi.org/10.1365/s35764-021-00380-5.

Deistler, N., Rentrop, C., 2022b. A Method for an IT-GRC Approach in SMEs – Design Phase. In *PACIS 2022 Proceedings*. 316.

EU-Commission, 2005. Definition of SMEs. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN. Access on: 11.02.2022

Hartawan, F., Suroso, J. 2017. Information Technology Services Evaluation Based ITIL V3 2011 and COBIT 5. In *Center for Data and Information. In Intelligent Information and Database Systems*. 9th Asian Conference.

Henderson, J. C., Venkatraman, N. 1989. Strategic alignment. A framework for strategic information technology management. In: *CISR WP No. 190*. Massachusetts, USA.

Hevner, A., Salvatore M., Jinsoo P., Sudham R. 2004. Design Science in Information Systems Research. In: *MIS Quarterly* (28:1), S. 75-105.

Hillebrand A, et al, 2017. Aktuelle Lage der IT-Sicherheit in KMU.WIK https://www.wik.org/fileadmin/Sonstige_ Dateien/ IT-Sicherheit_in_KMU/ __2_.pdf. Access on: 28. Nov. 2020.

Henschel T., Heinze I. 2016. Governance, Risk und Compliance im Mittelstand, Praxisleitfaden für gute Unternehmensführung. Erich Schmidt Verlag, Berlin, Deutschland.

ISACA 2018 Cobit 2019: Einführung und Methodik. ISACA.org, USA.

Johannsen A., Kant D. 2020. IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU. In: *HMD Praxis der Wirtschaftsinformatik*, Vol. 57, S. 1058–1074.

Knoll M., Strahringer S. 2017. IT-GRC-Management im Zeitalter der Digitalisierung. In: *Knoll M, Strahringer S (Hrsg) IT-GRC-Management* –. Springer Vieweg, Wiesbaden, Deutschland, S. 1–24.

Lankhorst, M. 2009. Enterprise Architecture at work. In *The Enterprise Engineering*, Springer Berlin, Deutschland.

Peffers, K., Tuunanen T., Rothenberger A., Chatterjee S. 2008. A Design Science Research Methodology for Information Systems Research. In: *Journal of Management Information Systems* (24:3), S. 45-77.

Pries-Heje, J., Baskerville, R., Venable, J. 2008. Strategies for Design Science Research Evaluation. In: *Proceedings of the ECIS 2008 conference*, Galway, Ireland.

Rentrop C. 2022. IT-Governance. Erfolgsfaktor für die digitale Transformation. Erich Schmidt, Berlin, Deutschland.

Rohlfing, M., Funck, D., 2002. SMEs Kritische Diskussion quantitativer und qualitativer Definitionsansätze. In: *IMS-Forschungsberichte Nr.7*. Universität Göttingen. Deutschland.

Weill, P., Ross, J. W. 2004. IT governance. How top performers manage IT decision rights for superior results. In: *Harvard Business School*. Boston, Massachusetts. USA.

Yasin, M., et al. 2020. Designing Information Security Governance Using COBIT 2019 Framework and ISO 27001:2013. In *14th International Conference on Telecommunication Systems, Services, and Applications (TSSA).*

Yin, R. K. 2014. Case study research: Design and methods (5th ed.), Los Angeles, CA: Sage Publications.