HMD Praxis der Wirtschaftsinformatik
https://doi.org/10.1365/s40702-023-00974-0

IT-Compliance in KMU – Eine Methode zum angepassten Einsatz von Rahmenwerken

Nico Deistler

Eingegangen: 15. November 2022 / Angenommen: 27. März 2023

Zusammenfassung Die digitale Transformation von Geschäftsprozessen und die stärkere Integration von IT-Systemen führen zu Chancen und Risiken für kleine und mittlere Unternehmen (KMU). Risiken, die zu fehlender IT-Governance, Risk und Compliance (GRC) führen können. Ziel dieses Beitrags ist es, die Design- und Evaluierungsphase der Erstellung eines Artefakts darzustellen. Dabei wird der Design Science Research Ansatz nach Hevner verwendet. Das Artefakt wird für die Auswahl von Standards entwickelt, indem KMU-relevante Ausprägungen und bestehende Rahmenwerke auf die definierten Kriterien angepasst werden

Schlüsselwörter IT-Compliance · GRC · KMU · Design-Science Research

IT-Compliance in SME—a method for the adapted use of frameworks

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 conditions

Keywords IT-compliance · GRC · SME · Design-science research

✉ Nico Deistler
KIPS – Konstanzer Institut für Prozesssteuerung, HTWG Konstanz,
Alfred-Wachtel-Straße 8, 78462 Konstanz, Deutschland
E-Mail: nico.deistler@online.de

Published online: 03 May 2023

1 Einleitung

Kleine und mittlere Unternehmen (KMU) sind für ihre Innovationskraft bekannt und werden zunehmend mit den Herausforderungen der Digitalisierung konfrontiert. Um ihre Wettbewerbsvorteile zu erhalten und auszubauen, sind sie gezwungen, sich aktiv mit dieser Entwicklung auseinanderzusetzen. Die digitale Transformation von Geschäftsprozessen und die stärkere Integration von IT-Systemen bringen sowohl Chancen als auch Risiken. Risiken können zu fehlender IT-Governance, Risk und Compliance (GRC) führen, zum Beispiel in Bezug auf Informationssicherheit und Datenschutz.

Eine durchgeführte Literaturanalyse (Deistler und Rentrop 2020) hat ergeben, dass die bisherigen Best-Practice-Ansätze und Rahmenwerke größtenteils nicht mittelstandstauglich und daher in KMU nicht weit verbreitet sind. Die Ergebnisse einer Befragung von IT-GRC-Verantwortlichen zeigen, dass die Gründe für diesen Status quo zu hohen Kosten für die IT, begrenzte Mitarbeiterressourcen, fehlendes Know-how und nicht zu KMU-Strukturen passende Rahmenwerke sind. Dies führt dazu, dass die Unternehmen keinen ganzheitlichen Ansatz, sondern nur einzelne technologische Maßnahmen umsetzen. Zudem spielen Digitalisierung, Cloud-Anwendungen und Cybersicherheit als Treiber bereits eine große Rolle (Deistler und Rentrop 2022a). Aufgrund der Heterogenität ist es nicht sinnvoll, einen einheitlichen Standard für alle KMU zu adaptieren (Beißel 2017). Stattdessen sollten KMU-relevante Ausprägungen abstrahiert und ein Leitfaden für die Auswahl geeigneter Standards bereitgestellt werden.

Ziel dieses Beitrags ist es, ein Artefakt für die Auswahl von Standards zu entwickeln, indem KMU-relevante Ausprägungen und bestehende Rahmenwerke auf die definierten Kriterien angepasst werden.

2 Status Quo

Zunächst erfolgte eine systematische Sichtung früherer Forschungsarbeiten zu IT-Compliance nach Webster and Watson (2002). Herangezogen wurden hierfür die einschlägigen wissenschaftlichen Internetdatenbanken, mit dem Fokus auf Zeitschriften, Konferenzen und Monographien aus dem deutschsprachigen Raum sowie ausgewählten internationalen Zeitschriften (Senior Scholar's Basket of IS Journals) im Bereich der Information Systems (IS). Im ersten Schritt wurde die relevante Literatur nach den Suchwörtern Compliance, IT-Compliance, KMU und mittelständische Unternehmen untersucht. Aus dieser Treffermenge sind mehr als 100 Veröffentlichungen extrahiert worden. Im nächsten Schritt wurden die Beiträge auf eine tatsächliche Compliance-Relevanz untersucht und thematische Gruppierungen gebildet. Im weiteren Verlauf wurden Publikationen identifiziert, die konkrete Themenfelder von IT-Compliance in Verbindung mit KMU beschreiben (Deistler und Rentrop 2020).

Beiträge fokussieren sich auf die Themen IT-Risikomanagement, IT-Security, Cloud Computing, IT-Governance und der Implementierung von Referenzmodellen. Vor allem bei den Beiträgen in Verbindung mit KMU zeigt sich, dass sich diese fast ausschließlich auf die Themen Digitalisierung und Compliance-Management-

Systeme beziehen. Die Bereitschaft in den Unternehmen aktiv Maßnahmen zur IT-Compliance und IT-Sicherheit anzugehen, ist trotz einer steigenden Risikowahrnehmung jedoch gering (Hillebrand et al. 2017). Die Gründe und Motive hierzu sind zum einen die gefühlt hohen Kosten durch externes Know-How oder den Aufbau von eigenen Mitarbeitern, die zudem noch rar am Arbeitsmarkt sind (Deistler und Rentrop 2022a). Zudem passen die Rahmenwerke nicht zu den Strukturen in KMU, was auch von Johannsen und Kant (2020) beschrieben wurde.

Es existieren gerade bei komplexeren Rahmenwerken wie COBIT Einführungsbarrieren in kleinen und mittleren Unternehmen. Diese liegen darin, dass Teile des Ansatzes noch weitgehend von KMU ausspezifiziert werden müssen, und umfassende Anforderungen und Prozessempfehlungen beherrscht werden müssen (Beißel 2017).

Die jüngere Empirie zeigt verschiedene Ansätze für KMU. Henschel und Heinze (2016) präsentieren einen GRC-Ansatz für den Mittelstand, dieser ignoriert jedoch weitgehend die besonderen Anforderungen und das Ausmaß der digitalen Transformation, das mittlerweile auch KMU erreicht hat. Knoll und Strahringer (2017, S. 2) definieren IT-GRC als eine integrierte Planungs- und Kontrollsicht von Chancen und Risiken eines Unternehmens, die sich aus der Nutzung von Informationen als Produktionsfaktor im Zeitalter der Digitalisierung ergeben. Ihr Ansatz gibt eine gute Orientierung, bedarf aber für KMU noch eines „Tailorings“. Am Beispiel des Bereichs IT-Risk wird von Beißel (2017) aufgezeigt, wie vorhandene Rahmenwerke sinnvoll differenziert werden können. Johannsen und Kant (2020) entwickelten einen kompetenz-orientierten Ansatz zur Wahrnehmung, Messung und Steuerung des IT-Governance, Risiko- und Compliance-Managements in KMU.

Ziel dieser Arbeit ist es, ein Artefakt für die Auswahl geeigneter Standards zu entwickeln, indem KMU-relevante Ausprägungen abstrahiert und bestehende Ansätze und Standards auf die definierten Ausprägungen zugeschnitten werden. Auf Basis der Problemstellung und des Forschungsstands lässt sich folgende Forschungsfrage ableiten: *Wie kann ein IT-GRC-Ansatz so gestaltet werden, dass er die bestehenden Rahmenwerke nutzt und den spezifischen Bedürfnissen von KMU gerecht wird?*

3 Forschungsansatz

In diesem Kapitel wird der methodische Ansatz für die Entwicklung und Evaluierung des Artefaktes zur Auswahl geeigneter Standards in KMU beschrieben.

Das Vorhaben ist nach dem Design Science Forschungsansatz nach Hevner (Hevner et al. 2004) durchgeführt worden. Ziel ist die Entwicklung und Evaluierung eines Artefakts, um damit die Forschungsfrage zu adressieren. Zunächst erfolgte in der Phase Problem Identification & Objectives mithilfe einer Literaturstudie (Deistler und Rentrop 2020) und Experteninterviews (Deistler und Rentrop 2022a) die Identifikation und klare Beschreibung des relevanten IT-Problems sowie der Nachweis der Forschungslücke. Im Anschluss folgt die Phase Design & Demonstration, in der ein Artefakt, in diesem Fall eine Methode, entwickelt wird, um IT-Compliance in KMU angemessen umzusetzen. Dieser erste Ansatz wurde im Rahmen von zwei internationalen WI-Konferenzen (IADIS und PACIS 2022) vorgestellt, diskutiert und

Anpassungen direkt eingearbeitet (Deistler und Rentrop 2022c). Die weitere Evaluation wurde mithilfe von zwei Fallstudien durch Praxispartner durchgeführt, auf die im nächsten Abschnitt eingegangen wird. Hierbei wurde das Artefakt eingesetzt und auf Funktionsfähigkeit, Qualität und Wirksamkeit getestet. Die zwei Phasen Design & Demonstration, sowie Evaluation laufen iterativ so lange ab, bis das finale Artefakt entwickelt ist.

3.1 Durchführung der Fallstudien

Der Idealtyp einer Evaluation eines Artefakts besteht in der vollständigen Anwendung in der Praxis (Pries-Heje et al. 2008). Dies findet jedoch im Rahmen dieser Arbeit nicht statt. Aus reinen Praktikabilitätserwägungen heraus fehlt dem Autor ein Zugang zu einer IT-Organisation mit der für eine Organisationsgestaltung notwendigen Autorität. Auch die beschränkte Laufzeit und Ressourcen des Vorhabens stehen einer solchen idealtypischen Vorgehensweise zur Evaluation entgegen. Daher wurde zur Evaluierung des Artefaktes die Durchführung vergleichender Fallstudien nach Yin (2014) ausgewählt. Demzufolge werden Experteninterviews durchgeführt, mithilfe dessen ein breites Fachwissen, welches die Experten aus ihrer beruflichen Praxis erworben haben, abgefragt und repräsentativ dargestellt wird. Weiterhin wurde das Instrument der Triangulation angewendet (Yin 2014). Die Interviews haben im Zeitraum August bis Oktober 2022 stattgefunden und hatten unterschiedliche Zielgruppen und Ziele zum Zweck.

Zum einen sollte das methodische Vorgehen evaluiert werden. Hierzu wurden zehn Experten aus Compliance relevanten Positionen in mittelständischen Unternehmen, Wissenschaftler und Berater aus dem Umfeld der Wirtschaftsinformatik befragt (siehe Abschn. 4.3).

Zum zweiten sollte das implementierte Designobjekt evaluiert werden. Um die Menge an Fällen für den Rahmen der Arbeit handhabbar zu halten, wurden diese auf vier beschränkt, ein KMU je Archetyp sowie ein externer Berater (siehe Abschn. 4.4).

4 Methode zum angepassten Einsatz von Rahmenwerken in KMU

Ausgehend von der Phase Problem Identification & Objectives wird in diesem Kapitel die Entwicklung und Evaluation des Artefaktes vorgestellt. Das methodische Vorgehen ist in Abb. 1 grafisch dargestellt. Ein wesentlicher Bestandteil sind die Strukturelemente sowie KMU relevante Ausprägungen. Diese wurden auf Basis der vorhandenen Literatur ausgewählt und dienen dem Artefakt als strukturgebende Elemente. Die Herleitung und Definition werden vorab erläutert.

4.1 Definition der Strukturelemente

Mithilfe der Strukturelemente sollen die einzelnen Prozesse und Aktivitäten, losgelöst von dem jeweiligen Fokus eines Rahmenwerkes, in eine einheitliche vergleichende Struktur gebracht werden. Zur Herleitung der passenden Elemente ist

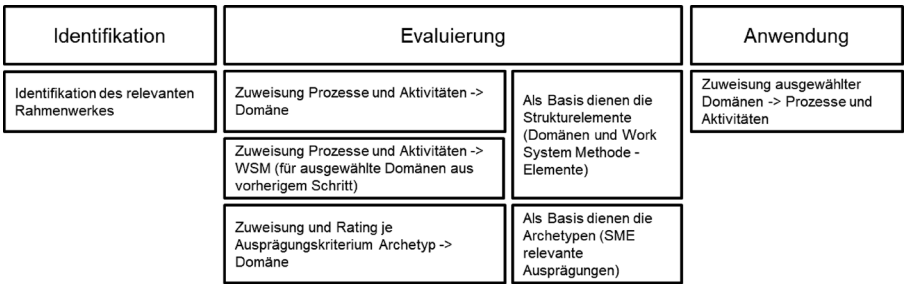

Abb. 1 Methodisches Vorgehen

ein Blick in das strategische Alignment von Business und IT notwendig, das als wesentliche Voraussetzung angesehen wird, damit IT zum Geschäftserfolg beitragen kann. Henderson und Venkatraman haben hierfür ein Modell entwickelt, um die Wirkungsweise des Alignments zu verdeutlichen. Dies ist in eine externe und interne Perspektive unterteilt und enthält unter anderem die Positionen Infrastruktur, Prozesse, Fähigkeiten, Kompetenzen, Governance und Scope (Henderson und Venkatraman 1989). Weill & Ross schlagen die Differenzierung in IT-Prinzipien, Architektur, Infrastruktur, Geschäftsanforderungen und Investitionen vor (Weill und Ross 2004). Dies erweist sich in der Praxis jedoch als zu wenig granular, da der Bereich der Infrastruktur sehr umfassend ist. Demzufolge schlägt Rentrop (Rentrop 2023) eine Einteilung in sieben Domänen vor: IT Prinzipien (Teilbereich: Stakeholder, Strategische Rolle, Grundlegende Ausrichtung der IT), Steuerung der IT (Teilbereich: Strategie, Budgetierung, Investitionsentscheidungen, Kostenmanagement), Architektur (Teilbereich: Gestaltung des Bebauungsplans, Standardisierung, Data Governance), Sourcing (Teilbereich: Sourcing Strategie, Lieferantenauswahl, Beziehungsgestaltung), Security, Risk & Compliance, Organisation und Personal (Teilbereich: IT im Unternehmen, IT innerhalb, Personelle Entscheidungen) und IT Services.

Die genannten Domänen decken alle Bereiche ab und eignen sich daher für die weiteren Schritte als strukturgebende Elemente.

Es ist jedoch noch ein weiteres Strukturelement notwendig, mit welchem insbesondere der Aspekt berücksichtigt wird, dass KMUs spezifische Herausforderungen, beispielsweise in Bezug auf Mitarbeiter und Kosten, haben. Darüber hinaus gibt es Unterschiede nach Branchen sowie nach kleinen und mittleren Unternehmen (Deistler und Rentrop 2022b).

Aus diesem Grund ist die Work System Methode (WSM) von Alter geeignet, diese zu differenzieren und einzuordnen. Die Work System Methode ist ein Ansatz zum Analysieren von Systemen in Organisationen, unabhängig davon, ob die IT eine wesentliche Rolle spielt oder nicht. Diese Methode ist breiter anwendbar als Techniken, die darauf ausgelegt sind, detaillierte Softwareanforderungen zu spezifizieren, und sie ist präskriptiver und leistungsfähiger als domänenunabhängige Systemanalysemethoden wie die Soft System Methode (Alter 2002). Für diesen Beitrag verwenden wir nicht alle Elemente die Alter in seinem Modell verwendet, sondern beschrän-

ken uns auf die für uns relevanten kohärenten Elemente Prozesse und Aktivitäten, Mensch, Informationen und Technologie. Diese werden im Folgenden erläutert.

Prozesse und Aktivitäten: Arbeitsschritte, durch die Arbeit innerhalb eines Arbeitssystems ausgeführt wird. Diese bilden in unserem Fall die relevanten Objectives (COBIT 2019 [ISACA 2018] und ISO/IEC 27001:2013) und Praktiken (ITIL4) ab.

Mensch (P): Die Personen, die zumindest einen Teil der Arbeit im Geschäftsprozess ausführen, sind die Menschen des Arbeitssystems.

Informationen (I): Informationen umfassen kodifizierte und nicht kodifizierte Informationen, die verwendet und erstellt werden, während die Menschen ihre Arbeit ausführen.

Technologien (T): Zu den Technologien gehören die Werkzeuge und Techniken, die die Menschen des Arbeitssystems bei der Ausführung ihrer Arbeit verwenden (Alter 2002).

4.2 Definition KMU-relevanter Ausprägungen

In einem nächsten Schritt wird eine weitere Klassifizierung nach KMU-relevanten Ausprägungen vorgenommen. Dazu muss zunächst eine Klassifizierung der Unternehmensgrößen innerhalb von KMU vorgenommen werden, da diese einen wesentlichen Einfluss auf die Ausgestaltung eines IT-GRC-Ansatzes hat. Dabei wird auf ein gängiges Begriffsverständnis zurückgegriffen. Demnach wird ein Unternehmen mit weniger als 9 Mitarbeitern als Kleinstunternehmen, mit 10 bis 49 Mitarbeitern als kleines Unternehmen und mit 50 bis maximal 249 Mitarbeitern als mittleres Unternehmen definiert (EU-Kommission 2005). Für einen IT-GRC-Ansatz geht diese Einteilung jedoch nicht weit genug. Auch das Vorhandensein von Technologie im Unternehmen hat einen wesentlichen Einfluss. Es ist davon auszugehen, dass es einen Zusammenhang zwischen der Ausgestaltung bzw. dem Reifegrad der Technologie und der Anzahl der Beteiligten gibt. Um dies in das Modell einfließen zu lassen, werden in Anlehnung an Rohlfing und Funck (2002) und COBIT2019 Focus Area SMEs (ISACA 2018) drei Archetypen entwickelt, nach denen eine Differenzierung innerhalb von KMU möglich ist und somit die unterschiedlichen Ausprägungen in KMU berücksichtigt werden, wie in Tab. 1 dargestellt.

Darüber hinaus sind aktuelle Trends und Entwicklungen, die aus der Phase Problem Identification & Objectives stammen, für alle Archetypen zu berücksichtigen. Diese sind Information Security Awareness, Cybersicherheit, Cloud Compliance und Datenschutz (Deistler und Rentrop 2022a).

Nachdem die als Basis dienenden strukturgebenden Elemente beschrieben wurden, geht es im nächsten Schritt um die Phasen Identifikation, Evaluierung und Anwendung. Vorab ist zu ergänzen, dass in dieser Arbeit aufgrund der höheren Aussagekraft nicht ein Rahmenwerk, sondern drei verbreitete Rahmenwerke ausgewählt und evaluiert wurden (Deistler und Rentrop 2022a). Daher kann der nächste

Tab. 1 Archetypen

Archetyp	Ausprägungen
1	Kleines Unternehmen, IT hauptsächlich ausgelagert, keine klare Verantwortung für die IT, begrenzte interne IT-Kenntnisse/-Kapazitäten, relativ hohe Risikotoleranz aufgrund geringer Risikokapazität, einfache Befehlsstruktur und begrenzte Organisationsstrukturen vorhanden
2	Kleines Unternehmen, IT hauptsächlich intern, IT-Abteilung vorhanden, komplexere Aufgaben werden ausgelagert, begrenzte interne IT-Fähigkeiten und/oder -Kapazitäten, relativ hohe Risikotoleranz aufgrund geringer Risikokapazität, einfache Befehlsstruktur und begrenzte Organisationsstrukturen vorhanden
3	Mittelgroßes Unternehmen, heterogene IT-Landschaft und IT-Abteilung vorhanden, möchten eher kaufen (und möglicherweise anpassen) als selbst entwickeln, komplexere Aufgaben auslagern

Schritt, das Mapping der ausgewählten Rahmenwerke als optional für die eigentliche Methode angesehen werden.

4.3 Mapping der ausgewählten Rahmenwerke

Das etablierte und laufend überarbeitete COBIT 2019 Rahmenwerk dient dabei als Referenzrahmen, welches für die Strukturierung und das Mapping anderer Standards genutzt wird. Es wurden bereits Mappings von COBIT 2019 auf ITIL4 (Hartawan und Suroso 2017) und ISO/IEC 27001:2013 (Yasin et al. 2020) durchgeführt. Dies geschah mit Hilfe der ArchiMate Language nach Lankhorst. ArchiMate ist eine offene und unabhängige Modellierungssprache für Unternehmensarchitektur, die die Beschreibung, Analyse und Visualisierung von Architektur innerhalb und zwischen Geschäftsbereichen in einer eindeutigen Weise darstellen kann (Lankhorst 2009). So wurde eine Vergleichbarkeit der verschiedenen Rahmenwerke herausgearbeitet, welche in Abb. 2 (Teil „Mapping COBIT2019, ITIL4, ISO/IEC 27001:2013“ der Tabelle) dargestellt ist.

4.3.1 Schritt 1: Identifikation der relevanten Rahmenwerke

Für die Identifikation der relevanten Rahmenwerke ist das komplette Vorliegen des einzelnen Rahmenwerkes, insbesondere der jeweiligen Anforderungen, die auch Objectives, Praktiken oder Scope genannt werden, von Relevanz.

ISO/IEC 27001:2013 und COBIT 2019 sind beides Rahmenwerke, die sich mit der Art und Weise befassen, wie Organisationen ihre IT-Systeme verwalten und überwachen. COBIT hat klar definierte Ziele und Governance-Strukturen, während ISO/IEC 27001:2013 verlangt, dass die Ziele der Informationssicherheit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit je nach organisatorischem Kontext definiert werden. Der Unterschied zwischen diesen beiden Normen besteht darin, dass sich ISO/IEC 27001:2013 hauptsächlich auf die Sicherheit bezieht, während COBIT 2019 die IT als Ganzes betrachtet und einen funktionalen Blickwinkel einnimmt. In ITIL4 liegt der Fokus auf der operativen Betrachtung und Bewertung des Sicherheitsprozesses mit Schwerpunkt auf der Informationssicherheit. ITIL4 und ISO 27001:2013 definieren in erster Linie, wie Anforderungen umgesetzt werden sollen, COBIT 2019 definiert in erster Linie, was umgesetzt werden soll. COBIT

Relevanz Archetyp 1	Relevanz Archetyp 2	Relevanz Archetyp 3	Mapping COBIT2019, ITIL4, ISO/IEC 27001:2013			IT-Prinzipien			Steuerung der IT			Architektur			Sourcing			Security,Risk,Compliance			Organisation & 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							

Abb. 2 Ergebnis je Archetyp

2019 befindet sich also auf einer höheren Ebene. Stark vereinfacht ausgedrückt sind ITIL4 und ISO/IEC 27001:2013 operativ und taktisch, während COBIT 2019 eher strategisch ist.

4.3.2 Schritt 2: Evaluierung der relevanten Rahmenwerke

Im Rahmen der Evaluierungsphase erfolgen zunächst die Zuordnungen der Prozesse und Aktivitäten zu Domänen und darauf aufbauend die Zuordnung der ausgewählten Domänen zu den WSM-Elementen. Im letzten Schritt erfolgt die Zuordnung mithilfe eines Ratings der KMU Ausprägungen je Archetyp zu den Domänen (siehe auch Abb. 1). Diese Zuordnungen und das Vorgehen wurden im Rahmen der Fallstudien evaluiert und werden im Folgenden im Detail vorgestellt.

Um im ersten Schritt eine Zuordnung der Prozesse und Aktivitäten zu den definierten sieben Domänen durchzuführen, wurden Techniken der ArchiMate Language (Lankhorst 2009) und der aus der Fallstudienforschung vorgeschlagene Evidenzen (Yin 2014), wie Handbücher, Prozessmodelle und Servicekataloge, herangezogen. Im Detail wurden alle Prozesse und Aktivitäten aus den Rahmenwerken einzeln gesichtet und der jeweiligen Domäne zugeordnet. Dabei sind Mehrfachzuordnungen möglich (siehe Abb. 2). Die zehn Experten überprüften und ergänzten die Ergebnisse dieser Vorstufe. Das für jeden Interviewpartner zugrunde gelegte Verfahren zur Erhebung der Daten orientierte sich an der konkreten Zuweisung der Prozesse und Aktivitäten zu Domänen in Form einer vorab erstellten Matrix. Abweichungen wurden identifiziert, nochmals bewertet und angepasst.

Auf dieser Grundlage wurden im nächsten Schritt die ausgewählten Prozesse und Aktivitäten und dazugehörigen Domänen zu den WSM-Elementen Mensch, Information und Technologie zugeordnet. Zur Verdeutlichung, für die Aktivität und Prozess EDM01 aus COBIT 2019 wurde eine Domänenzuordnung zu IT-Prinzipien erarbeitet. Infolgedessen ist für diese Domäne zu evaluieren, ob zur Zielerreichung Menschen, Information oder/und Technologie notwendig sind. Auch hier kann es zu Mehrfachzuordnungen kommen. Beispielsweise kann ein Prozess, wie APO05 aus COBIT 2019, mehrere Prozesse und Aktivitäten erfordern, wie IT-Prinzipien, Management der IT und Architektur. Dies führt dazu, dass mehrere Personen für diese Prozesse benötigt werden und somit auch mehrere Zuordnungen zu Menschen durchgeführt werden. Die Personalintensität zur Abdeckung dieses Prozesses spiegelt sich somit wider. Das Ergebnis dieser Zuordnungen ist in Abb. 2 mit einem „x“ dargestellt.

Im letzten Schritt wurden die drei Archetypen anhand ihrer Ausprägungen bewertet und den entsprechenden Domänen zugeordnet. Es wurde ein 2-stufiges Bewertungsmodell verwendet: hoch (h; +1) für die Angabe, dass diese Domäne passend und wichtig zur Ausprägung ist und vorrangig abgebildet werden sollte und niedrig (l; –1) für die Angabe, dass diese Domäne nicht berücksichtigt werden sollte. Keine Bewertung bedeutet, dass die Domänen für diese Ausprägungen neutral sind und damit mit 0 bewertet wird. Beispielsweise wurde für die Ausprägung „IT hauptsächlich ausgelagert“ im Archetyp 1 die Domäne Sourcing als hoch bewertet, da davon ausgegangen werden kann, dass die Themen wie Strategien der IT (Cloud-Anwendung, Integration) und Auswahl der Lieferanten/Anbieter als ein wichtiges

Tab. 2 Zuweisung und Rating zu Archetyp 1 im Detail und Archetyp 2 und 3 zusammenfassend

Archetyp 1	IT Prinzipien	Steuerung der IT	Architektur	Sourcing	Security, Risk & Compliance	Organisation & Personal	IT Services
Kleines Unternehmen	l	h	l	h	h	l	l
IT hauptsächlich ausgelagert	–	–	–	h	–	–	l
Keine klare Verantwortung für die IT	–	h	–	–	–	–	–
Begrenzte interne IT-Kenntnisse/-Kapazitäten	–	–	–	–	–	l	–
Relativ hohe Risikotoleranz aufgrund geringer Risikokapazität	–	–	–	–	h	–	–
Einfache Befehlsstruktur und begrenzte Organisationsstrukturen vorhanden	–	–	–	–	h	l	–
Information Security Awareness, Cyber Security, Cloud Compliance und Datenschutz	–	–	–	–	h	–	–
Ergebnis Archetyp 1	–1	2	–1	3	4	–3	–2
Ergebnis Archetyp 2	0	2	–1	3	4	–3	2
Ergebnis Archetyp 3	0	2	1	4	3	–2	4

Merkmal hierfür eingestuft werden kann. Die Domäne IT Services jedoch als nicht relevant erachtet werden kann, da das Betreiben der IT-Systeme (mit seinen Teilbereichen wie zum Beispiel: Change-Management, Software-Entwicklung) bei einer Auslagerung primär dem Dienstleister obliegt. Aufgrund dieser qualitativen Messungen haben wir hier eine subjektive Interpretation. Um jedoch eine hohe Validität zu erreichen, wurde dies mit allen zehn Interviewten mehrfach diskutiert und angepasst. Das zusammengefasste Ergebnis ist in Tab. 2 für den Archetyp 1 komplett und die Ergebnisse für Archetyp 2 und 3 in der unteren Zeile dargestellt.

Schlussendlich erfolgte durch jeden Interviewten eine Zuordnung der relevanten Prozesse und Aktivitäten je Archetyp. Im Weiteren erfolgt der letzte Schritt: die Anwendung des relevanten Rahmenwerks.

4.3.3 Schritt 3: Anwendung der relevanten Rahmenwerke

Im weiteren Verfahren wurde auf der Grundlage der Bewertungen aus Tab. 2 die finalen Zuordnungen durchgeführt. Domänen mit einer Bewertung größer als 0 (siehe „Ergebnis“ in Tab. 2) wurden als relevant eingestuft und in das Soll-Objekt aufgenommen (siehe Abb. 2), Domänen mit einer Bewertung unter 0 wurden als nicht relevant für diesen Archetyp betrachtet. Wenn ein Prozess wie beispielsweise EDM02 mehrere Domänen abdeckt, wie die Domäne IT-Prinzipien und Manage-

ment der IT, die mit –1 und +2 bewertet wurden, wurde dieser Geschäftsprozess aufgenommen, weil die Relevanz mit +2 deutlich hervorgehoben wurde. Ist jedoch ein Prozess wie BAI01 zu zwei Domänen zugeordnet und eine davon Organisation & Personal, die mit –3 im Archetyp 2 eingestuft wurde, ist dieser Prozess nicht aufgenommen worden, da davon auszugehen ist, dass dies schwer anzuwenden ist. Dieses Verfahren wurde für alle drei Archetypen durchgeführt.

Anschließend wurden drei Experten, die bereits in die Einführung, Anpassung und den Betrieb in Bezug auf COBIT 2019, ITIL, ISO/IEC27001:2013 in ihrer Organisation involviert waren und auf Basis ihrer Erinnerung und Erfahrungen den Betrieb und die Hintergründe schildern konnten, befragt. Dabei hat jeder Experte ein Archetyp vertreten. Das für jeden Fall zugrunde gelegte Verfahren zur Erhebung der Daten orientierte sich an einem Leitfaden. Es wurde zudem eine Pilotfallstudie mit einem Berater eingebaut, um das Datenerhebungsverfahren zu verbessern. Der Einstieg bildete allgemeine Fragen zu den Rahmenbedingungen der Organisation und des Projektes/Implementierung des relevanten Rahmenwerkes. In diesem Zusammenhang sollen gesammelte Erfahrungen der Befragten identifiziert werden. Im nächsten Schritt wurde das Soll-Objekt (Artefakt je Archetyp) den Erfahrungen des Experten gespiegelt und Feedback auf Realisierbarkeit erfragt. Hierbei wurde auch ein Positiv-/Negativtest durchgeführt, bedeutet es wurde geprüft, ob das Soll-Objekt des Archetyp 1 passend ist, es wurde aber auch geprüft, ob Archetyp 2 oder 3 auch passend wären. Begleitend zu den Experteninterviews wurde eine Triangulation der so erhobenen Informationen durchgeführt. Bei Experte A wurde beispielsweise Einsicht in die Dokumentation einer internen Prüfung genommen und gesichtet, welche Prozesse und Aktivitäten aus dem ISO Standard als nicht effektiv bewertet wurden. Ebenfalls wurden Projektpräsentationen bei Experte C eingesehen, die die Aussage manifestierten, das personalintensive Prozesse minimiert und Projekte aufgesetzt wurden, um diese mithilfe von IT-Anwendungen zu automatisieren. Jeder Interviewpartner wurde noch ein zweites Mal befragt, um die Ergebnisse zu bestätigen und die Beschreibungen zu präzisieren.

5 Diskussion der Ergebnisse

Werden die Anzahl der Zuweisungen der WSM-Elemente, Mensch (47), Information (42) und Technologie (33) im Ausgangszustand des Rahmenwerkes betrachtet und diese mit den Zuweisungen in den entwickelten Archetypen verglichen, so lassen sich folgende Ergebnisse feststellen. Für den Archetyp 1 resultiert eine Anzahl an Zuweisungen von Menschen (22), Informationen (22) und Technologie (15), die den Ausprägungen dieses Archetyps entsprechen. Die WSM-Zuweisungen für den Archetyp 2 und 3 bestätigen ebenfalls eine Reduktion des Elementes Mensch im Verhältnis zum Ausgangszustand. Damit wird auf das Problem fehlender Mitarbeiterressourcen in KMU eingegangen. Weiterhin hat das Element Technologie (32) im Archetyp 3 die höchste Anzahl an Zuweisungen, was mit den Ausprägungen dieses Archetyps korreliert. Der gleiche Sachverhalt ist bei der Anzahl der relevanten Prozesse und Aktivitäten zu erkennen, so sind von den im Ausgangszustand 40

relevanten Prozesse und Aktivitäten 15 im Archetyp 1, 29 im Archetyp 2 und 33 im Archetyp 3 als relevant evaluiert worden.

Die Ergebnisse werden als durchweg hilfreich bei den Interviewten gesehen. Die Methode ermöglicht es, IT-GRC Verantwortlichen die Rahmenwerke in eine KMU Organisationsstruktur zu überführen beziehungsweise anzupassen. Durch die Fokussierung auf KMU relevante Ausprägungen in der entwickelten Methode, wird eine Priorisierung von Prozessen und Aktivitäten vorgenommen. Risiken können damit reduziert werden, weil die (fehlenden) Kapazitäten zielorientierter eingesetzt werden. Schließlich sollen die Flexibilität und Innovationsfähigkeit, für die KMU bekannt sind, aufrechterhalten werden und nicht Prozesse und Aktivitäten aufgebürdet werden, die für große Unternehmen leicht umzusetzen sind, KMU hingegen bürokratisieren.

In den dargestellten Schritten wurde der Nutzen, die Qualität und die Wirksamkeit der entwickelten Methode untersucht (Hevner et al. 2004). Die erfolgreiche Simulation in den drei Archetypen beweist den Nutzen der Methode. Dies zeigt sich in der Durchführung der einzelnen Schritte (Peffers et al. 2008) und in der Bewertung der einzelnen Fälle durch die beteiligten Experten. Mit dem endgültigen Entwurf kann die Forschungsfrage beantwortet werden.

Das Artefakt beschreibt einen generischen methodischen Ansatz, der es ermöglicht, bestehende Rahmenwerke anhand KMU-spezifischer Bedürfnisse zu bewerten. Weiterhin resultiert daraus ein angepasster IT-GRC-Ansatz. Entgegen der bisherigen grundlegenden Ausrichtung der Forschung konzentriert sich dieser Beitrag auf die Konkretisierung von Ansätzen. Das Artefakt hat die Ziele, eine praktisch anwendbare und theoretisch begründete Methode zu entwickeln, erfüllt.

Als letzten Schritt der Evaluation wurde die endgültige Methode mit allen Fallbeispielen verglichen, um ihre Zuverlässigkeit und Gültigkeit zu belegen.

6 Zusammenfassung

Die Ergebnisse aus zehn Interviews und weiteren drei Feedbackschleifen ergaben, dass die Methode in der Praxis anzuwenden ist, ein „Tailoring“ von etablierten Rahmenwerken erfolgen kann und KMU damit Handlungsempfehlungen an die Hand bekommen, um ein gewisses Maß an IT-Compliance zu erreichen. Zudem kann die Methode mit geringem Aufwand durchgeführt werden.

Die Auswahl der Fälle könnte jedoch Einschränkungen mit sich bringen. Die Verallgemeinerung könnte verbessert werden, indem noch mehr Fälle aus anderen Branchen und mit einer anderen Organisationsstruktur untersucht werden. Zudem könnte eine vollständige Anwendung in der Praxis erprobt werden. Es kann zudem ein gewisser Bias hin zu positiven Extremfällen unterstellt werden, da davon auszugehen ist, dass solche Unternehmen sich zur Teilnahme bereiterklärten, in denen die Projekte als erfolgreich gesehen werden. Zudem basiert unsere Untersuchung ausschließlich auf qualitativen Daten, da Zuordnungen schwer zu quantifizieren sind.

Zusätzlich zu den beschriebenen Ausprägungen muss ein Unternehmen möglicherweise weitere individuelle Merkmale berücksichtigen, die zu einem weiteren Archetyp führen können und damit das Ergebnis verändern. Weiterhin sollte das

Auslassen von Prozessen und Aktivitäten von jedem Unternehmen nochmals kritisch geprüft werden, ob diese tatsächlich nicht notwendig sind, da die Rahmenwerke in der Regel einen ganzheitlichen Ansatz vertreten. Wir sind sicher, dass diese Arbeit einen Beitrag zu Theorie und Praxis im Bereich IT-Compliance in KMU beitragen wird.

Zusammenfassend kann der Beitrag ein Anstoß für KMU sein, ihr Bewusstsein in Bezug auf IT-GRC zu schärfen und gibt Handlungsempfehlungen für ein angepasstes Mindestniveau an IT-Compliance.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Alter S (2002) The work system method for understanding information systems and information systems research. Commun Assoc Inform Syst 9:Article 6

Beißel S (2017) Differenzierung von Rahmenwerken des IT-Risikomanagements. HMD 1(54):37–54

Deistler N, Rentrop C (2020) IT-compliance in KMU – state of the art. HMD 57:1047–1057

Deistler N, Rentrop C (2022a) IT-Compliance in KMU – Experteninterviews zum Status quo. Wirtschaftsinform Manage. https://doi.org/10.1365/s35764-021-00380-5

Deistler N, Rentrop C (2022b) An IT-GRC Approach in SME. In: Proceedings of the 15th IADIS International Conference Porto, S 233–237

Deistler N, Rentrop C (2022c) A Method for an IT-GRC Approach in SMEs – Design Phase. In: PACIS 2022 Proceedings 316. https://aisel.aisnet.org/pacis2022/316. Zugegriffen: 01.08.2022

EU-Kommission (2005) Definition of SMEs. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN. Zugegriffen: 11. Febr. 2022

Hartawan F, Suroso J (2017) Information technology services evaluation based ITIL V3 2011 and COBIT 5 in center for data and information. In. In: Intelligent information and database systems. 9th Asian conference

Henderson JC, Venkatraman N (1989) Strategic alignment. A framework for strategic information technology management. In: CISR WP No. 190 Massachusetts

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

Hevner A, Salvatore M, Jinsoo P, Sudham R (2004) Design science in information systems research. MISQ 28(1):75–105

Hillebrand A et al (2017) Aktuelle Lage der IT-Sicherheit in KMU.WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH. https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf. Zugegriffen: 28. Nov. 2020

International Standard Organization (2014) ISO/IEC 27001:2013. Information Technology – Security techniques – Information security management systems – overview and vocabulary

ISACA (2018) COBIT 2019: Einführung und Methodik (ISACA.org)
ITIL Foundation: ITIL4 Edition
Johannsen A, Kant D (2020) IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU. HMD 57:1058–1074
Knoll M, Strahringer S (2017) IT-GRC-Management im Zeitalter der Digitalisierung. In: Knoll M, Strahringer S (Hrsg) IT-GRC-Management – Governance, Risk und Compliance. Grundlagen und Anwendungen. Springer Vieweg, Wiesbaden, S 1–24
Lankhorst M (2009) Enterprise architecture at work. In: The enterprise engineering series. Springer, Berlin Heidelberg
Peffers K, Tuunanen T, Rothenberger A, Chatterjee S (2008) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–77
Pries-Heje J, Baskerville R, Venable J (2008) Strategies for design science research evaluation. In: Proceedings of the ECIS 2008 conference Galway
Rentrop C (2023) IT-Governance. Erfolgsfaktor für die digitale Transformation. Erich Schmidt Verlag, Berlin
Rohlfing M, Funck D (2002) SMEs Kritische Diskussion quantitativer und qualitativer Definitionsansätze. In: IMS-Forschungsberichte Nr. 7. Universität Göttingen, Göttingen
Webster J, Watson R (2002) Analyzing the past to prepare for the future: writing a literature review. MISQ 26(2):xiii–xxiii
Weill P, Ross JW (2004) IT governance. How top performers manage IT decision rights for superior results. Harvard Business School, Boston
Yasin M, Arman A, Edward I, Shalannanda W (2020) Designing information security governance recommendations and roadmap using COBIT 2019 framework and ISO 27001:2013. In: 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA)
Yin RK (2014) Case study research: design and methods, 5. Aufl. SAGE, Los Angeles