IT-Compliance in KMU – State of the art

Nico Deistler · Christopher Rentrop

Eingegangen: 1. November 2019 / Angenommen: 28. März 2020 / Online publiziert: 24. April 2020
© Der/die Autor(en) 2020

Zusammenfassung Kleine und mittelständische Unternehmen (KMU) sind bekannt für ihre Innovationskraft und bilden das Rückgrat der deutschen Wirtschaft. Wie Studien zeigen sind sie in Bezug auf Compliance-Maßnahmen im Vergleich zu kapitalmarktorientierten Unternehmen jedoch im Rückstand. Eine gesonderte Betrachtung der IT-Compliance erfolgt dabei in den Studien in der Regel nicht. Auch wenn zu den Gründen und Motiven fehlender IT-Compliance-Strukturen in KMU kaum Forschungsergebnisse vorliegen, zeigen doch die vielen Publikationen, die sich mit Teilaspekten von Compliance und KMU beschäftigen, dass Handlungsbedarf besteht. Insbesondere die aktuellen Veränderungen unter dem Stichwort Digitalisierung deuten auf eine gesteigerte Bedeutung von IT-Compliance-Maßnahmen vor allem in mittelständischen Unternehmen. In dieser Arbeit sollen daher mithilfe einer Literaturrecherche die aktuell behandelten Themen in Bezug auf IT-Compliance und KMU analysiert sowie aktuelle Themenschwerpunkte herausgearbeitet werden.

Schlüsselwörter IT-Compliance · Compliance · Mittelständische Unternehmen · KMU · Literaturrecherche

N. Deistler · C. Rentrop (✉)

Fakultät Informatik, HTWG Konstanz, Alfred-Wachtel-Straße 8, 78462 Konstanz, Deutschland
E-Mail: christopher.rentrop@htwg-konstanz.de

N. Deistler
E-Mail: ndeistle@htwg-konstanz.de

IT Compliance in SME—State of the art

Abstract Small and medium-sized enterprises (SMEs) are known for their innovative strength and form the backbone of the German economy. Studies show, however, that they are falling behind capital market-oriented companies in terms of compliance measures. In these studies there is no detailed analysis for the subarea IT-Compliance. The increasing trends of digitization and industry 4.0 drive the massive change, which increase the necessity of IT-Compliance measures especially in SME.

Although there is little discussion on the reasons and motives of missing IT-Compliance efforts in SME, many publications, which deal with partial aspects of Compliance and SME, demonstrate the need for action. Therefore, the aim of this paper is reviewing the current state in literature and identifying current topics in IT-Compliance in SMEs.

Keywords IT-Compliance · Compliance · SME · State of the art

1 Einleitung

Das Thema Compliance, unter dem die Einhaltung (inter-)nationaler gesetzlicher Bestimmungen, regulatorischer Standards und Anforderungen der Stakeholder verstanden wird, ist in vielen Unternehmen angekommen und bedingt durch Skandale in Konzernen vermehrt in der öffentlichen Wahrnehmung. Die steigende Anzahl von Regeln und Anforderungen sowie harte Strafen und Reputationsverlust bei Nichtanwendung haben zu einem erhöhten Bewusstsein geführt.

Ebenso erlebt die Informationstechnologie (IT) einen regelrechten Aufschwung. IT-Systeme werden durch die weitere Automatisierung von Geschäftsprozessen einen höheren Durchdringungsgrad erreichen und damit einen immer größeren Stellenwert einnehmen. Die effiziente Einbindung und Ausgestaltung der IT in Geschäftsprozesse mittels Best-Practice-Ansätzen wie Control Objectives for Information and Related Technology (COBIT) oder IT Infrastructure Library (ITIL) haben sich etabliert und tragen zu einem Wertbeitrag und einer erhöhten Compliance der IT bei.

Für kapitalmarktorientierte Konzerne ist die Ausgestaltung der IT nach diesen Ansätzen und damit die Einhaltung von IT-Compliance selbstverständlich (Nilles und Senger 2012). Ganz anders sieht es bei mittelständisch geprägten Unternehmen (KMU) aus. Wie Studien zeigen haben sie diesem Thema bisher wenig Aufmerksamkeit gewidmet. Betrachtungsweise der Publikationen ist überwiegend das Thema Compliance im Generellen (Grüniger et al. 2014). Eine Fokussierung auf IT-Compliance erfolgt nicht. Dies bietet den Anlass für Untersuchungen, explizit für den Teilbereich IT-Compliance in KMU. Die steigende Anzahl von Veröffentlichungen, die sich mit Teilaspekten von Compliance und KMU beschäftigen, zeigen dass Handlungsbedarf vorhanden ist. Zudem werden technologische Veränderungen eine größere Aufmerksamkeit bei KMU erfordern (Legner et al. 2017).

Auf dieser Grundlage wird das Ziel der Arbeit definiert. Mithilfe einer Literaturstudie sollen die wissenschaftlichen Beiträge zu den Themen IT-Compliance in KMU untersucht und der aktuelle Forschungsstand aufgezeigt werden.

Die Arbeit ist wie folgt strukturiert: Im ersten Abschnitt wird zunächst grundlegendes zum Thema IT-Compliance in KMU erörtert. Im Anschluss wird das methodische Vorgehen der Literaturrecherche vorgestellt und im weiteren Verlauf die Ergebnisse dargestellt und diskutiert. Zum Schluss erfolgen ein Ausblick sowie die Darstellung des weiteren Forschungsbedarfs.

2 Grundlegendes zu IT-Compliance in KMU

Seit Anfang der 1990er-Jahre rückt das Thema Compliance infolge von Bilanzskandalen verstärkt in das Blickfeld der Wirtschaftswelt und hat in den letzten Jahren enorm an Bedeutung gewonnen. IT-Compliance ist ein Teilbereich der Corporate Compliance, in dem sämtliche gesetzliche und regulatorische Vorgaben hinsichtlich des betrieblichen Einsatzes von IT adressiert werden (Klotz 2011; Strasser und Wittek 2012). Unter der IT-Governance, die sich als Teilbereich zur Corporate Governance versteht, wird IT-Compliance als Zustand bezeichnet, der durch geeignete Maßnahmen anzustreben ist und somit eine Zielgröße der IT-Governance darstellt. Zudem sind Schnittmengen mit Themen des IT-Risikomanagement vorhanden (Weill und Ross 2004). Einzuordnen ist IT-Compliance demzufolge als eigenständiger Forschungsbereich.

Grundsätzlich werden in der Literatur vier Perspektiven der IT-Compliance betrachtet (Klotz 2009):

- IT-Compliance als Verhalten, bei den von den Mitarbeitern für die IT relevanten Vorgaben beachtet und erfüllt werden (z. B. Verhaltenskodex).
- IT-Compliance als Zustand, indem für die IT relevanten Vorgaben nachvollziehbar eingehalten werden (zur Erfüllung der Interessengruppen).
- IT-Compliance als Managementsystem (Identifikation der relevanten Regelwerke, die Ableitung der Anforderungen, Implementierung und Überwachung von Maßnahmen zur Erfüllung der Compliance-Anforderungen) sowie
- IT-Compliance als Institution, zur Durchführung und Zuweisung von Verantwortlichkeiten (z. B. Ausrichtung zentral vs. dezentral).

Innerhalb der Literaturrecherche wird kein Fokus auf einzelne Perspektiven gelegt, da zunächst generell analysiert werden soll, welche Beiträge vorhanden sind.

Weiterhin kann hinsichtlich der Compliance von IT sowie Compliance durch IT unterschieden werden. Dabei wird bei Erstem die IT als Bewertungsobjekt betrachtet, um für die jeweiligen IT-Systeme Compliance-Anforderungen herzustellen. Aufgrund der ansteigenden und komplexer werdenden Systeme wird mit einer wachsenden Bedeutung dieser Thematik in der Praxis und in der Wissenschaft zu rechnen sein (Capgemini 2016; Legner et al. 2017). Aus diesem Grund wird diese Perspektive besonders in die Betrachtungen mit einbezogen. Bei Compliance durch IT wird die IT als Hilfsmittel zur Erfüllung der Anforderungen bezeichnet (Kronsnabl 2010). Die auf dem Markt befindlichen Softwarelösungen umfassen entweder einen

ganzheitlichen Ansatz, wie B Wise IT GRC (Governance, Risk & Compliance) und SAP GRC oder fokussieren sich auf einzelne Teilaspekte der genannten Bereiche. Beide Sichtweisen greifen ineinander.

Nachdem die unterschiedlichen Perspektiven der IT-Compliance aufgezeigt wurden, sind im nächsten Abschnitt generelle Anforderungen an IT-Compliance beschrieben.

Unternehmen müssen eine Vielzahl von gesetzlichen und regulatorischen Vorgaben beachten. Nicht zuletzt aufgrund des Neuigkeitsgrades und ständigen Veränderungen wie beispielsweise die EU-DSGVO (EU-Datenschutzgrundverordnung) gibt es diverse Anforderungen. Grundsätzlich können die Anforderungen in vier Gruppen unterteilt werden. Die erste Gruppe bezieht sich auf rechtliche Vorgaben, die gesetzliche Regelungen oder auf dessen Grundlage erlassene Vorschriften abbilden. Beispiele hierfür sind Gesetze, Rechtsprechungen oder Verwaltungsvorschriften, die sich auf den betrieblichen Einsatz von IT auswirken. In der zweiten Gruppe werden Verträge sowohl allgemeiner Art als auch IT-spezifischer Art mit Kunden, Lieferanten oder Dienstleistern verstanden. Eine weitere Gruppe sind interne Regelwerke, die vor allem Richtlinien, Unternehmensstandards und Verfahrensanweisungen beinhalten, die unternehmensinterne Festlegungen bezüglich der IT enthalten. Diese werden oftmals verwendet, um externen Interessensgruppen (z. B. Wirtschaftsprüfungsgesellschaften) die Einhaltung darzulegen. Zur Gruppe der externen Regelwerke gehören überwiegend Rahmenwerke, Normen und Standards, die sich durchgesetzt haben und eine gewisse Art von Best-Practice-Ansätzen der Ausgestaltung von IT darstellen. Dieser Gruppe kommt eine besondere Beachtung zu Teil, da die Erfüllung der Vorgaben bei der Auftragsvergabe von Kunden erwartet oder vorgeschrieben wird. Oftmals werden die Vorgaben auch freiwillig erfüllt, um ein positives Unternehmensimage zu erreichen (Strasser und Wittek 2013).

Für die Erreichung von IT-Compliance sind ein gezieltes Management und die Implementierung von Prozessen notwendig. In zahlreichen empirischen Untersuchungen werden verschiedene Aspekte der Implementierung einzelner Referenzmodelle betrachtet. Die höchste Anwendung erfahren die Frameworks COSO, COBIT und ITIL. ISO/IEC stellt unterstützende Methoden und internationale Standards bereit (Johannsen und Goeken 2007). ITIL adressiert dabei eher die operative Ebene. COBIT 5 hingegen umfasst IT-Prozesse der IT-Governance und Compliance und hebt nach einigen Quellen, wie zum Beispiel Brand und Boonen (2005) sowie Heschl und Middelhof (2005), die besondere Bedeutung hervor. Begründet wird dies mit dem Abdeckungsgrad des Modells bezogen auf die Kernaufgabengebiete. Meist liegen den einzelnen Frameworks Partikularinteressen zugrunde, die wiederum nur einzelne Prozesse und Risiken abdecken. Jedoch sind durchaus Anknüpfungspunkte und Schnittmengen einzelner Frameworks vorhanden, die eine Kombination von Modellen ermöglichen (Falk. 2012).

3 Design und Methode der Literaturrecherche

Die Literaturrecherche verfolgt das Ziel, sowohl wissenschaftliche als auch praxisorientierte Beiträge der letzten zehn Jahre zu den Themen IT-Compliance in

Im ersten Schritt wurde nach Webster & Watson die relevante Literatur nach den Suchwörtern Compliance, IT-Compliance, KMU und mittelständische Unternehmen untersucht. Dabei ist zu unterscheiden zwischen den wissenschaftlichen Beiträgen, die eine Suche nach Titel, Abstract oder Keywords ermöglichen und den primär praxisorientierten Beiträgen, bei denen lediglich eine Schlagwortsuche möglich ist. Eine Verknüpfung der Suchbegriffe hat im ersten Schritt nicht stattgefunden. Aus dieser Treffermenge sind mehr als 100 Veröffentlichungen extrahiert worden. Im nächsten Schritt wurden die Beiträge auf eine tatsächliche Compliance-Relevanz untersucht (siehe Spalte „Compliance-Relevanz“ in Tab. 1) und thematische Gruppierungen gebildet (siehe „Schwerpunktthema“ in Tab. 1). Im weiteren Verlauf wurden Publikationen identifiziert, die konkrete Themenfelder von IT-Compliance in Verbindung mit KMU beschreiben (siehe Spalte „davon KMU-Relevanz“ in Tab. 1). Die Ergebnisse sind in der Tab. 1 zusammengefasst.

Tab. 1 Darstellung der Forschungsergebnisse nach Schwerpunktthemen

Schwerpunktthema	Literatur		Quellen
	Anzahl	Davon Compliance- Relevanz KMU-Rele- vanz	
Digitalisierung/ Industrie 4.0	18	10	Legner et al. (2017), Ludwig et al. (2016), Capgemini (2016), Zimmermann (2017), Lindner et al. (2018), Knoll (2017), Ley und Bley (2016), Uhl et al. (2018), Knoll (2017), Lindner et al. (2018)
IT-Outsourcing und Compliance	7	3	Strasser und Wittek (2013), Weiss (2016), Paulus (2011)
Business IT Alignment	2	–	N. a.
Risikomanagement	3	–	N. a.
IT-Projekte und Compliance	2	–	N. a.
Compliance-Management-Systeme & Best-Practice-Ansätze	27	5	Kardel (2011), Barlette und Fomin (2008), Kolek (2018), Zeller et al. (2016), Schäfer et al. (2008)
Datenschutz	2	–	N. a.

N. a. Nicht anwendbar

4 Ergebnisse und Diskussion der Literaturrecherche

Im Folgenden werden die Ergebnisse der Literaturrecherche dargestellt. Zunächst werden allgemeine Ergebnisse beschrieben, um dann im nächsten Schritt auf die einzelnen Schwerpunktthemen einzugehen. Dabei erfolgt jeweils die Darstellung der Ergebnisse mit einer anschließenden Diskussion.

Es zeigt sich, dass viele Publikationen im Suchbereich Compliance den Fokus auf die Themen IT-Risikomanagement, IT-Security, Cloud Computing, IT-Governance und der Implementierung von Referenzmodellen haben. IT-Compliance wird oftmals nur als Teilbereich innerhalb dieser Beiträge beschrieben. Zudem werden Begriffe wie IT-Governance, IT-Risk-Management oder IT-Business in der Literatur häufig als Synonyme für Aspekte der IT-Compliance verwendet. Vor allem bei den Beiträgen in Verbindung mit KMU zeigt sich, dass sich diese fast ausschließlich auf die Thematiken Digitalisierung, Compliance-Management-Systeme sowie auf das Outsourcing von IT beziehen. Aufgrund dessen sind die drei Schwerpunktthemen identifiziert worden, auf die im Folgenden näher eingegangen werden soll. Zur konkreten Kombination von IT-Compliance in KMU wurden nur sehr wenige Artikel gefunden (siehe Tab. 1).

4.1 Digitalisierung/Industrie 4.0

Der deutsche Mittelstand, als das Rückgrat der Wirtschaft bezeichnet und Weltmarktführer in vielen Spezialgebieten, könnte an Innovationskraft verlieren, wenn die aktuellen Trends nicht verfolgt werden, da sind sich fast alle Studien einig

(Legner et al. 2017). Komplexere Verbindungen von Maschinen, Standorten und Unternehmen sowie dazugehörige Mitarbeiter- und Arbeitsstrukturen werden zu einer Veränderung in den Arbeitsabläufen führen (Ludwig et al. 2016). Neben den sozialpartnerschaftlichen Fragestellungen (Ludwig et al. 2016) steht oftmals die Durchdringung der IT in weitere Geschäftsprozesse und dessen Implikationen für die Organisation im Fokus der Publikationen. Speziell für KMU weisen die Studien von Capgemini (2016) und Zimmermann (2017) gegenüber dem Einsatz von Digitalisierung eine eher abwartende Haltung im Vergleich zu Konzernen auf. Konzepte zur neuen Ausgestaltung wie New Work, agile Arbeit und weitere Schlagwörter werden in der Wissenschaft kontrovers diskutiert (Lindner et al. 2018). Aus der Compliance-Perspektive werden dabei überwiegend mögliche Gefahren unter dem Schlagwort Cyber Security, IT-Security oder ähnlich lautenden Begriffen erörtert, die mit einer steigenden Nutzung der IT einhergehen (Knoll 2017). Die ansteigende Vernetzung von Systemen, das Kommunizieren der Systeme untereinander, könnten vor allem Bedrohungen von Extern mit sich ziehen (Ley und Bley 2016). In einer Fallstudie mit einem mittelständischen Unternehmen wurde untersucht, welche Möglichkeiten bestehen, das Geschäftsmodell nachhaltig zu transformieren und dabei die Chancen mittels Industrie 4.0 zu nutzen und gleichzeitig die Risiken gering zu halten. Ergebnis dieser Studie war, dass die wichtigste Voraussetzung die Kooperation mit Technologiepartnern ist und die Verfügbarkeit einfacher und vertikal integrierbarer Plattformen (Uhl et al. 2018). Eine weitere Veröffentlichung stellt ein ähnliches Ergebnis dar, mit der Ergänzung, dass als wichtige Grundvoraussetzung das Bewusstsein für Risiken steht. Denn nur wenn auch die Risiken richtig eingeschätzt werden, kann die passende Behandlungsstrategie gefunden werden. Ein wichtiger Baustein ist hierfür das Verständnis für Ursache-Wirkungsketten. Gerade nicht-technische Schwachstellen müssen ob ihrer hohen Bedeutung für den Einsatz neuer IT-Lösungen richtig erkannt und eingeschätzt werden. Der Autor beschreibt einen systematischen Risikomanagement-Prozess als wichtigste Herausforderung. Erst auf diesem Fundament könnten weiterführende Überlegungen zur zielgerichteten und besonnenen Auseinandersetzung mit den Risiken der Digitalisierung diskutiert werden (Knoll 2017).

Aus den Ergebnissen werden folgende Punkte besonders deutlich. Die potenziellen Möglichkeiten, die die Digitalisierung von Prozessen mit sich bringt werden in KMU bisher noch kritischer als in Konzernen gesehen. Die Veränderungen in der Organisation und der Informationstechnik werden jedoch voranschreiten. Die Informationstechnik wird im Wettbewerb zu einem entscheidenden Faktor für den Unternehmenserfolg werden (Ludwig et al. 2016). Sowohl in der Perspektive Compliance durch IT als auch Compliance von IT entstehen dadurch neue Risiken. Der Themenschwerpunkt Digitalisierung behandelt viele Themen, die aber nur teilweise Berührungspunkte mit Compliance aufweisen. Eine direkte Betrachtung in Bezug auf Compliance durch und von IT erfolgt nicht. Damit bildet es den Trigger für weitere Forschungen, explizit im interdisziplinären Gebiet von KMU und IT-Compliance. Die daraus resultierende Fragestellung ist, wie damit umgegangen wird und welche Möglichkeiten bestehen, auf diese Veränderungen zu reagieren. Die Ergebnisse hierzu werden im nächsten Themenschwerpunkt beschrieben.

4.2 Compliance-Management-Systeme & Best-Practice-Ansätze

Ein weiterer Themenschwerpunkt zielt auf Compliance-Management-Systeme und Best-Practice-Ansätze (Rahmenwerke) ab. Wie bereits im Abschn. 2 beschrieben, decken diese Rahmenwerke unterschiedliche Anforderungen, mit dem Ziel einer Sicherstellung von IT-Compliance ab. Kardel beschreibt die meist sehr begrenzten Ressourcen in KMU und der damit erschwerten Umsetzung gängiger Rahmenwerke. Als mögliche Vorgehensweise sieht er eine Kombination von verfügbaren IT-Managementmodellen. Zunächst sollte mittels der Risikoanalysemethode OCTAVE die Identifizierung von Assets und ihren Schutzbedarf ermittelt werden. Im nächsten Schritt erfolgt die Evaluierung von IT-Komponenten nach dem BSI-Grundsatzkatalog, um zuletzt nach dem Reifegradmodell CCMI eine Bewertung der Verbesserung der Prozesse durchzuführen (Kardel 2011).

Eine empirische Studie (Barlette und Fomin 2008) befasste sich mit der Eignung von IT-Sicherheitsmanagement-Standards für KMU in Frankreich mit dem Ergebnis, dass weniger als 20 % dieser Unternehmen ein betriebliches IT-Sicherheitsmanagement oder einen Notfallplan vorliegen haben. Dies stellt einen offensichtlichen Schwachpunkt im Vergleich zu Großunternehmen dar. Des Weiteren stellte die Studie heraus, dass eindeutige Unterschiede zwischen den tatsächlich eingeführten IT-Sicherheitsmaßnahmen und den vorhandenen IT-Sicherheitslücken vorhanden sind. KMU fokussieren sich überwiegend auf die Vermeidung der mit niedriger Eintrittswahrscheinlichkeit existierenden Bedrohungen, anstatt kostspieligerer und häufig auftretender Bedrohungen vorzubeugen. Zudem werden überwiegend die Anreize einseitig auf einen technologischen Schwerpunkt, wie Virenschutz gesetzt und nicht im Sinne einer ganzheitlichen Sicherheitsstruktur auch organisatorische Maßnahmen gelebt.

In einer weiteren Studie (Kolek 2018) wurde die Akzeptanz von IT-Rahmenwerken in Deutschland erforscht. Inhalt war deren Eignung hinsichtlich Unternehmensgröße sowie auftretende Herausforderungen bei deren Einführung. Der Untersuchungsgegenstand wurde begrenzt, sodass nur Unternehmen betrachtet wurden, die einen Umsatz von mehr als 2 Mio. € pro Jahr erzielen und mehr als 40 Mitarbeiter beschäftigen. Eine große Herausforderung für diese Unternehmen ist das mangelnde Wissen über die effiziente Umsetzung von Rahmenwerken und Standards. Dies ist insbesondere auf große Schwierigkeiten mit bereits etablierten IT-Rahmenwerken und deren extreme Anzahl an Anforderungen zurückzuführen, die in keinem Verhältnis zur Kapazität eines mittelständischen Unternehmens stehen. Die Rahmenwerke sind generisch aufgebaut, um idealerweise alle Anforderungen an Compliance innerhalb eines Unternehmens abzudecken. Es fehlt ein Vorgehen, das die Möglichkeiten und Fähigkeiten von KMU berücksichtigt, um IT-Prozesse eigenständig und im Sinne einer effizienten Compliance-Struktur umzusetzen (Zeller et al. 2016). Eine weitere Ursache ist die komplexer werdende Architektur der IT, die nicht mehr nur aus klassischen Mainframe-Systemen besteht, sondern dezentraler aufgebaut ist. Hinzu kommen sich ständig beschleunigende Technologiezyklen, die die Etablierung einer effizienten Compliance erschweren (Schäfer et al. 2008).

Aus den genannten Gründen sollte nochmal genauer bewertet werden, inwiefern die Übertragbarkeit von Konzepten aus großen Unternehmen in KMU übernommen

werden kann. Dabei sollten KMU-spezifische Merkmale wie geringe Verfügbarkeit von Ressourcen beachtet werden. Wie Studien zeigen, stellt die Anwendung der Referenzmodelle hier offensichtlich ein Problem dar. Zudem gibt es keine empirische Untersuchung, die explizit die Gründe und Motive von fehlenden IT-Compliance-Maßnahmen in KMU untersucht.

4.3 IT Outsourcing und Compliance

Als dritter Themenschwerpunkt wurde der Bereich IT-Outsourcing und Compliance identifiziert. Hierbei geht es um eine alternative Möglichkeit, IT-Compliance sicher zu stellen. Neben dem Outsourcing klassischer Bereiche wie der Betrieb der Infrastruktur oder des Rechnungswesens stellt das Auslagern von operativen IT-Compliance-Aufgaben auf externe Dienstleister eine besondere Form dar. Darunter wird die ganzheitliche Auslagerung der Planung und Durchführung aller operativen Aufgaben entlang des IT-Compliance-Prozesses und dessen kontinuierliche und nachweisbare Erfüllung der relevanten Vorgaben verstanden (Strasser und Wittek 2013). Die Auslagerung dieser Prozesse können Vorteile mit sich bringen, wie eine breite Fachexpertise des Dienstleisters, Neutralität oder der Einsatz standardisierter Verfahren.

Die steigende Nutzung von Cloud-Anwendungen könnte diesen Trend ebenfalls verstärken (Weiss 2016). Ferner muss aber auch beachtet werden, dass beim Outsourcing von IT-Compliance-Aufgaben die Risiken sowie die Verantwortung nicht auf externe Dienstleister übertragen werden kann und somit immer im eigenen Unternehmen verbleiben (Paulus 2011). Nichtsdestotrotz könnte dieses Modell, das aktuell noch eine Marktlücke darstellt, insbesondere für KMU von Interesse sein, da hiermit vor allem das teure Vorhalten von Personal entfallen würde.

5 Fazit und Ausblick

Festzustellen ist, dass die Literaturrecherche sehr heterogene Ergebnisse geliefert hat. Es gibt keine Publikation, die sämtliche Fragestellungen des Themas wissenschaftlich fundiert vereint. Notwendig sind ein Vergleich und eine kritische Auseinandersetzung mit den von den Autoren vorgestellten Forschungen.

Die dynamischen Themenbereiche rund um Digitalisierung und deren Auswirkungen werden in der Wissenschaft und Praxis kontrovers diskutiert und zeigen eindeutig auf, dass es zu Veränderungen in der Organisation und IT Architektur kommen wird. Welche Auswirkungen damit auf die Compliance-Maßnahmen von KMU bestehen, werden nur im Generellen beschrieben. Eine Spezifizierung auf den Teilbereich IT-Compliance wird nicht durchgeführt. Dies ist generell herauszustellen und begründet somit eine Grundlage für weitere Forschungen in diesem Bereich.

In der Theorie geben die Rahmenwerke den Soll-Zustand mit dem Ziel einer Sicherstellung von IT-Compliance vor. Bei der Implementierung, respektive Nutzung dieser Rahmenwerke, scheint jedoch eine große Lücke zwischen KMU und großen Unternehmen vorhanden zu sein. Die Rahmenwerke sind generisch aufgebaut, um idealerweise alle Anforderungen abzudecken. Für große Unternehmen, die

mit den nötigen Ressourcen ausgestattet sind, stellt die Anwendung und Anpassung der eigenen Prozesse und Strukturen an die Modelle keine großen Probleme dar. Bei KMU hingegen fehlt ein Vorgehen, unter Berücksichtigung der Möglichkeiten und Fähigkeiten von mittelständischen Unternehmen, um ihre Prozesse eigenständig und im Sinne einer effizienten Compliance-Struktur anzupassen. Die Anwendung der Referenzmodelle stellt hier offensichtlich ein Problem dar. Wie Studien zeigen liegen bei mittelständischen Unternehmen die Compliance Strukturen weit hinter den notwendigen Maßnahmen zurück. Allerdings liegen bislang keine Ergebnisse einer übergreifenden empirischen Untersuchung vor, die die Gründe und Motive von fehlenden IT-Compliance-Maßnahmen in KMU untersucht. Dies bildet eine weitere Forschungsgrundlage und sollte im Rahmen einer weiteren Arbeit beantwortet werden.

Gerade mittelständische Unternehmen, die mit ihrer Innovationskraft und Wertschöpfung die Wirtschaft vorantreiben, sollten eine effiziente IT-Compliance nicht vernachlässigen. Die Veränderungen werden die Notwendigkeit noch weiter verstärken. Demzufolge scheint es angeraten, weitere Forschungen in diesem Bereich durchzuführen und neben den Motiven und Gründen, weshalb IT-Compliance-Maßnahmen nicht in der notwendigen Form umgesetzt werden, auch Handlungsempfehlungen zu eruieren. Die bereits genannten Möglichkeiten wie Outsourcing-Modelle könnten eine durchaus plausible Möglichkeit darstellen, die IT-Compliance in KMU zu verbessern.

Funding Open Access funding provided by Projekt DEAL.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Literatur

- Barlette Y, Fomin VV (2008) Exploring the suitability of IS security management standards for SMEs. In: Hawaii International Conference on System Sciences (HICSS) Waikoloa, Big Island Hawaii, S 1–10
- Brand K, Boonen H (2005) IT Governance: Das Taschenbuch basierend auf COBIT. Van Haren, Zaltbommel
- Capgemini (2016) Studie IT-Trends 2016. Digitalisierung ohne Innovation. Capgemini Consulting, Paris
- Falk M (2012) IT Compliance in der Corporate Governance. Anforderungen und Umsetzung. Springer, Wiesbaden
- Grüniger S, Schöttl L, Quintus S (2014) Studie Compliance im Mittelstand. HTWG Konstanz, Konstanz
- Heschl J, Middelhoff D (2005) IT Governance. Modelle zur Umsetzung und Prüfung. Books on Demand GmbH, Norderstedt

- Johannsen W, Goeken M (2007) Referenzmodelle für IT Governance. Strategische Effektivität und Effizienz mit COBIT, ITIL & Co. Dpunkt, Heidelberg
- Kardel D (2011) IT-Sicherheitsmanagement in KMU. HMD 48(5):44–51
- Klotz M (2009) Facetten der IT-Compliance. IT-Serv Manag 4(9):5–8
- Klotz M (2011) Regelwerke der IT-Compliance – Klassifikation und Übersicht Teil 1: Rechtliche Regelwerke. SIMAT Stralsund Information Management Team, Fachhochschule Stralsund, No. 03-11-011, Stralsund. <http://nbn-resolving.de/urn:nbn:de:0226-simat03110110>
- Knoll M (2017) IT-Risikomanagement im Zeitalter der Digitalisierung. HMD 54(1):4–20
- Kolek E (2018) IT Sicherheit der Digitalisierung in Kleinen und Mittleren Unternehmen: Eine literaturbasierte und empirische Studie von Effekten und Barrieren. In: Multikonferenz Wirtschaftsinformatik (MKWI), S 1706–1717
- Kronsnabl S (2010) Vorstellung der Studienergebnisse: IT-Sicherheitsstandards und IT-Compliance. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschrift/3GS_Tag_2010/IBI_Kronsnabl.pdf?__blob=publicationFile&v=1. Zugegriffen: 30. Okt. 2019
- Legner C, Eymann T, Hess T, Matt C, Böhm T, Drews P, Mädche A, Urbach N, Ahlemann F (2017) Digitalization: opportunity and challenge for the business and information systems engineering community. Bus Inf Syst Eng 59(4):301–308
- Ley C, Bley K (2016) Digitalisierung: Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. HMD 53:29–41
- Lindner D, Ludwig T, Amberg M (2018) Arbeit 4.0 – Konzepte für eine neue Arbeitsgestaltung in KMU. HMD 55(5):1065–1085
- Ludwig T, Kotthaus C, Stein M, Durt H, Kurz C, Wenz J, Doublet T, Becker M, Pipek V, Wulf V (2016) Arbeiten im Mittelstand 4.0-KMU im Spannungsfeld des digitalen Wandels. HMD 53:71–86
- Nilles M, Senger E (2012) Nachhaltiges IT-Management im Konzern – von den Unternehmenszielen zur Leistungserbringung in der IT. HMD 49(2):86–96
- Paulus S (2011) Outsourcing von GRC-Aufgaben im Mittelstand. Risk Fraud Compliance 6(1):31–35
- Schäfer G, Strolz G, Hertweck D (2008) IT Compliance im Mittelstand. HMD 45(5):69–77
- Strasser A, Wittek M (2013) Dienstleistungsspektrum der IT Compliance. HMD 50(4):33–41
- Strasser A, Wittek M (2012) IT Compliance. Informatik Spektrum 35(1):39–44
- Uhl A, Heinrich P, Günthner R (2018) IoT-basierte Geschäftsmodelle für den Schweizer Mittelstand – Konzepte für die digitale Zukunft. HMD 55(2):271–283
- 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 J (2004) IT governance: how top performers manage IT decision rights for superior results. Harvard Business School Press, Boston
- Weiss A (2016) Ohne Cloud ist das Scheitern der KMU vorprogrammiert. Wirtschaftsinform Manag 5:52–54
- Zeller V, Hoffmann J, Gruber M, Schuh G (2016) GradeIT – Prozessqualität bei kleinen und mittleren IT-Service-Providern. HMD 53(2):200–212
- Zimmermann V (2017) Unternehmensbefragung 2017 – Digitalisierung der Wirtschaft: breite Basis, vielfältige Hemmnisse. KfW Bankengruppe, Frankfurt