Technische Hochschule
Brandenburg
University of
Applied Sciences

IT-Governance, Risiko- und Compliance-Management (IT-GRC) für KMU – Literaturanalyse und Ansatzbildung

Andreas Johannsen, Daniel Kant

Ergebnisse einer Studie durch das Institut für Betriebliche Integration und Digitalisierung (IBID)

am Fachbereich Wirtschaft der Technischen Hochschule Brandenburg

Impressum

Autoren: Andreas Johannsen, Daniel Kant

Schriften des Instituts für Betriebliche Integration und Digitalisierung (IBID)
Herausgeber: Prof. Dr. Andreas Johannsen, Technische Hochschule Brandenburg
8. Jahrgang 2020

Druck: Druckerei der Technischen Hochschule Brandenburg
Kontakt: Technische Hochschule Brandenburg
University of Applied Sciences
Magdeburger Str. 50
14770 Brandenburg an der Havel
T +49 3381 355 - 101
F +49 3381 355 - 199
E andreas.johannsen@th-brandenburg.de
ibid.th-brandenburg.de
ISBN: 978-3-945500-05-7
ISSN 2198-090X
Stand: 27. Mai 2020

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Abstract

Kleine und mittlere Unternehmen aller Branchen versuchen sich nach wie vor angemessen mit den Herausforderungen der Globalisierung und der digitalen Transformation auseinanderzusetzen. Das vorliegende Arbeitspapier beschreibt eingangs Merkmale von KMU und wachsende Herausforderungen in den Bereichen IT-Governance, IT-Risikomanagement und IT-Compliance (IT-GRC) für KMU, sowie empirische Befunde zur tatsächlich realisierten IT-Governance, IT-Sicherheit und IT-Compliance. KMU bauen derzeit Kompetenzen und Lösungen in der Produktionsautomatisierung (Industrie 4.0) als auch der digitalen Geschäfts- und Verwaltungsprozesse auf. In Bezug auf IT-GRC sind KMU faktisch jedoch oft noch unreif. Bestehende Ansätze des IT-Governance-, Risiko- und Compliance-Managements sind unseres Erachtens noch zu wenig für KMU ausgestaltet. Das Arbeitspapier stellt vor diesem Hintergrund einen zunächst aus der Literatur abgeleiteten, und dann zusammen mit Feedback von 14 IT-GRC Experten aufgestellten, Kompetenz-orientierten Ansatz zur Wahrnehmung, Messung und Steuerung des IT-Governance, Risiko- und Compliance-Managements in KMU vor, der sechs relevante Kompetenzkategorien enthält. Es stellt dann zwei webbasierte Tools zur Messung und Erfassung der Handlungsbedarfe und zur Unterstützung von Management-Maßnahmen vor. Der Ansatz sowie die prototypisch realisierten Tools unterstützen das IT-GRC Management von KMU Reifegrad-abhängig und Bedarfs-orientiert. Bei der Unterstützung wird der Fokus darauf gelegt, KMU bei der Umsetzung der ständig wachsenden IT-GRC-Anforderungen schlanke und konkrete Methoden, Werkzeuge und Hilfsmittel an die Hand zu geben, und die verschiedenen Stakeholder einzubinden.

2 KMU und IT-Governance, Risiko- & Compliance-Management

2.1 Motivation und Zielsetzung

Kleine und mittlere Unternehmen (KMU) sehen sich zunehmend den Herausforderungen der digitalen Transformation gegenübergestellt, um weiter wettbewerbsfähig zu bleiben. Den Chancen der digitalen Transformation nahezu sämtlicher Märkte und Branchen stehen Risiken und Hemmnisse gegenüber, die sich aus den Informationstechnologien und der mit ihnen verbundenen Regulierung im Bereich Datenschutz als auch erforderlicher Kompetenzen und Strukturen zur IT-Sicherheit ergeben. In einem dreijährigen Projekt (KIW 2020a) im Rahmen des BMWi-Programms „Mittelstand Digital" suchen wir nach Ansätzen, die Digitalisierung von IT-KMU zu steuern und dabei auch alle Bereiche angemessen zu beachten, die betroffen sind, um auch Informationssicherheit und Datenschutz ganzheitlich und rechtskonform anzugehen. Bestehende Ansätze, insbesondere die des Governance-, Risk- und Compliance-Managements (GRC), sind noch zu wenig für KMU ausgestaltet (Knoll und Strahringer 2017), seien sie nun anwendende KMU oder KMU der IT-Branche (IT-KMU). (Albayrak und Gadatsch 2017) stellen im Rahmen ihrer empirischen Erhebung für KMU fest, dass eine Segregation von Aufgabenträgern für GRC-Aufgaben oft schwer möglich ist, und schlagen daher eine besondere, KMU-geeignete IT-Steuerungsorganisation sowie IT-Projektstrukturen vor. Daher zielt dieses Arbeitspapier darauf ab, folgende Forschungsfrage zu beantworten:

Wie kann ein Ansatz des IT-Governance-, Risiko- und Compliance-Managements gestaltet sein, mit dem KMU die digitale Transformation rechtskonform und sicher steuern können, und auf dessen Basis sowohl empirische Erhebungen als auch Managementempfehlungen in Bezug auf Kompetenzen, Unterstützungsmaßnahmen und praxisgerechte Werkzeuge für KMU abgeleitet werden können?

2.2 Merkmale von KMU

Es wird hierbei der KMU-Definition des ifM Bonn gefolgt, das neben definierten Umsatzgrenzen ein Unternehmen mit 10 bis 49 Mitarbeitern als Kleinunternehmen einordnet, und mit einer Mitarbeiteranzahl von 50 bis maximal 499 sowie höchstens 50. Mio € Umsatz im Jahr als mittleres Unternehmen definiert (ifM Bonn 2016). KMU unterscheiden sich von Großunternehmen jedoch nicht nur quantitativ, sondern auch qualitativ.

Die Literatur weist wesentliche qualitative Merkmale von KMU aus, siehe u.a. (Todesco 2010), (Lindner 2019) und (Leeser 2020). Demnach hat die Geschäftsführung eines KMU maßgeblichen und persönlichen Einfluss auf alle strategischen Entscheidungen und trägt das unternehmerische Risiko, das Unternehmen sichert die persönliche Erwerbs- und Existenzgrundlage der Geschäftsführung, es liegt oft eine starke Nischenexpertise und langjährige Miterbeiterkompetenzen vor, und es gibt geringe Budgetgrenzen im Vergleich zu Großunternehmen. Schließlich ist in KMU die Durchführung von Aufgaben hinsichtlich der IT oder Digitalisierung oft neben den normalen Aufgaben des Tagesgeschäftes zu leisten. Dennoch sind KMU alles andere als eine homogene Gruppe von Unternehmen. Insbesondere ist eine Differenzierung nach kleinen und mittleren Unternehmen vorzunehmen, da insbesondere kleine Unternehmen oft über keine eigene IT-Abteilung verfügen, im Vergleich zu mittleren Unternehmen mit zunehmend eigener IT-Abteilung (Hillebrand et al. 2017, S. 55).

2.3 Herausforderungen für KMU

Im Zeitraum der Literaturanalyse (2012 bis 2020) werden als allgemeine Herausforderungen für KMU wiederholt die Wettbewerbs- und Innovationsfähigkeit, die Digitalisierung, wirtschaftspolitische und gesellschaftliche Rahmenbedingungen (Fachkräftemangel, Anstieg Altersstruktur) sowie Finanzierungshemmnisse genannt, siehe z.B. (Welter et al. 2014) oder (Wagner 2017). Im Bereich der Digitalisierung sind die größten Herausforderungen für KMU die Qualifizierung der Mitarbeiter, die Datensicherheit und der Datenschutz, die Definition von für KMU geeigneten Industriestandards und -Plattformen, der Rollenwandel der IT hin zu Cloud Computing und professionellem IT-Servicemanagement, als auch generell fehlende Ressourcen (Leeser 2020), (Becker et al. 2017), (Demary et al. 2016).

In Bezug auf den Reifegrad des IT-GRC Managements in KMU werden folgende Herausforderungen im Rahmen unserer Literaturanalyse häufiger genannt (vergleiche Bömelburg und Zähres 2015): erhöhte

Risiken durch Familienkonflikte oder Entfernung der Eigentümer vom Management (Nachfolge), weniger ausgeprägte Rechnungswesen- und Controllingsysteme, sowie Insolvenzrisiken und Finanzierungsprobleme. Sie plädieren als Lösung für ein integriertes GRC-System. Todesco (2010) berichtet besonders bei kleinen Unternehmen von mangelnder kaufmännischer Ausbildung und strategischer Orientierung der Unternehmer.

Die jüngere Empirie zeigt nach wie vor eklatante Lücken bei KMU in Bezug auf IT-GRC Kompetenzen. Im Jahr 2018 gaben laut einer Bitkom-Studie 73% der KMU an, bereits von Datendiebstahl oder Cyberspionage aktiv betroffen gewesen zu sein (Bitkom 2018). Die Dunkelziffer dürfte höher liegen. Neben Reputationsverlusten können in der Folge sogar Regressansprüche bis zu 4% des gesamten weltweit erzielten Jahresumsatzes anstehen (Artikel 82 der DSGVO). Neben der IT-Compliance weisen KMU auch bei der IT-Governance erheblichen Nachholbedarf auf. Wichtige verantwortliche Stellen fehlen - ein IT-Sicherheitsbeauftragter ist nur in 13% der kleinen Unternehmen vorhanden (Hillebrand et al. 2017). Es existieren gerade bei schwergewichtigen Governance-Frameworks wie COBIT Einführungsbarrieren in kleinen und mittleren Unternehmen (van Landeghem und Deschoolmeester 2014). Diese liegen u.a. darin, dass Teile des Ansatzes, wie z.B. die sieben „Enabler", noch weitgehend vom KMU ausspezifiziert werden müssen, und umfassende Anforderungen und Prozessempfehlungen beherrscht werden müssen (Beißel 2017).

Aktuelle Studien zeigen jedoch, dass trotz einer in den letzten Jahren deutlich gestiegenen Risikowahrnehmung bei KMU die Bereitschaft, aktiv Maßnahmen zur IT-Sicherheit und IT-Compliance durchzuführen, weiterhin gering ist (Henseler-Unger und Hillebrand 2018) sprechen daher von einer „Umsetzungslücke", und fragen nach den Beweggründen für die mangelnde IT-Sicherheitskultur.

Diese „Umsetzungslücke" sollte nicht mit mono-kausalen Erklärungsmustern abgetan werden. Hilfreich können Ansätze sein, die verschiedene Sichtweisen aufdecken. Bei den Entscheidern stehen z.B. meist fehlende Ressourcen im Vordergrund, daneben fehlt hier noch IT-GRC Problembewusstsein, bei den IT-Abteilungen werden die Mitarbeiter als größte „Schwachstelle" der IT-Sicherheit gesehen, die Mitarbeiter als „Nutzer" vermissen demgegenüber oft die Sichtweise einer „usable security" bei den IT-Verantwortlichen (Passwörter müssen kryptisch und lang sein, USB-Schnittstellen werden von IT-Verantwortlichen deaktiviert etc).

2.4 Kritik bisheriger IT-GRC Ansätze für KMU

(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. Wir orientieren uns an diesem ausgereiften Ansatz, stellen aber fest, dass dieser für KMU noch eines „Tailorings" bedarf. (Henschel und Heinze 2016) präsentieren zwar 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.

Am Beispiel des Bereichs IT-Risk wird von (Beißel 2017) aufgezeigt, wie vorhandene Rahmenwerke sinnvoll differenziert werden können. Für das Risikomanagement liegen insb. mit den Frameworks CRAMM, FRAAP, OCTAVE-S und TARA KMU-geeignete Ansätze vor, die allerdings nicht alle IT-GRC Bereiche integriert umfassen. Schließlich seien stellvertretend (Anke et al. 2017) als ein weiteres Beispiel eines zwar gelungenen methodischen Ansatzes genannt, der jedoch nur Teilbereiche, hier Teile der IT-Compliance, abbildet. Gleiches gilt für den aus der Literatur abgeleiteten IT-Compliance-Ansatz von (Deistler und Rentrop 2020).

Unsere Literaturanalyse zu GRC-Ansätzen ergab, dass bisherige Ansätze, Standards und Metriken zum großen Teil nicht mittelstandsgerecht und daher bei deutschen KMU weitgehend unbekannt oder nicht verbreitet sind. Nicht verbreitet ist zum Beispiel das fünfstufige Reifegradmodell des NIST in Form des Federal Information Technology Security Assessment Framework. Das COBIT-5 und aktuell COBIT 2019 Prozessreferenzmodell ist bei KMU zum Teil bekannt, aber nicht verbreitet (Klotz 2019). COBIT-5 besteht aus den beiden übergreifenden Prozessdomänen „Governance" und „Management" sowie insgesamt 37 Prozessen (siehe Müller 2018, S. 170). Im deutschsprachigen Raum ist der Ansatz des BSI Grundschutzes zwar Standard, aber bei vielen KMU noch nicht etabliert (Hillebrand et al. 2017).

2.5 Kritik bisheriger IT-GRC Werkzeuge für KMU

Umfassende GRC-Suiten großer Anbieter richten sich mit ihrem Funktionsumfang sowie ihrer Modul-Komplexität an Großunternehmen (Bhattarcharyya 2019), (SAP 2019). Hofmann und Hofmann (2017) untersuchten 36 verbreitete, schlankere kommerzielle IT-GRC- als auch ISMS-Werkzeuge, mit dem Ergebnis, dass diese die Anforderungen der ISO 27001 in der Regel nicht vollumfänglich erfüllen. Bereits (Rehäußer 2015) fand in seiner ISMS-Marktstudie heraus, dass die untersuchten Werkzeuge eine zum Teil noch mangelhafte ISMS-Prozessunterstützung aufwiesen.

Im deutschsprachigen Raum ist der IT-Sicherheits-Ansatz des BSI Grundschutzes De-facto-Standard, jedoch verlieren sich die Verantwortlichen in KMU trotz der Option einer „BSI Basisabsicherung" hier schnell in über 4000 Seiten Dokumentation. Open Source oder Lizenz-basierte ISMS-Softwareprodukte wie z.B. (Verinice 2019) sind geeignet, wenn ein mittleres Unternehmen den BSI-Grundschutz umsetzen will (Hofmann und Hofmann 2017) oder um eine Zertifizierung nach ISO 27001 anzustreben. Jedoch sind diese Werkzeuge mit einem erheblichen ISMS-Einführungs- und Betriebsaufwand verbunden, den kleine Unternehmen eher meiden.

Schlanke und explizit für kleine und mittlere Unternehmen konzipierte Vorgehensmodelle und Werkzeuge wie (ISIS12 2018) und ISA+ (ISA 2020) nehmen demgegenüber eine Reduzierung der IT-

Grundschutz-Kataloge sowie der ISO/IEC 27001 vor, um so die Einführung eines mittelstandsgerechten ISMS zu erleichtern. Aufgrund des leichtgewichtigen Ansatzes eignet sich ISIS12 lediglich als ISO-Vorstufe. Außerdem fehlt es an Export- und Importfunktionalitäten zu Managementsystemen oder Schwachstellenscannern. Die ISIS12-Bausteine und Maßnahmen basieren auf dem IT-Grundschutz-Kompendium, und weisen im Bereich der IT-Governance und des IT-Compliance Managements Lücken auf.

Auf dem Softwaremarkt gibt es noch kaum integrierte IT-GRC-Werkzeuge, die auch für KMU geeignet sind. Die derzeitig verfügbaren ISMS-Werkzeuge für den Zielmarkt der KMU sind in Bezug auf eine Einbettung in eine IT-Strategie und –Planung, ein internes Kontrollsystem (IKS) nach (Albayrak und Gadatsch 2017), sowie umfassende und dennoch konkrete IT-Compliance Unterstützung vielfach noch unzureichend umgesetzt (Hofmann und Hofmann 2017).

Zusammenfassend stellen wir fest, dass bei den dediziert für KMU entwickelten IT-GRC Werkzeugen eine Einbettung in eine IT-Strategie und –Planung, ein internes Kontrollsystem (IKS) nach (Albayrak und Gadatsch 2017), umfassende und dennoch konkrete IT-Compliance Unterstützung, sowie die Bedeutung von Mitarbeiter-bezogenen Maßnahmen für die Informationssicherheit vielfach noch unzureichend umgesetzt sind.

3 Methodik

Da es für Großunternehmen und auch den gehobenen Mittelstand bereits vielfältige Quellen zur obigen Forschungsfrage gibt, wurde zuerst eine Literaturanalyse durchgeführt, um Themenbereiche zu identifizieren und relevante Kategorien zu entwerfen. Die aus der Literaturanalyse gebildeten acht Kategorien wurden dann mit der Bitte um Feedback 14 IT-GRC-Experten gezeigt. Aus dem Expertentest der Kategorien entstanden daraufhin sechs finale Kategorien mit leicht angepassten Inhalten. Nach dieser ersten Evaluation des Ansatzes folgten Entwurfs- und Evaluationsphasen für zwei aus dem Ansatz abgeleitete Werkzeuge, die am Ende des Beitrags kurz vorgestellt werden. Die weiteren Entwurfs-, Evaluations- und Diffusions-Iterationen der beiden Werkzeuge gemäß Konstruktionsorientiertem Forschungsansatz werden Inhalt von separaten Publikationen sein.

3.1 Schritt 1 und 2: Literatursuche und Reduzierung

Unsere Literaturanalyse ist methodisch ähnlich wie bei Lindner und Ley (2019) in vier Schritten aufgebaut, welche die Digitalisierung von KMU untersuchten und zu Implikationen für die IT-Organisation mit besonderem KMU-Fokus kamen. Im ersten Schritt wurde die Literatursuche an sich vorgenommen. Wir bildeten auf Deutsch und Englisch den Suchstring

- KMU AND (Governance OR Risk OR Compliance OR Sicherheit).

Zeitlich wurde die Suche auf die Jahre 2012 bis 2020 reduziert, da eine vorgelagerte händische Suche ergab, dass aufgrund der dynamischen Entwicklungen unter anderem bei Technologien und Regulierung im GRC-Umfeld vor 2012 kaum relevante Ergebnisse zu finden waren. Die Suche wurde auf die Datenbanken Springerlink (https://link.springer.com), IEEE Explore (https://ieeexplore.ieee.org) und WISO (https://www.wiso.net.de) als auch EconBiz (https://www.econbiz.de/) und ein Vorkommen der Suchbegriffe bei WISO im Titel und Abstract reduziert. Die initiale Suche ergab insg. 1622 Treffer, die allesamt als .csv exportiert wurden.

Alle Treffer wurden anhand der Relevanz zur Forschungsfrage betrachtet und dann die Anzahl der Treffer reduziert. Die Treffer wurden erst dann nach allgemein unternehmensrelevanter und IT- sowie KMU-relevanter Literatur reduziert. Dazu wurden Titel und Keywords nach Stichworten wie „KMU" und „SME" ausgewertet. Nach dieser inhaltlichen Prüfung blieben 534 Treffer übrig.

3.2 Schritt 3 und 4: Kategorienbildung und Auswertung

Im dritten Schritt wurden die verbliebenen Treffer zu inhaltlichen Kategorien zugeordnet. Aus 342 Publikationen (ca. 65%) wurden von den Autoren gemeinsam acht Kategorien gebildet, aus 35% der Publikationen wurden keine Kategorien gebildet, da es sich um spezielle Einzelthemen mit zu geringer Trefferanzahl oder allgemeiner KMU-Relevanz handelte.

Zur Inhaltsanalyse wurden aus jeder Kategorie für KMU inhaltlich relevante Artikel ausgewählt, wobei schlussendlich auch die Aktualität der Artikel zur Priorisierung herangezogen wurde. Im Ergebnis wurden so insgesamt 238 Publikationen vollständig gelesen und ausgewertet. Die Kategorien werden im Kapitel 3 erläutert.

3.3 Expertentest des Ansatzes und der Kategorien

Die Kategorien mit jeweils einer Kurzbeschreibung der Kategorien wurden 14 Experten ausgehändigt. Alle Experten haben IT-GRC-Erfahrung, und zwar durchschnittlich 15 Jahre. Sie sind entweder als Forscher (50%), als ISB bzw. Referent Unternehmenssicherheit (28%) oder als Geschäftsführer bzw. IT-Leiter (22%) von KMU-Organisationen der Sicherheitsbranche tätig. Sämtliches Feedback wurde schriftlich gegeben und von den beiden Autoren in zwei Workshops qualitativ ausgewertet. Die Anpassungen werden ebenfalls im Kapitel 4 erläutert.

3.4 Entwicklung zweier IT-GRC Werkzeuge für KMU

Auf Basis der aus der Literaturanalyse abgeleiteten KMU-Anforderungen und der finalen sechs Kategorien des IT-GRC Ansatzes für KMU wurden abschließend zwei Tools für die Projektarbeit mit KMU konzipiert, zum einen ein IT-GRC Reifegradermittlungs-Werkzeug und eine IT-GRC Information Security Toolbox zur Unterstützung des Aufbaus und Betriebs eines integrierten, IT-basierten GRC-Managements in KMU.

3.5 Empirische Erprobung zweier IT-GRC Werkzeuge für KMU

Die erste prototypische Version unseres IT-GRC Reifegradermittlungs-Werkzeugs für KMU liegt mittlerweile vor, und wurde in einem Pretest mit zehn Geschäftsführern von IT-KMU getestet. Die Selbsteinschätzung mit den zehn Geschäftsführern wurde von Dezember 2019 bis April 2020 als Online-Befragung durchgeführt, die Ergebnisse des Pretests werden in die Verbesserung der IT-GRC Reifegradfragen eingehen. Eine empirische Erhebung des IT-GRC Reifegrads von ca. 50 KMU ist für den Sommer 2020 geplant (siehe Kapitel 6).

4 Ein Ansatz für IT-GRC in KMU

4.1 Beschreibung des Ansatzes

Kleine und mittlere Unternehmen sind, wie bisher dargestellt, oft sowohl mit der Umsetzung von IT-Sicherheitsstandards wie z.B. BSI Grundschutz, ISO 27001, etc.) überfordert, als auch was die Konformität mit umfassenden IT- und Datenschutz-Gesetzen (DSGVO, ePrivacy-Verordnung, IT-Sicherheitsgesetz 2.0 - siehe Abbildung 1) betrifft. Daher ist es notwendig, einen KMU-freundlichen Ansatz zu entwickeln, welcher die unterschiedlichen Dimensionen und Sichtweisen vereint.

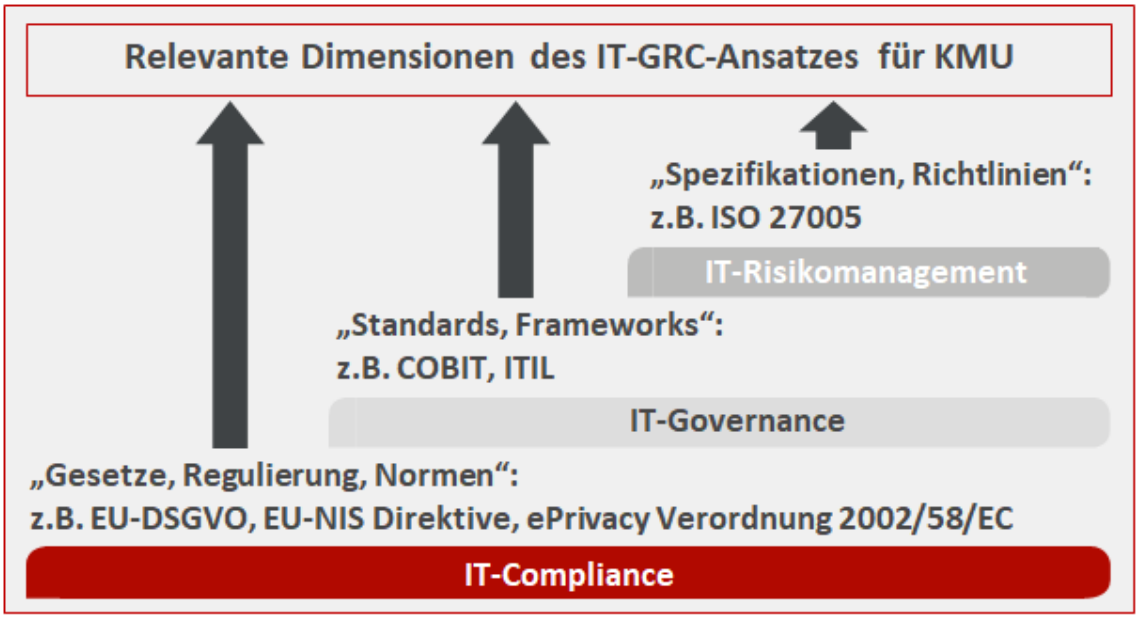

Abbildung 1 GRC als Dimensionen unseres IT-GRC-Ansatzes Quelle: Eigene Darstellung

KMU können gemäß der Literaturanalyse bei Berücksichtigung der wesentlichen relevanten Themen schon mit überschaubarem Aufwand eine signifikante Erhöhung des erforderlichen Schutzniveaus

erreichen, wenn sie alle relevanten Kompetenzen beachten. Um die Wahrnehmung und das Management der relevanten Fähigkeiten eines KMU zu unterstützen, wird auf Basis der Literaturanalyse im Folgenden ein IT-Governance, Risiko- und IT-Compliance (IT-GRC) Ansatz für KMU abgeleitet. Nach Sichtung, Priorisierung, quantitativer (Anzahl der Publikationen zum Thema/Kompetenzbereich) und inhaltlicher Analyse wurden acht Kategorien identifiziert, zu denen in Bezug auf KMU in den 1622 Treffern publiziert wurde. Es waren dies die Kategorien:

1. Information Security Awareness
2. IT-Governance
3. IT-Compliance und Datenschutz
4. Information Security Management
5. Technische und physische IT-Sicherheit
6. Cybersicherheit und Cloud Computing
7. Web Application Security und Secure Software Engineering
8. Mobile Security und BYOD

Diese Kategorien wurden den 14 Experten vorgelegt, mit der Bitte, jede Kategorie zu kommentieren und dann ein übergreifendes Feedback zur Eignung eines Ansatzes für KMU bestehend aus diesen Kategorien zu geben.

Das umfangreiche Feedback fiel in mehreren Punkten auch recht einhellig aus, d.h. es wurde von einem Drittel bis sogar der Mehrheit der Experten gleichermaßen gegeben. Dies betrifft die folgenden Punkte:

a) Die Wichtigkeit und Bedeutung aller Kategorien für die KMU-Praxis wurde bestätigt
b) Die Kategorien 5. und 7. wurden als nicht disjunkt und Teil der Kategorien 4. und 6. angesehen.
c) Die Kategorie 4. „Information Security Management (ISM)" wurde als übergreifend über viele anderen Kategorien eingestuft. Es wurde von mehreren Experten empfohlen, hier für KMU lediglich das Etablieren eines KMU-freundlichen, schlanken „ISMS" oder ISMS- Sicherheitsprozesses (z.B. nach Vorbild BSI-Standard 200-1) aufzunehmen.
d) Auch wenn die Reihenfolge keine Priorisierung bedeutete, wurde recht übereinstimmend von stark Management-bezogenen Kategorien hin zu technischen Kategorien sortiert, siehe die finale Kategorienliste unten.

Die finalen Kategorien, sind demnach:

1. IT-Compliance
2. IT-Governance
3. Security Awareness
4. ISMS
5. Cyber-Sicherheit
6. Mobile Sicherheit

Die Kategorie „ISMS" ist dabei gemäß der einschlägigen Normen (insb. BSI Grundschutz und ISO27001) sehr umfassend, jedoch wurde sie von jedem Experten als ein einzelner Bestandteil des Ansatzes bestätigt, da der Begriff ISMS in der KMU-Praxis faktisch nicht selten auf einen speziellen Unternehmensprozess, meist auf technische IT-Sicherheitsmaßnahmen, oder gar auf ein ISMS-Softwarewerkzeug reduziert wird. Die einzelnen Kategorien und ihre aus der Literatur abgeleiteten Inhalte werden im nächsten Abschnitt vorgestellt.

4.2 Kategorien

1. IT-Compliance

IT-Compliance bezeichnet nach (Klotz 2017, S. 866) einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden. Auch wenn die Compliance-Vorgaben für große Unternehmen insbesondere bei Finanzen (Prüfungsstandard IDW PS 980, AktG, KonTraG) und Prozessen (CMMI, SPICE) für KMU nicht gelten (Ahn et al. 2014), (Andelfinger und Kneuper 2014), stellen neben den für KMU relevanten Compliance-Bereichen (siehe Henschel und Heinze 2016, S. 157) die IT-Compliance und insbesondere der Bereich des Datenschutzes für KMU heute eine zentrale Herausforderung dar.

Relevanz für KMU:

Die Relevanz der IT-Compliance für KMU steigt kontinuierlich. Die rechts-konforme Generierung und Nutzung ständig steigender Datenvolumina innerhalb bekannter oder neuartiger Nutzungs- und Geschäftsmodelle (IoT, Arbeit 4.0, Industrie 4.0) einerseits und neue Gesetzgebungen andererseits stellen KMU vor erhebliche Kompetenzprobleme. Erste Praxisberichte deuten beispielsweise darauf hin, dass nur ein geringer Anteil selbst der europäischen KMU volle DSGVO-Compliance erreicht hat (Sirur et al. 2018), (Dehmel und Kälber 2019).

2. IT-Governance

IT-Governance, besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt (Bergmann und Tiemeyer 2017, S. 762). Ein bei KMU neuralgischer Punkt der IT-Governance ist die Ausgestaltung der verantwortlichen Rollen und Stellen - ab einer bestimmten Unternehmensgröße mindestens IT-Leiter, IT-Sicherheits-Beauftragter,

und Datenschutzbeauftragter. In einer Befragung von Albayrak und Gadatsch (2017, 156) gaben über ein Drittel der KMU an, dass keine IT-Arbeitsteilung vorliege und prinzipiell „jeder alles macht". Dies wird von der Studie von Hillebrand et al. (2017, S. 56) mit 1.505 Befragten bestätigt.

Relevanz für KMU:
Wir folgern übereinstimmend mit Albyarak/Gadatsch (2017, S. 157) aus der Analyse mindestens eine IT-Steuerungsorganisation, eine IT-Strategie/IT-Planung, ein IT-Kennzahlensystem sowie IT-Projektstrukturen als wichtige Elemente für IT-Governance von KMU (siehe Tabelle 2 zu Inhalten und Kompetenzbereichen der einzelnen Kategorien). IT-Governance erfordert zudem Elemente eines IKS in Bezug auf angemessene organisatorische und personelle Maßnahmen insbesondere zur IT-Sicherheit. Diese Maßnahmen werden in KMU deutlich seltener umgesetzt als technische Maßnahmen (Hillebrand et al. 2017). Ein zunehmend wichtiges Teilgebiet der IT-Governance für KMU ist laut unserer Analyse daneben die Datensouveränität im Zuge der inter-organisationalen bzw. Cloud-basierten, kommerziellen Datennutzung, siehe (Jarke et al. 2019, S. 550), (Wohlfarth 2019), (Kant et al. 2020), (Johannsen et al. 2020).

3. Security Awareness
(Weber et al. 2019, S. 9) sehen den Begriff Security Awareness als eine Kurzform der Information Security Awareness, die sie nach (Richter et al. 2018, S. 8) als den – bezüglich der Sicherheitsgefahren – bewussten Umgang mit Informationen, unabhängig vom Medium, definieren. Unter Security Awareness sind konkret Maßnahmen im Umgang mit Informationssicherheit. gemeint bezüglich der Sensibilisierung („aufmerksam machen"), der Schulung („Lösungen vermitteln") und des Trainings („Lösungen in der Praxis üben"), siehe (Kersten und Klett 2015, S.49). Security Awareness ist ein wichtiges und wachsendes Feld der IT-Sicherheit, weil der Faktor Mensch gleichzeitig Gestalter aber auch Schwachstelle für IT-Sicherheit ist (Weber et al. 2019).

Relevanz für KMU:
Security Awareness, d.h. der bezüglich der Sicherheitsgefahren bewusste Umgang mit Informationen, Informations-Systemen oder –Technologien ist aufgrund geringeren Know-Hows in KMU besonders relevant, und kann nur erfolgreich gelingen, wenn alle Stakeholder in ihren Bereichen entsprechend sensibilisiert sind, weshalb unsere abgeleiteten Werkzeuge alle Zielgruppen bis zu den IT-Nutzern beinhaltet.

4. Information Security Management System (ISMS)
Ein ISMS ist ein System zum betrieblichen Management der Informationssicherheit, welches nach den verbreiteten Standards der ISO27001 oder des BSI Grundschutz aufgebaut wird (vgl. Kersten et al. 2020, S. 5; und Müller 2018, S. 91). Diese Kategorie beschreibt mithin Richtlinien, Verfahren und Methoden, die eine Organisation als sozio-technisches System proaktiv implementieren sollte, um die

Informationssicherheit zu steuern. Diese sind sowohl technischer Natur und beziehen sich auf IT-Systeme von Firewalls bis hin zu Sicherheitsmechanismen wie Verschlüsselung oder Authentifizierung als auch organisatorischer Natur wie z.B. das Herstellen physischer IT-Sicherheit beim Zugang zu (IT-) Räumen oder Einrichtungen.

Relevanz für KMU:
Bekannte Standards wie ISO/IEC 27001, COBIT oder BSI Grundschutz (auch in der Basis-Version für KMU) erweisen sich nach wie vor als zu komplex für viele KMU, dennoch besteht oft dringender Handlungsbedarf, ein ISMS aufzubauen. Gerade kleine Unternehmen können ein ISMS auch mit passenderen Ansätzen wie z.B. ISIS12 aufbauen, sollten dabei aber die anderen Kategorien unseres Ansatzes nicht vernachlässigen.

5. Cyber-Sicherheit
Die Cybersicherheit umfasst sämtliche Bedrohungen aus dem globalen Internet, verbundene IT und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen (Pohlmann 2019). Die ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, enthält als einschlägiger Standard wichtige Anforderungen für die Sicherheit im Internet. (Müller 2017, S. 128).

Relevanz für KMU:
Die Cyber-Sicherheit umfasst nach Müller (20173, S. 128) sämtliche Bedrohungen aus dem globalen Internet, verbundene IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen. Sie beinhaltet damit auch den Begriff und Bereich des Cloud Computings, vgl. (Krcmar et al. 2018). Aufgrund der zunehmenden Auslagerung von IT-Diensten und Infrastrukturen von KMU in die Cloud hat diese Kategorie eine zunehmende Rezeption gerade in jüngeren Publikationen unserer Literaturanalyse erfahren, was ihr steigende Bedeutung für KMU verleiht (Schonschek 2019), (Kant et al. 2020).

6. Mobile Sicherheit
Mobile Endgeräte bergen nicht nur besondere Angriffsvektoren aus Sicht der IT-Sicherheit in sich (Buck et al. 2016), (Watson und Zheng 2017), sondern sind auch aus IT-Governance Sicht (Knüpffer 2017), (Kohne et al. 2015) sowie IT-Compliance Sicht (Disterer und Kleiner 2014) ein wichtiger Problem- und Gestaltungsbereich. Compliance-Anforderungen lassen sich auch für KMU unter anderem aus der DSGVO, dem Bundesdatenschutzgesetz BDSG, aber ebenso aus Regelwerken wie den IT-Grundschutz-Katalogen des BSI oder Vorgaben aus ISO 27000 ableiten. Bring Your Own Device (BYOD) bezeichnet in diesem Zusammenhang die - aus IT-GRC-Sicht problematische - Nutzung privater Endgeräte in Unternehmen, die besonders in KMU die Regel ist, da hier grundsätzlich weniger umfangreiche

Angebote von Seiten der IT-Abteilung bei größerem Freiheitsgrad der Mitarbeiter bestehen als in großen Unternehmen (Hillebrand et al. 2017, S. 54).

Relevanz für KMU:
Gerade junge Mitarbeiter im Umfeld von Startups und KMU gehen risikofreudiger mit Daten und Apps im Netz um (Borchardt et al. 2018), (Eierdanz et al. 2019). Durch die immerwährende Erreichbarkeit beim Arbeiten 4.0 verschwimmen Grenzen (Hofmann 2018). Gerade kleine Unternehmen sind meist geprägt von Tools und Methoden aus dem Consumer-Bereich, da sie betriebliche IT-Standards weniger rigide als in Großunternehmen beachten müssen, zu IT-Konsumerisierung siehe (Urbach und Ahlemann 2018, S. 81), so dass auch hier noch großer Handlungsbedarf besteht.

Tabelle 1: Inhalte und Kompetenzbereiche der sechs Kategorien des IT-GRC-Ansatzes
Quelle: Eigene Darstellung

Kategorie	**Inhalte und Kompetenzbereiche (Auszug)**
1. IT-Compliance	Aufstellung und Umsetzung Unternehmens-ethischer Richtlinien Umsetzung der Datenschutzgrundverordnung (DSGVO) Umsetzung weiterer allg. gesetzl. Vorgaben (insb. AO, HGB, GoBD) Umsetzung interner Regelwerke und Verfahrensanweisungen Identifikation und Umsetzung relevanter externer Normen und Standards Einhaltung Branchenspezifischer Regularien und Gesetze
2. IT-Governance	Installation geeigneter IT-Steuerungsstrukturen und IT-Aufsichtsrollen Installation eines schlanken IKS als IT-Kennzahlensystem Entwicklung einer ganzheitlichen IT-Strategie mit periodischer IT-Planung Regelung von Entscheidungsfindungsprozessen zur Digitalisierung Etablierung eines IT-Investitions- und Projektmanagements Steuerung und Überwachung von IT-Ressourcen
3. Security Awareness	Erhebung Sensibilisierungsgrad der Mitarbeiter sowie des Managements Vorhandensein von Ansprechpartnern und Meldestellen Planung und Durchführung Sensibilisierungskampagne mit Maßnahmen Informieren der Mitarbeiter über aktuelle Sicherheitsbedrohungen Evaluierung von Maßnahmen zur Erhöhung des Sicherheitsbewusstseins Kenntnisse von Meldewegen und Maßnahmen bei Sicherheitsvorfällen
4. ISMS	Formulierung einer Informationssicherheitsleitlinie Tailoring & Aufbau IT-Risikomanagement (z.B. nach ISO 27005, ISIS12) Etablierung eines Notfallmanagements, im Falle von IT-KMU inkl. CERT Datensicherungs-, Berechtigungs-, und physisches Sicherheitskonzept Erstellung einer Richtlinie zur IT-Nutzung für Mitarbeiter Regelmäßige Bewertung und Anpassung von Maßnahmen (PDCA)
5. Cyber-Sicherheit	Erkennung und Prävention von Cyber-Angriffen und Malware Überwachung des Netzwerkverkehrs (z.B. Deep Packet Inspection) Etablierung einer Cloud-Richtlinie, Update- und Patch-Management Verhinderung von Datenabfluss, Logging/Monitoring von Zugriffen

Kategorie	Inhalte und Kompetenzbereiche (Auszug)
	Schutz vor gängigen Webschwachstellen Verschlüsselung der Kommunikation, Umsetzung von Security by Default
6. Mobile Sicherheit	Einsatz Mobile Application & Device Management Systems (MAM/MDM) BYOD-Richtlinie, BYOD-Nutzungsvereinbarung Dateisystem-Verschlüsselung, Fernlöschung, Fernortung Verschlüsselungsmechanismen für Fernzugriff auf Ressourcen Sicherstellung von Authentizität, Verwendung digitaler Zertifikate Black – und Whitelisting von Apps Sperrbildschirme, Passwortkomplexität, 2-Faktor-Authentifizierung

In Tabelle 1 sind die wichtigsten Inhalte und Kompetenzbereiche für KMU aufgeführt, die nach der Literaturanalyse und dem in Abschnitt 4.1 gegebenen Expertenfeedback für den IT-GRC-Ansatz Berücksichtigung gefunden haben.

5 Konzeption und Pretest des IT-GRC-Reifegrad Werkzeugs

Die Erfassung der subjektiven Wahrnehmung des IT-GRC-Reifegrads von KMU auf Basis unseres Ansatzes erfolgt in einem strukturierten Prozess mit sechs Schritten, in dem die Zielgruppen (Geschäftsführer/Vorstände, DSB, ISB, IT-Leiter, Business Owner sowie mehrere IT-Nutzer aus verschiedenen Fachabteilungen) eine Selbsteinschätzung als Online-Befragung durchführen sollen:

1. Zunächst werden lediglich je eine Hauptaussage zu den sechs Kategorien bewertet („IT-GRC-Quick Check", hierzu werden Geschäftsführer/Vorstände angesprochen).
2. Eine erste Auswertung der Bewertung dieser Hauptaussagen steht sofort als Download (PDF) zur Verfügung.
3. Für die eigentliche IT-GRC Reifegrad-Erfassung werden nach Registrierung ausgewählten Personen des KMU 36 Aussagen zur Selbsteinschätzung gemailt.
4. Zur Selbsteinschätzung durch die definierten Zielgruppen werden zu jeder der Aussagen jeweils die Bedeutung der Aussage für das KMU und die Fähigkeit des KMU Likert-skaliert bewertet. Daneben können Freitexte eingegeben werden.
5. Aus den Selbsteinschätzungen wird teilautomatisiert ein Gesamtbericht mit Empfehlungen erstellt, welcher der Geschäftsführung des KMU zugesandt wird.
6. Optional geht dieser Gesamtbericht als Input in einen IT-GRC-Workshop ein, der als Kick-Off Workshop für jeweils erforderliche IT-GRC-Maßnahmen durchgeführt werden kann.

Alle Antworten werden in einer Likert-Skala angegeben, je Aussage immer in Bezug auf die Wichtigkeit der Kompetenz bzw. Maßnahme für das Unternehmen (sehr wichtig = 5, wichtig = 4, neutral = 3, weniger wichtig = 2, nicht wichtig = 1), als auch in Bezug auf die Fähigkeit des eigenen Unternehmens

im Bereich der Kompetenz bzw. Maßnahme (sehr gut = 5, gut = 4, befriedigend = 3, ausreichend = 2, ungenügend = 1). Im Rahmen eines Pretests mit zehn Geschäftsführern von KMU wurden einige Aussagen adaptiert. Die Erhebung soll im Sommer 2020 mit ca. 50 KMU verschiedener Branchen erfolgen.

6 Beispielhafte Ergebnisse zum IT-GRC Reifegrad Werkzeug

Beide Auswertungen (Kurzauswertung zu den sechs Kategorien als pdf und teilautomatisierte Gesamtauswertung der 36 Aussagen) sind so angelegt, dass eingegebene Fähigkeiten mit eingegebenen Wichtigkeiten verglichen werden, und aus einem Wichtigkeits-Überhang grundsätzlich Schwächen und Handlungsbedarfe interpretiert werden, während gleich hohe Werte oder ein Fähigkeits-Überhang als Stärken interpretiert werden. Abbildung 2 zeigt eine erste Kurzauswertung im Rahmen eines Pretests, der vor und nochmals nach der Expertenbewertung und Reduzierung auf sechs Kategorien durchgeführt wurde. Der Pretest wurde mit sechs Geschäftsführern von kleinen IT-Unternehmen und vier Geschäftsführern von mittleren IT-Unternehmen durchgeführt. Besonders deutlich sind Handlungsbedarfe in den Kategorien „Security Awareness" und „Mobile Sicherheit", da hier die arithmetischen Mittelwerte für die Bedeutung der Kategorie für das Unternehmen höher sind als die Werte zur Fähigkeit des Unternehmens. Zusätzliche Freitextantworten waren ebenfalls möglich.

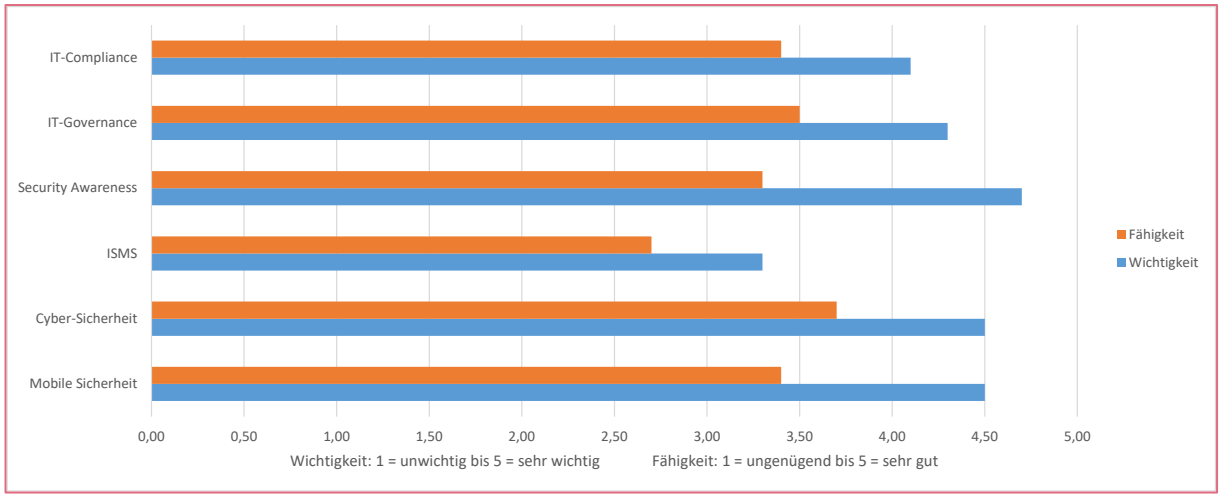

Abbildung 2 IT-Governance-, Risk- und Compliance Reifegrad von 10 IT-KMU

Quelle: Eigene Darstellung

In Abbildung 3 sind demgegenüber die Selbsteinschätzungen der Befragten zur Kategorie „Informationssicherheits-Managementsystem" sowie dazugehörigen Aussagen dargestellt. Bei den Kompetenzen „Unsere Sicherheitsrichtlinie ist verabschiedet und bekannt", und „Unser Unternehmen führt regelmäßig Sicherheitsmaßnahmen im Rahmen eines PDCA-Prozesses durch" wurde die Fähigkeit um durchschnittlich einen Likert-Wert geringer bewertet als die Wichtigkeit, so dass besonders hier Indikatoren für Handlungsbedarfe existieren.

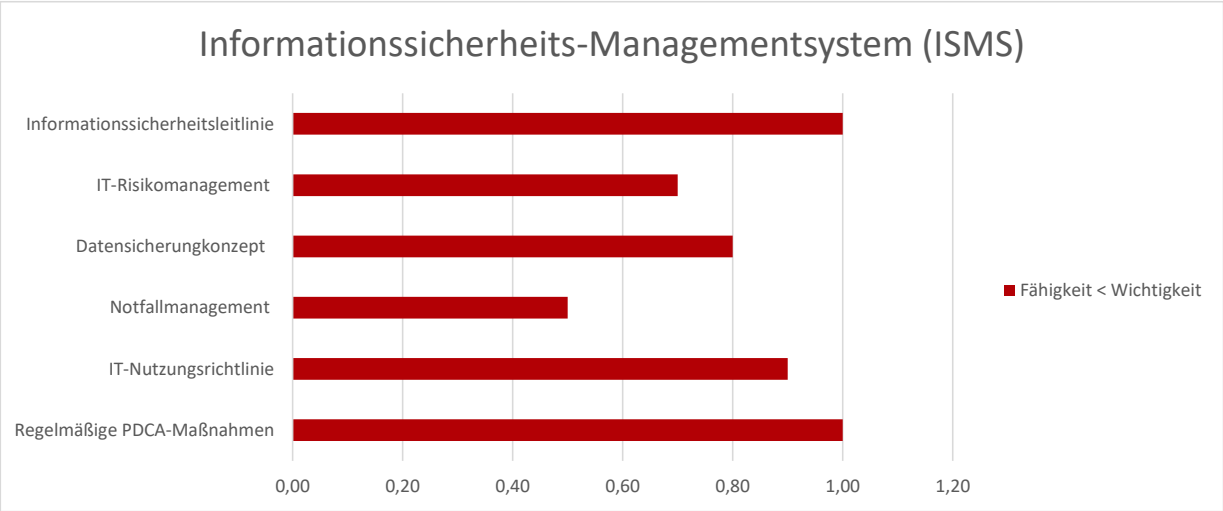

Abbildung 3 Pretest-Bewertungsergebnisse der Kategorie „ISMS" (n = 10)

Quelle: Eigene Darstellung

7 Nutzen des IT-GRC-Ansatzes für KMU

7.1 IT-GRC Reifegrad Werkzeug: Erzeugung integrativer Sichten

Der integrativen Bewertung über alle Kategorien des Ansatzes wird derzeit im prototypischen IT-GRC Reifegrad Werkzeug als einem Erhebungs- und Bewertungstool Rechnung getragen, indem bei Kategorien mit hohem Fähigkeitsüberhang empfohlen wird, Ressourcen und Aufmerksamkeit eher auf Kategorien mit Wichtigkeits-Überhang zu allokieren. Auch auf Widersprüche zwischen den eingegebenen Daten macht das Werkzeug automatisiert aufmerksam. So können unterschiedliche Wahrnehmungen eines einzelnen Teilnehmers (z.B. wurde die physische Sicherheit als sehr hoch eingestuft, aber der Aussage ebenfalls zugestimmt, dass fremde Personen jederzeit Zugang zum Serverraum hätten) oder auch unterschiedlicher Stakeholder aufgedeckt werden. Eine automatisierte Auswertung des IT-GRC-Tools zeigt zum Beispiel, dass der Geschäftsführer und der IT-Leiter der Aussage „Unsere Sicherheitsrichtlinie ist verabschiedet und bekannt" stark zustimmen, während der DSB sowie einige Business Owner und IT-Nutzer aus den Fachabteilungen dieser Aussage weniger zustimmen.

Unterschiede der Bewertungen der einzelnen Stakeholder können transparent gemacht werden, was als einer der Hauptvorteile gegenüber den derzeit verfügbaren Werkzeugen gelten kann (siehe Abschnitt „1.5 Kritik bisheriger IT-GRC Werkzeuge für KMU"). Beispielsweise bewerten die Business Owner und IT-Nutzer die Compliance sowie auch die mobile Sicherheit gemäß der Interviews mit drei Geschäftsführern zu unserem Pretest als niedrig, da sie von „Schatten-IT" und fragwürdigen Apps sowie von Umgehung der Mobile Device Management Richtlinie in ihren Unternehmensbereichen wissen, während der DSB und die IT-Leitung beide Kategorien höher bewertet, da sie von einem Richtlinien-konformen Handeln ausgehen und keine Kenntnis der Schattensysteme und Apps in den

Unternehmensbereichen hätten. In unseren bundesweiten Projektworkshops (KIW 2020a) und in von den KMU selbständig durchgeführten Workshops kann und sollte im Einzelfall geklärt werden, welche Sicht die jeweils zutreffende ist.

7.2 IT-GRC Information Security Toolbox: Management-Unterstützung für KMU

Neben dem IT-GRC Reifegrad Werkzeug als Erhebungs- und Bewertungswerkzeug besteht der zweite Baustein zum Entwurf eines Artefakts nach unserem IT-GRC-Ansatz aus der IT-GRC Information Security Toolbox, einem Werkzeug zur Unterstützung des KMU-Managements für IT-Governance, Risiko- und Compliance Management. Die Toolbox stellt unter Nutzung der im Reifegrad Werkzeug eingegebenen Daten der unterschiedlichen Stakeholder vorkonfigurierte Ergebnistypen in Form von Hilfen, Checklisten, Muster-Verträgen, Richtlinien, Formularen und Dokumenten bereit, die den Nutzern erste Orientierung bieten, jedoch noch individuell weiter auszuprägen sind. Die Tabelle 2 zeigt wichtige Beispiele dieser Ergebnisse, die zum großen Teil bereits für die erste Version entwickelt wurden und während des Projekts ständig erweitert werden, siehe (KIW 2020a).

Tabelle 2: Umsetzungshilfen der IT-GRC Information Security Toolbox
Quelle: Eigene Darstellung

Kategorie	**Muster, Checklisten, Verträge, Richtlinien etc. (Beispiele)**
1. IT-Compliance	DSGVO-Datenschutzerklärung für Webseiten (KIW-DS 2019) Muster für ADV-Vertrag nach DSGVO (KIW-ADV 2019)
2. IT-Governance	Empfehlungen zur organisatorischen Verankerung von IT-GRC-Rollen Leitfaden für IT-Programm- und Projektmanagement
3. Security Awareness	IT-Notfallkarte "Verhalten bei IT-Notfällen" (ACS 2019b) Verhaltungsregeln zum Thema Social Engineering Umgang mit Phishing und SPAM
4. ISMS	Information Security Policy (Muster), (KIW 2020b) Leitfaden zur Einführung eines ISMS Leitfaden für Notfallmanagement Tailoring-Checklisten ISO27001, ISIS12 und BSI GS
5. Cyber-Sicherheit	Schutz vor gängigen Webschwachstellen (OWASP 2017) Top 12 Maßnahmen bei Cyber-Angriffen (ACS 2019a) Cloud-Richtlinie, Richtlinie Nutzung von Cloud-Diensten Leitfaden zur E-Mail-Sicherheit für Unternehmen Basismaßnahmen der Cyber-Sicherheit (BSI 2018)
6. Mobile Sicherheit	BYOD-Richtlinie, BYOD-Betriebsvereinbarung Home-Office-Betriebsvereinbarung (Muster) Checkliste Mobile Sicherheit für Smartphones und Tablets im Unternehmen

Diese zum Teil kommentierten elektronischen Dokumente ersetzen zwar im Zweifel keinen Rechtsanwalt oder Sicherheitsberater, bieten aber ein erstes Verständnis sowie eine Orientierung zur weiteren Nutzung. Die Dokumente sind daher elementarer Bestandteil einer „usable security", gerade für kleine Unternehmen. Die Information Security Toolbox soll den Aufbau und Betrieb eines ISMS sowie auch einer IT-Governance- und Compliance-Struktur im KMU praxisgerecht ergänzen.

8 Zusammenfassung und Ausblick

Wir haben ausgehend von unserer Forschungsfrage über eine Literaturanalyse und Expertenbefragung einen IT-GRC Ansatz bestehend aus sechs Kategorien ausdefiniert, der relevante und für KMU Handlungs-leitende Inhalte und Kompetenzfelder beschreibt. Aufgrund der limitierten Ressourcen und weiterer dargestellter Merkmale der KMU bedarf es eines Ansatzes, der dem Mittelständler relevante Inhalte und Kompetenzbedarfe auf einen Blick in den entsprechenden Kategorien aufzeigt und den Entscheidungsträgern aussagekräftige und prägnante Handlungsempfehlungen an die Hand gibt, ohne dabei zu technisch zu werden.

Der von uns verfolgte Ansatz ermöglicht die Entwicklung und konzeptuelle Integration von Methoden und Werkzeugen, die Kernkompetenzen von IT-Governance, IT-Risikomanagement, und IT-Compliance vereinen. Als Schwerpunkte unserer Literatur-gestützten Ansatzbildung haben sich neben der zu erwartenden Begriffs-Triade GRC die Kategorien Security Awareness, mobile Sicherheit und Cyber-Sicherheit heraus kristallisiert.

Uns ist bewusst, dass ein Ansatz bestehend aus diesen sechs Kategorien Unklarheiten und Widersprüche birgt. So sind im Vergleich zum IT-GRC-Dreieck von Knoll und Strahringer (2017, S. 8) die IT-Governance und IT-Compliance bei uns neben grundlegenden GRC-Dimensionen auch einzelne Kategorien, während die anderen vier Kategorien „Security Awareness", „ISMS", „Mobile Sicherheit" und „Cyber-Sicherheit" der Dimension IT-Risikomanagement zuordenbar sind. Auch sind die Kategorien nicht disjunkt, wir hatten unter anderem schon darauf hingewiesen, dass in der Kategorie „ISMS" je nach zugrunde gelegter Norm bereits Inhalte anderer Kategorien enthalten sind.

Das gleiche gilt für die Security Awareness, deren Maßnahmen eigentlich in jedem Informations-Sicherheitsmanagement (ISM) enthalten sein sollten. Wir interpretieren die steigende Anzahl und die in der Literatur behandelte hohe qualitative Bedeutung der Security Awareness als Beleg, dass diese Kategorie den Faktor Mensch in IT-GRC Ansätzen besonders widerspiegelt und für KMU sehr relevant ist. Die Empfehlungen, die das IT-GRC Reifegrad Werkzeug auf Basis der Eingaben aus der Reifegrad Erhebung teilautomatisiert im Gesamtbericht erzeugt, enthalten bei entsprechenden Handlungsbedarfen unter anderem eine Anzahl an Awareness-Maßnahmen, insbesondere die Teilnahme an Awareness-Webinaren, Red Team und Blue Team Rollenspielen, und Simulations-Workshops zu psychologischer Sicherheit und Awareness.

Weitere Arbeiten betreffen die integrative Ausarbeitung von Beziehungen der Dimensionen und Kategorien des Ansatzes untereinander, die wir mit unterschiedlichen Fragebögen für die diversen Stakeholder in KMU im IT-GRC Reifegrad Werkzeug begonnen haben. Hier sollte weitere theoretische Konzeption und empirische Evaluation zu den wechselseitigen Beziehungen innerhalb der IT-GRC Triade und den enthaltenen Kategorien erfolgen.

Eine künftige Aufgabe bleibt das notwendige weitere Tailoring von IT-Risikomanagement Ansätzen für KMU. Zum Begriff des Tailorings von IT-Projekt- und Risikomanagementansätzen siehe (Johannsen et al. 2017, S. 48). Aufgrund der Heterogenität von KMU ist es aus unserer Sicht jedoch schwierig bis unmöglich, einen der verbreiteten Standards für alle KMU zu adaptieren, wie es (Guldentops 2014) zum Beispiel für Cobit QuickStart vorschlägt. Anstatt dessen abstrahieren wir allgemein KMU-relevante Inhalte und Kompetenzen in unserer ISMS-Kategorie und geben ähnlich wie Beißel (2017) Hilfen und Leitlinien zur Wahl des nach weiteren Parametern wie Branche und Unternehmensgröße jeweils passenden Standards wie etwa ISIS12, BSI Grundschutz Basis oder Cobit 2019 Fokusbereich „KMU".

Abschließend werden wir unseren Ansatz und unsere Werkzeuge weiter nach kleinen versus mittleren Unternehmen differenzieren, da die Unterschiede in den IT-GRC Anforderungen etwa eines Handwerksbetriebs mit 12 Mitarbeitern im Vergleich zu einem IT-Dienstleister mit 250 Mitarbeitern enorm sind, und auch hier bisher kaum Literatur mit Erkenntnissen zu differenzierenden Ansätzen vorliegt.

9 Literaturverzeichnis

- ACS (2019a) Allianz für Cybersicherheit. Herausgeber: Bundesamt für Sicherheit in der Informationstechnik. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/Notfallkarte/TOP_12_Massnahmen.pdf?__blob=publicationFile&v=6. abgerufen am 10.02.2020

- ACS (2019b). Allianz für Cybersicherheit. Herausgeber: Bundesamt für Sicherheit in der Informationstechnik. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/Notfallkarte/IT-Notfallkarte_DINA4_eigenesLogo.pdf;jsessionid=5CFFA6B04DC1092950E331705C9F3EE9.2_cid351?__blob=publicationFile&v=4. abgerufen am 10.02.2020

- Ahn H, Maxa C, Panitz J C (2014) Steuerung von IT-Compliance Management Systemen in Konzernstrukturen. In: HMD (2014) 51:240–251

- Albayrak C A, Gadatsch A (2017) Digitalisierung für kleinere und mittlere Unternehmen (KMU): Anforderungen an das IT-Management. In: Knoll M, Strahringer S (Hrsg) IT-GRC-Management – Governance, Risk und Compliance. Grundlagen und Anwendungen. Springer Vieweg, Wiesbaden, S 151-166

- Albayrak C A, Gadatsch A (2018) Sind kleinere und mittlere Unternehmen (KMU) bereits auf die Digitale Transformation vorbereitet?. In: Multikonferenz Wirtschaftsinformatik 2018, Lüneburg, Band 4. S 1683-1693. 1693. http://mkwi2018.leuphana.de/programm/tagungsband/. abgerufen am 15.12.2019

- Andelfinger U, Kneuper R (2014) Governance und Compliance von Anfang an wirksam umsetzen. In: HMD (2014) 51:217–227.
- Anke J, Berning W, Schmidt J, Zinke C (2017) IT-gestützte Methodik zum Management von Datenschutzanforderungen. In: HMD (2017) 54:67–83

- Becker J, Krcmar H, Niehaves B (2009) Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Physika, Heidelberg

- Becker W, Ulrich P, Botzkowski T (2017) Industrie 4.0 im Mittelstand. Best Practices und Implikationen für KMU. Springer Gabler

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

- Bergmann R, Tiemeyer E (2017) IT-Governance. In: Tiemeyer E (Hrsg) Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. Hanser, München. S 759-813

- Bhattarcharyya A (2019) Governance, Risk & Compliance (GRC) Technology. 19th Annual Regional Audit Conference, Abu Dhabi. The Institute of Internal Auditors. Deloitte & Touche (M.E.)

- Bitkom (2017) Nur vier von zehn Unternehmen sind auf Cyberangriffe vorbereitet. https://www.bitkom.org/Presse/Presseinformation/Nur-vier-von-zehn-Unternehmen-sind-auf-Cyberangriffe-vorbereitet.html. abgerufen am 16.12.2019

- Bitkom (2018) Bitkom-Mittelstandsbericht 2018. Studie. https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Mittelstandsbericht-2018.html. abgerufen am 17.12.2019. abgerufen am 19.12.2019

- Bömelburg P, Zähres R (2015) Risiko- & Compliance-Management im Mittelstand – ein Plädoyer für ein integriertes System. In: Fahrenschon G, Kirchhoff A G, Simmert D B (Hrsg) Mittelstand – Motor und Zukunft der deutschen Wirtschaft. Erfolgskonzepte für Management, Finanzierung und Organisation. Springer, S 539-556

- Borchard I, Jurczok F, Javakhishvili E, Repoh I (2018) DIVSI U25-Studie. Euphorie war gestern. Die „Generation Internet" zwischen Glück und Abhängigkeit. Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), Hamburg, 2018, https://www.divsi.de/wp-content/uploads/2018/11/DIVSI-U25-Studie-euphorie.pdf abgerufen am 03.03.2020.

- BSI (2018) Basismaßnahmen der Cyber-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_006.pdf?__blob=publicationFile&v=4. abgerufen am 11.02.2020

- BSI Grundschutz (2020) Edition 2020 des IT-Grundschutz-Kompendiums. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html;jsessionid=B400C9556D86FA1A65AE526DE2E99E1B.1_cid341. abgerufen am 21.02.2020

- Buck et al (2016) Mobile Applikationen im Arbeitsalltag: Geringe Literacy als Sicherheitsgefahr für Unternehmen. HMD – Praxis der Wirtschaftsinformatik Heft 307, 53(1):87–97

- Dehmel S, Kelber U (2019) DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft.https://www.bitkom.org/sites/default/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf. abgerufen am 02.03.2020

- Deistler, N., Rentrop, C. (2020) IT-Compliance in KMU – State of the art, in: HMD (2020): https://doi.org/10.1365/s40702-020-00612-z

- Demary V, Engels B, Röhl K, Rusche C (2016) Digitalisierung und Mittelstand. Eine Metastudie. IW-Analyse - Nr. 109. Institut der deutschen Wirtschaft Köln Medien GmbH.

- Disterer und Kleiner (2014) Compliance von mobilen Endgeräten HMD (2014) 51:307–318 DOI 10.1365/s40702-014-0044-x
- Drechsler D (2019) Schutz vor Social Engineering. Angriffspunkte und Abwehrmöglichkeiten in digitalwirtschaftlichen Ökosystemen. Erich Schmidt Verlag GmbH & Co, Berlin

- Eierdanz F, Herzog-Buchholz E, Sieling E, Schick C (2019) Demografiefestigkeit 4.0 – Chancen des digitalen Wandels zur Förderung von Beschäftigungsfähigkeit und Arbeitgeberattraktivität nutzen. In: Arbeit 4.0 im Mittelstand. Chancen und Herausforderungen des digitalen Wandels für KMU, Springer, Berlin.

- Gardner B, Thomas V (2014) Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. Verlag: Syngress.

- Guldentops E (2014) Governance of IT in small and medium sized enterprises. In: Devos J, van Landeghem H, Deschoolmeester D (Hrsg) Information systems for small and medium-sized enterprises. Springer, Berlin/Heidelberg, S 3–24

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

- Henseler-Unger I, Hillebrand A (2018) Aktuelle Lage der IT-Sicherheit in KMU. In: DuD, Datenschutz und Datensicherheit Nr. 11, S 686-690. https://link.springer.com/content/pdf/10.1007%2Fs11623-018-1025-y.pdf abgerufen am 11.01.2020

- Hevner A. et al (2004) Design Science in Information Systems Research. In: MIS Q 28, S 75–105. University of Minnesota, Minneapolis.

- Hillebrand A, Niederprüm A, Schäfer S, Thiele S, Henseler-Unger I (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. abgerufen am 21.11.2019

- Hofmann J (2018) Arbeit 4.0 – Digitalisierung, IT und Arbeit IT als Treiber der digitalen Transformation. Springer Vieweg

- Hofmann M, Hofmann A (2017) ISMS-Tools zur Unterstützung eines nativen ISMS gemäß ISO 27001. Gesellschaft für Informatik. https://dl.gi.de/bitstream/handle/20.500.12116/3928/B21-2.pdf?sequence=1&isAllowed=y. abgerufen am 13.02.2020

- ifM Bonn (2016) KMU-Definition des IfM Bonn. https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/. abgerufen am 13.01.2020

- ISA (2020). ISA+ Fragenkatalog. Bayerischer IT-Sicherheitscluster e.V. http://www.gppag.de/downloads/201507_isapluskatalog.pdf.abgerufen am 09.03.2020

- ISIS12 (2018) Bayerischer IT-Sicherheitscluster. Handbuch zur effizienten Gestaltung von Informationssicherheit für Kleine und Mittlere Organisationen (KMO). Version 1.9.

- Jarke M, Otto B, Ram S (2019) Data Sovereignty and Data Space Ecosystems. In: Business & Information Systems Engineering. vol. 61(5):549–550. https://doi.org/10.1007/s12599-019-00614-2. abgerufen am 20.12.2019

- Johannsen A, Eifert F, Annan T (2020) Der IT-Mittelstand als Wegbereiter für Datengetriebene und kooperative Geschäftsmodelle. In: Wissenschaft trifft Praxis. Nr. 13, Jan. 2020, S 59-65

- Johannsen A, Kramer A, Kostal H, Sadowicz E (2017) Basiswissen für Software-Projektmanager im sequenziellen und agilen Umfeld. Aus- und Weiterbildung zum Certified Professional for Project Management (CPPM). dpunkt Verlag

- Kant D, Creutzburg R, Johannsen A (2020) Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan. IS&T International Symposium on Electronic Imaging 2020 Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2020. Society for Imaging Science and Technology. https://www.ingentaconnect.com/content/ist/ei zugegriffen am: 10.03.2020.

- Kersten H, Klett G (2015) Der IT Security Manager. Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden. Springer Vieweg. 4. Auflage.

- Kersten H, Klett G, Reuter J, Schröder K W (2020) IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Springer Vieweg. 2. Aktualisierte Auflage

- KIW-ADV (2019) ADV-Vertrag. Auftragsdatenverarbeitung im Einklang mit der DSGVO. Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft, Berlin, https://itwirtschaft.de/wp-content/uploads/2019/12/ADV-Vertrag.pdf. abgerufen am 10.02.2020.

- KIW-DS 2019 (2019) Datenschutzerklärung für eine Webseite. Muster. Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft, Berlin, https://itwirtschaft.de/wp-content/uploads/2019/12/Muster_DSGVO_2.pdf. abgerufen am 10.02.2020.

- KIW (2020a) Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft, www.it-wirtschaft.de zugegriffen am 10.01.2020.

- KIW (2020b) Information Security Policy, Informationssicherheitsrichtlinie für eine Kooperation. Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft, Berlin, https://itwirtschaft.de/wp-content/uploads/2019/09/Info-Sec-Policy-1_7.pdf zugegriffen am 10.02.2020.

- Klotz, M (2017) IT-Compliance. In: Ernst Tiemeyer (Hrsg) Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 6. Aufl. Hanser, München S 857-902

- Klotz M (2019) IT-Compliance nach COBIT 2019. SIMAT Arbeitspapiere. No. 11-19-034. Hochschule Stralsund. Stralsund Information Management Team (SIMAT). Stralsund.

- 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

- Knüpffer W et al (2017) Integration mobiler IT-Systeme. Einsatzfelder – Management – Strategie. Erich Schmidt Verlag, Berlin

- Kohne A, Ringleb S, Yücel C (2015) Bring your own Device. Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen,Risiken und Möglichkeiten. Springer Vieweg, Wiesbaden.

- Leeser D C (2020) Digitalisierung in KMU kompakt, Compliance und IT-Security, Springer Vieweg

- Lindner D (2019) KMU im digitalen Wandel Ergebnisse empirischer Studien zu Arbeit, Führung und Organisation. Springer.

- Lindner D, Leyh C. (2019) Digitalisierung von KMU – Fragestellungen, Handlungsempfehlungen sowie Implikationen für IT-Organisation und IT-Servicemanagement. In: HMD (2019) 56:402-418.

- Krcmar H, Eckert C, Roßnagel A, Sunyaev A, Wiesche M (2018) Management sicherer Cloud-Services. Springer Verlag, Wiesbaden

- Müller K (2018) IT-Sicherheit mit System. 6. Auflage. Springer Vieweg, Wiesbaden.

- OWASP (2017) Die 10 kritischsten Sicherheitsrisiken für Webanwendungen. (Deutsche Version 1.0). Open Web Application Security Project. https://www.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf. abgerufen am 20.12. 2019

- Pohlmann N (2019) Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Springer Vieweg

- Rehäußer P et al (2015) GSTOOL QUO VADIS? Evaluation von Information Security Management System Tools als Grundschutz Tool Alternativen. https://www.kronsoft.de/download/free/csc-studie.pdf. abgerufen am 14.12.2019

- Richter S, Straub T, Lucke C (2018) Information Security Awareness – eine konzeptionelle Neubetrachtung. In: Multikonferenz Wirtschaftsinformatik 2018. Lüneburg, Germany, S 1369–1380

- SAP (2019) SAP Governance, Risk, and Compliance (GRC) Solutions Road Map. https://blog.asug.com/hubfs/2019.pdf abgerufen am 20.02.2010

- Schonschek O (2019) Studie Cloud Security. IDG Research Services, München. www.computerwoche.de/studien. abgerufen am 04.02.2020

- Sirur S, Nurse J R C, Webb H (2018) Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In: 2nd International Workshop on Multimedia Privacy and Security (MPS'18), Toronto, ON, Canada, ACM, New York, NY, USA, S 88-95

- Todesco, Felix (2010): Die Unternehmensplanung bei kleinen und mittleren Unternehmen im Blickpunkt der aktuellen gesetzlichen Anforderungen an die Unternehmensführung, Dissertation, Universität Würzburg. https://opus.bibliothek.uni-wuerzburg.de/frontdoor/index/index/year/2010/docId/4210 abgerufen am 03.03.2020

- Urbach N,; Ahlemann F (2018) Der Wissensarbeitsplatz der Zukunft: Trends, Herausforderungen und Handlungsempfehlungen. In: Hofmann J (Hrsg) Arbeit 4.0 – Digitalisierung, IT und Arbeit IT als Treiber der digitalen Transformation, Springer Vieweg. S 79-94

- Verinice (2019) BSI IT-Grundschutz. SerNet GmbH, Göttingen. https://verinice.com/grundschutz. abgerufen am: 15.12.2019

- Wagner C(2017) Extreme Eigenkapitalausstattungen kleiner und mittlerer Unternehmen. Bestandsaufnahme und explorative Untersuchung. Springer Gabler Research

- Watson B, Zheng J (2017) On the User Awareness of Mobile Security Recommendations. In: ACM SE '17, Kennesaw, GA, USA.

- Weber K, Schütz A (2018) ISIS12-Hack: Mitarbeiter sensibilisieren statt Informieren. http://mkwi2018.leuphana.de/wp-content/uploads/MKWI_280.pdf. abgerufen am 09.03.2020

- Weber K, Schütz A E, Fertig T (2019) Grundlagen und Anwendung von Information Security Awareness. Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren. Springer Vieweg.

- Welter F, May-Strobl E, Schlömer-Laufen N, Kranzusch P, Ettl K (2014) Das Zukunftspanel Mittelstand Eine Expertenbefragung zu den Herausforderungen des Mittelstands. IfM-Materialien Nr. 229, Bonn. https://www.ifm-bonn.org/uploads/tx_ifmstudies/IfM-Materialien-229.pdf zugegriffen am 05.03.2020.

- Wohlfarth M (2019) Data Portability on the Internet. An Economic Analysis. In: Business & Information Systems Engineering 61(5):551–574