Johannsen, A.; Kant, D.

IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Johannsen, A.; Kant, D. (2020) : IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 57, Iss. 5, pp. 1058-1074,
https://doi.org/10.1365/s40702-020-00625-8

HMD (2020) 57:1058–1074
https://doi.org/10.1365/s40702-020-00625-8

SPEKTRUM

IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU

A. Johannsen · D. Kant

Eingegangen: 3. Januar 2020 / Angenommen: 13. Mai 2020 / Online publiziert: 25. Mai 2020

Zusammenfassung Kleine und mittlere Unternehmen aller Branchen versuchen sich nach wie vor angemessen mit den Herausforderungen der Globalisierung und der digitalen Transformation auseinanderzusetzen. Sie bilden in diesem Zusammenhang wachsende Kompetenz in der Produktionsautomatisierung (Industrie 4.0) und in digitalen Geschäfts- und Verwaltungsprozessen aus. In Bezug auf IT-GRC bleiben KMU demgegenüber faktisch oft noch unreif. Bestehende Ansätze des IT-Governance-, Risiko- und Compliance-Managements sind noch zu wenig für KMU ausgestaltet. Der Artikel 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 Ansatz enthält sechs relevante Kompetenzkategorien. Der Beitrag stellt dann zwei abgeleitete, 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 gemäß ihrem Reifegrad und bedarfsorientiert. 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.

Schlüsselwörter IT-Governance · IT-Risikomanagement · IT-Compliance · Security Awareness · IT-GRC Reifegrad · KMU

A. Johannsen · D. Kant (✉)
Fachbereich Wirtschaft, Technische Hochschule Brandenburg, Magdeburger Str. 50, 14770 Brandenburg an der Havel, Deutschland
E-Mail: daniel.kant@th-brandenburg.de

A. Johannsen
E-Mail: andreas.johannsen@th-brandenburg.de

IT-Governance, Risk-, and Compliance-Management (IT-GRC)—A Competence-Based Approach for SMEs

Abstract SMEs in all sectors are still trying to deal adequately with the challenges of globalisation and digital transformation. They are building up competence in production automation (Industry 4.0) as well as in the digitalisation of common business models and administrative processes, SMEs are, however, often still immature with regard to IT-governance, IT-security and IT-compliance. Existing approaches for IT-GRC are not suitable and tailored enough towards the needs and realities of SMEs. The article thus presents a literature-based approach for the perception, measurement and control of IT governance, risk and compliance management in SMEs, which includes six relevant categories of competence, and which was formed by also using feedback from 14 IT-GRC experts. The article then introduces two web-based tools for measuring IT-GRC maturity, but also for the management of measures in the relevant areas of competence for SMEs. The approach as well as the prototypically realized tools supports IT-GRC management in SMEs depending on the degree of their IT-GRC maturity. It entails fields of action and result types (recommendations, checklists, sample contracts). In the approach, emphasis is put on the involvement of diverse stakeholders and their points of view, needs-driven and lean methods as well as concrete tools and aids.

Keywords IT-Governance · IT Risk Management · IT-Compliance · Security Awareness · IT-GRC Maturity · SME

1 KMU und IT-Governance, Risiko- und Compliance-Management

1.1 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 den mit ihnen verbundenen Anforderungen in den Bereichen des Datenschutzes und der IT-Sicherheit ergeben. Um die Digitalisierung von KMU zu steuern und dabei alle relevanten Bereiche angemessen zu beachten, bedarf es eines ganzheitlichen Ansatzes, der auch die Informationssicherheit und den Datenschutz rechtskonform angeht. Bestehende Ansätze, insbesondere die des Governance-, Risiko- und Compliance-Managements (GRC), sind noch zu wenig für KMU ausgestaltet (Knoll und Strahringer 2017). 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 unser Beitrag 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?

1.2 Merkmale von KMU

Es wird 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 (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).

1.3 Herausforderungen für KMU

Allgemeine Herausforderungen für KMU sind die Wettbewerbs- und Innovationsfähigkeit, die Digitalisierung, wirtschaftspolitische und gesellschaftliche Rahmenbedingungen (Fachkräftemangel, Anstieg Altersstruktur) sowie Finanzierungshemmnisse (siehe z. B. Welter et al. 2014). Besonders bei kleinen Unternehmen wird von mangelnder kaufmännischer Ausbildung und strategischer Orientierung der Unternehmer berichtet. 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).

In Bezug auf den Reifegrad des IT-GRC Managements in KMU werden folgende Herausforderungen genannt (vgl. Bömelburg und Zähres 2015): erhöhte Risiken durch Familienkonflikte oder Entfernung der Eigentümer vom Management (Nachfolge), weniger ausgeprägte Rechnungswesen- und Controllingsysteme sowie Insolvenzrisiken und Finanzierungsprobleme. Bömelburg und Zähres (2015) plädieren als Lösung für ein integriertes GRC-System.

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 bei Nichtbeachtung der DSGVO in der Folge sogar Regressansprüche bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes anstehen (vgl. 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. 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).

Trotz einer in den letzten Jahren deutlich gestiegenen Risikowahrnehmung ist bei KMU die Bereitschaft, aktiv Maßnahmen zur IT-Sicherheit und IT-Compliance durchzuführen, weiterhin gering ist (Hillebrand et al. 2017). 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).

1.4 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. Ihr Ansatz gibt eine gute Orientierung, bedarf aber für KMU noch eines „Tailorings". 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.

Die Literaturanalyse zu IT-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, zum Beispiel das fünfstufige Reifegradmodell des NIST in Form des Federal Information Technology Security Assessment Framework. Das COBIT-5 (und aktuell COBIT 2019) Prozessreferenzmodell (Klotz 2019) ist bei KMU zum Teil bekannt, aber nicht verbreitet. 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 (BSI Grundschutz 2020), aber bei vielen KMU noch nicht etabliert (Hillebrand et al. 2017).

2 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. Eine Langfassung dieses Beitrags mit umfangreicher Literatur ist unter (Johannsen und Kant 2020) verfügbar.

2.1 Schritt 1 und 2: Literatursuche und Reduzierung

Die Literaturanalyse ist methodisch ähnlich wie bei Lindner und Leyh (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. Es wurde auf Deutsch und Englisch der folgende Suchstring gebildet:

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

Zeitlich wurde die Suche auf die Jahre 2012 bis 2020 reduziert. 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 im CSV-Dateiformat exportiert wurden. Alle Treffer wurden anhand der Relevanz zur Forschungsfrage betrachtet und dann die Anzahl der Treffer reduziert. Dazu wurden Titel und Keywords nach Stichworten wie „KMU“ und „SME“ ausgewertet. Nach dieser inhaltlichen Prüfung blieben 534 Treffer übrig.

2.2 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 Abschn. 3.2 erläutert.

2.3 Expertentest des Ansatzes und der Kategorien

Die Kategorien mit jeweils einer Kurzbeschreibung wurden 14 Experten ausgehändigt. Alle Experten haben durchschnittlich 15 Jahre IT-GRC-Erfahrung. Sie sind entweder als Forscher (50 %), als Informationssicherheits-Beauftragter (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 im Abschn. 3.1 erläutert.

2.4 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, siehe Abschn. 4.

2.5 Empirische Erprobung zweier IT-GRC Werkzeuge für KMU

Die erste prototypische Version des IT-GRC Reifegrad Werkzeugs für KMU wurde in einem Pretest mit Geschäftsführern von zehn IT-KMU getestet. Die Selbsteinschätzung mit den zehn Geschäftsführern wurde von Dezember 2019 bis März 2020 durchgeführt, die Ergebnisse des Pretests werden in die Verbesserung der IT-GRC Werkzeuge eingehen. Eine empirische Erhebung des IT-GRC Reifegrads von ca. 50 KMU ist für den Sommer 2020 geplant, siehe Abschn. 5.

3 Ein Ansatz für IT-GRC in KMU

3.1 Beschreibung des Ansatzes

KMU können gemäß der Literaturanalyse bei Berücksichtigung der wesentlichen relevanten Themen schon mit überschaubarem Aufwand eine signifikante Erhöhung des erforderlichen Schutz- und Konformitätsniveaus erreichen, wenn sie alle relevanten Kompetenzen beachten. Um die Wahrnehmung und das Management der relevanten Fähigkeiten eines KMU zu unterstützen, wird aus 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 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 (ISM)
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 mit der Bitte vorgelegt, jede Kategorie zu kommentieren und dann ein übergreifendes Feedback zur Eignung für KMU zu geben.

Das umfangreiche Feedback fiel in mehreren Punkten 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 empfohlen, hier für KMU lediglich das Etablieren eines KMU-freundlichen, schlanken „ISMS“ oder eines ISMS-Sicherheitsprozesses (z. B. nach Vorbild BSI-Standard 200-1) aufzunehmen.
d) Auch wenn die Reihenfolge keine Priorisierung bedeutete, wurde 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 einschlägiger Normen (insb. BSI Grundschutz und ISO 27001) 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.

3.2 Kategorien

3.2.1 IT-Compliance

IT-Compliance bezeichnet nach (Knoll und Strahringer 2017, S. 6) Kenntnis und Einhaltung aller die IT des Unternehmens betreffenden Vorgaben an das Unternehmen. Auch wenn die Compliance-Vorgaben für große Unternehmen insbesondere bei Finanzen (Prüfungsstandard IDW PS 980, AktG, KonTraG) und Prozessen (CMMI, SPICE) für KMU oftmals nicht gelten, stellen neben dem Datenschutz verschiedene für KMU relevante Compliance-Bereiche in der Umsetzung und Kontrolle für die IT-Compliance heute eine zentrale Herausforderung dar (Henschel und Heinze 2016, S. 157).

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 der europäischen KMU volle DSGVO-Compliance erreicht hat (Dehmel und Kälber 2019).

3.2.2 IT-Governance

IT-Governance umfasst nach Knoll und Strahringer (2017, S. 3) die konsequente Ausrichtung der Organisation, Steuerung und Kontrolle der IT eines Unternehmens an seiner Gesamtstrategie. 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, S. 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 1505 Befragten bestätigt.

Relevanz für KMU Es wird übereinstimmend mit Albyarak und 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 identifiziert (siehe Tab. 2). IT-Governance erfordert angemessene organisatorische und personelle Maßnahmen auch 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 der Analyse im Zeitalter des Cloud Computings zudem die Datensouveränität im Zuge der inter-organisationalen, kommerziellen Datennutzung (siehe Johannsen et al. 2020).

3.2.3 Security Awareness

Nach (Richter et al. 2018) ist Security Awareness – oder auch Information Security Awareness – der bezüglich der Sicherheitsgefahren bewusste Umgang mit Informationen, unabhängig vom Medium. In KMU sind konkrete Maßnahmen im Umgang mit Informationssicherheit bezüglich der Sensibilisierung und der Schulung („Lösungen vermitteln und üben“) erforderlich, Security Awareness ist daher ein wichtiges und wachsendes Feld der IT-Sicherheit.

Relevanz für KMU Security Awareness ist aufgrund geringeren „Know-Hows“ in KMU besonders relevant, und kann nur erfolgreich gelingen, wenn alle Stakeholder in ihren Bereichen entsprechend sensibilisiert sind, weshalb die unten abgeleiteten Werkzeuge alle Zielgruppen bis hin zu den IT-Nutzern beinhalten.

3.2.4 Informationssicherheits-Managementsystem (ISMS)

Ein ISMS ist ein System zum betrieblichen Management der Informationssicherheit, welches nach den verbreiteten Standards der ISO 27001 oder des BSI Grundschutz aufgebaut wird (vgl. Müller 2018, S. 91). Diese Kategorie beschreibt Richtlinien, Verfahren und Methoden, die eine Organisation implementieren sollte, um die Informationssicherheit zu steuern. Diese sind sowohl technischer Natur und beziehen sich auf IT-Systeme, von Firewalls bis hin zu Verschlüsselung oder Authentifizierung, als auch organisatorischer Natur wie z. B. das Herstellen physischer IT-Sicherheit beim Zugang zu (IT-) 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 einrichten (ISIS12 2018).

3.2.5 Cyber-Sicherheit

Die Cyber-Sicherheit umfasst nach Müller (2018, S. 128) sämtliche Bedrohungen aus dem globalen Internet, verbundene IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen. Die ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, enthält als einschlägiger Standard Anforderungen für die Sicherheit im Internet (vgl. Müller 2018).

Relevanz für KMU Cyber-Sicherheit umfasst den Bereich des Cloud Computings. Aufgrund der zunehmenden Auslagerung von IT-Diensten und Infrastrukturen von KMU in die Cloud hat diese Kategorie eine zunehmende Rezeption gerade in jüngeren Publikationen der Literaturanalyse erfahren, was ihr steigende Bedeutung für KMU verleiht (Kant et al. 2020).

3.2.6 Mobile Sicherheit

Mobile Endgeräte bergen nicht nur besondere Angriffsvektoren aus Sicht der IT-Sicherheit in sich, sondern sind auch aus IT-Governance Sicht sowie IT-Compliance Sicht ein wichtiger Problem- und Gestaltungsbereich (Knüpffer et al. 2017). Bring

Tab. 1 Inhalte und Kompetenzbereiche der sechs Kategorien des IT-GRC-Ansatzes

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
	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

Your Own Device (BYOD) bezeichnet in diesem Zusammenhang die – aus IT-GRC-Sicht problematische – Nutzung privater Endgeräte in Unternehmen, die in KMU verbreitet ist, da hier weniger umfangreiche Angebote von Seiten der IT-Abteilung bei größerem Freiheitsgrad der Mitarbeiter bestehen (Hillebrand et al. 2017, S. 54).

Relevanz für KMU Gerade junge Mitarbeiter im Umfeld von Startups und KMU gehen oft risikofreudiger mit Daten und Apps im Netz um. Durch die immerwährende Erreichbarkeit beim Arbeiten 4.0 verschwimmen Grenzen. Kleine Unternehmen sind meist geprägt von Tools und Methoden aus dem Consumer-Bereich (IT-Konsumerisierung), so dass auch hier noch großer Handlungsbedarf besteht.

In Tab. 1 sind die wichtigsten Inhalte und Kompetenzbereiche für KMU aufgeführt, die nach der Literaturanalyse und dem in Abschn. 3.1 gegebenen Expertenfeedback für den IT-GRC Ansatz Berücksichtigung gefunden haben.

4 IT-GRC Reifegrad Werkzeug: Beispielhafte Ergebnisse

Die Erfassung der subjektiven Wahrnehmung des IT-GRC-Reifegrads von KMU auf Basis unseres Ansatzes erfolgt mit dem IT-GRC-Reifegrad Werkzeug. Beide Auswertungen des Werkzeugs (Kurzauswertung zu den sechs Kategorien und teilautomatisierte Gesamtauswertung) sind so angelegt, dass eingegebene Fähigkeiten mit eingegebenen Wichtigkeiten je Aussage (jeweils Likert-skaliert) verglichen werden. Ein Wichtigkeits-Überhang wird als Handlungsbedarf, ein Fähigkeits-Überhang als Stärke interpretiert.

Abb. 1 zeigt eine Kurzauswertung im Rahmen des Pretests. 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.

In Abb. 2 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. Die roten Balken symbolisieren in allen sechs Kompetenzen Handlungsbedarf.

5 Nutzen des IT-GRC-Ansatzes für KMU

5.1 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

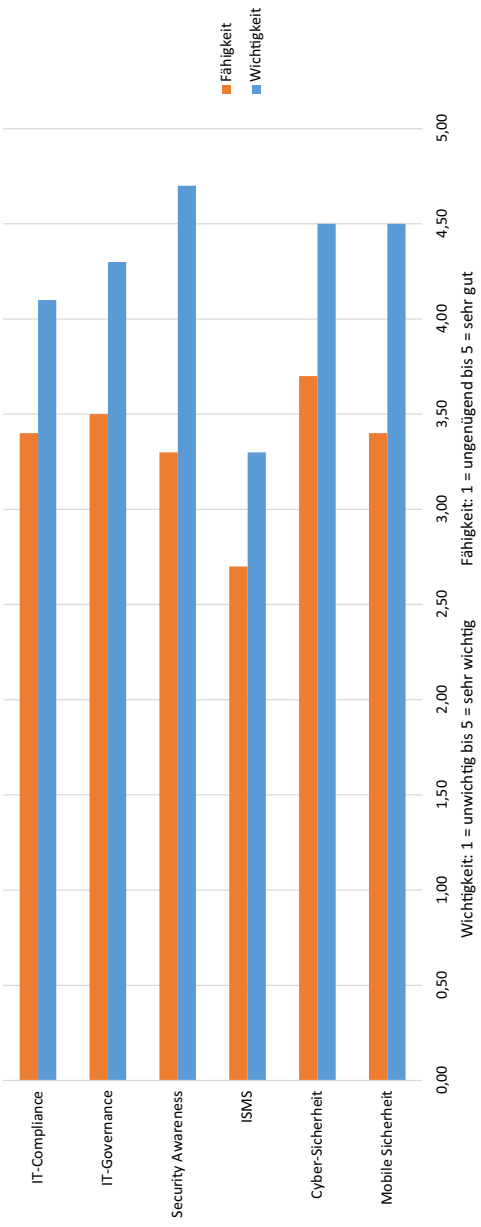

Abb. 1 IT-Governance-, Risiko- und Compliance Reifegrad von KMU ($n = 10$)

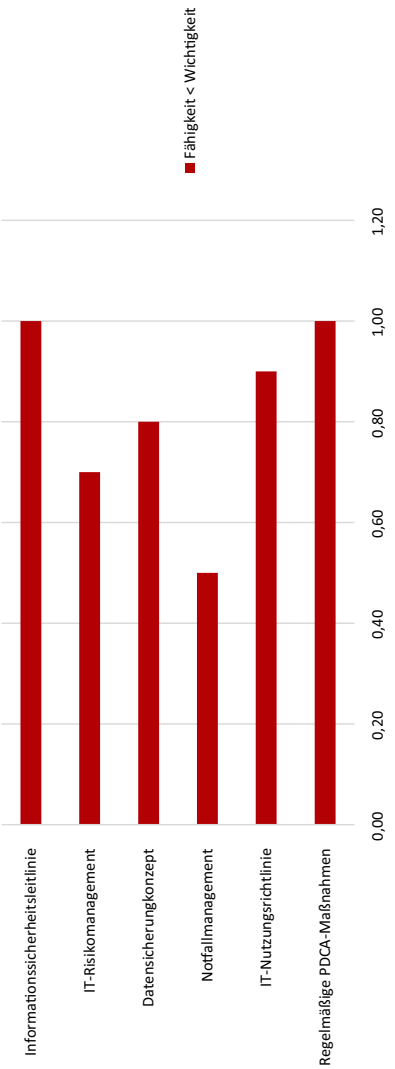

Abb. 2 Pretest-Bewertungsergebnisse der Kategorie „ISMS“ ($n = 10$)

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 einzelner Teilnehmer (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. Beispielsweise bewerten die Business Owner und IT-Nutzer die Compliance sowie auch die mobile Sicherheit gemäß des Feedbacks einiger der Geschäftsführer in 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 die IT-Leitung beide Kategorien höher bewerte, da sie von einem Richtlinien-konformen Handeln ausginge und keine Kenntnis der Schattensysteme und Apps in den Unternehmensbereichen hätte. In Projektworkshops (KIW 2020) und in den von KMU selbständig durchgeführten Workshops kann und sollte im Einzelfall geklärt werden, welche Sicht die jeweils zutreffende ist.

5.2 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 dem 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 IT-GRC 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 Tab. 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 2020).

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 einer IT-Governance- und Compliance-Struktur sowie eines ISMS im KMU praxisgerecht ergänzen.

Tab. 2 Umsetzungshilfen der IT-GRC Information Security Toolbox (siehe KIW 2020)

Kategorie	Muster, Checklisten, Verträge, Richtlinien etc. (Beispiele)
1. IT-Compliance	DSGVO-Datenschutzerklärung für Websites
	Muster für ADV-Vertrag nach DSGVO
2. IT-Governance	Empfehlungen zur organisatorischen Verankerung von IT-GRC-Rollen
	Leitfaden für IT-Programm- und Projektmanagement
3. Security Awareness	IT-Notfallkarte für koordiniertes IT-Notfallverhalten
	Verhaltungsregeln zum Thema Social Engineering
	Umgang mit Phishing und SPAM
4. ISMS	Information Security Policy (Muster)
	Leitfaden zur Einführung eines ISMS
	Leitfaden für Notfallmanagement
	Tailoring-Checklisten ISO 27001, ISIS12 und BSI GS
5. Cyber-Sicherheit	Schutz vor gängigen Webschwachstellen
	Liste priorisierter Maßnahmen bei Cyber-Angriffen
	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

6 Zusammenfassung und Ausblick

Es wurde ausgehend von der Forschungsfrage über eine Literaturanalyse und Expertenbefragung ein 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 den Entscheidungsträgern relevante Inhalte und Kompetenzbedarfe in den entsprechenden Kategorien auf einen Blick aufzeigt und aussagekräftige und prägnante Handlungsempfehlungen an die Hand gibt.

Der 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 der Literatur-gestützten Ansatzbildung haben sich neben der zu erwartenden Begriffs-Triade GRC die Kategorien Security Awareness, mobile Sicherheit und Cyber-Sicherheit herauskristallisiert.

Ein Ansatz bestehend aus diesen sechs Kategorien birgt Unklarheiten und Widersprüche. So sind im Vergleich zum IT-GRC-Dreieck von Knoll und Strahringer (2017, S. 8) die IT-Governance und IT-Compliance hier 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, es wurde unter anderem schon darauf hingewiesen, dass in der Kategorie „ISMS“ je nach zugrunde gelegter Norm bereits Inhalte anderer Kategorien enthal-

ten sind. Das gleiche gilt für die Security Awareness, deren Maßnahmen eigentlich in jedem Informations-Sicherheitsmanagement (ISM) enthalten sein sollten. Die steigende Anzahl und die in der Literatur behandelte hohe qualitative Bedeutung der Security Awareness kann als Beleg interpretiert werden, 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 (Webinaren, Rollenspiele etc.).

Noch erforderliche Arbeiten betreffen die integrative Ausarbeitung von Beziehungen der Dimensionen und Kategorien des Ansatzes untereinander, insbesondere mit unterschiedlichen Fragensets für diverse KMU-Stakeholder im IT-GRC Reifegrad Werkzeug.

Eine künftige Aufgabe bleibt das notwendige Tailoring von IT-Risikomanagement Ansätzen für KMU, also das Anpassen der Ansätze und Standards an Branchen- und Unternehmens-spezifische Gegebenheiten. Aufgrund der Heterogenität von KMU ist es nicht sinnvoll, einen der verbreiteten Standards für alle KMU zu adaptieren (siehe auch Beißel 2017). Anstatt dessen sollten allgemein KMU-relevante Kompetenzen abstrahiert werden, und Leitlinien zur Wahl des jeweils passenden Standards, wie etwa ISIS12, BSI Grundschutz Basis oder „Cobit 2019 Fokusbereich KMU“ gegeben werden. Abschließend sollte der Ansatz und die Werkzeuge weiter nach kleinen versus mittleren Unternehmen differenziert werden, da die Unterschiede in den IT-GRC Anforderungen etwa eines kleinen Handwerksbetriebs im Vergleich zu einem KMU mit 250 Mitarbeitern groß sind.

Förderung Diese Publikation wurde im Kontext des Projekts „Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft“ erstellt, welches im Rahmen von Mittelstand-Digital durch das Bundesministerium für Wirtschaft und Energie gefördert wird.

Funding Open Access funding provided by Projekt DEAL.

Literatur

Albayrak CA, 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
Beißel S (2017) Differenzierung von Rahmenwerken des IT-Risikomanagements. HMD 54:37–54
Bitkom (2018) Bitkom-Mittelstandsbericht 2018. Studie. https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Mittelstandsbericht-2018.html. Zugegriffen: 19. Dez. 2019
Bömelburg P, Zähres R (2015) Risiko- & Compliance-Management im Mittelstand – ein Plädoyer für ein integriertes System. In: Fahrenschon G, Kirchhoff AG, Simmert DB (Hrsg) Mittelstand – Motor und Zukunft der deutschen Wirtschaft. Erfolgskonzepte für Management, Finanzierung und Organisation. Springer, Berlin Heidelberg, S 539–556
BSI (2018) Basismaßnahmen der Cyber-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik. https://www.allianz-fuercybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSICS_006.pdf?__blob=publicationFile&v=4. Zugegrifen: 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. Zugegriffen: 21. Febr. 2020
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. Zugegriffen: 2. März 2020
Henschel T, Heinze I (2016) Governance, Risk und Compliance im Mittelstand, Praxisleitfaden für gute Unternehmensführung. Erich Schmidt Verlag, Berlin
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. Zugegriffen: 21. Nov. 2019
IfM Bonn (2016) KMU-Definition des IfM Bonn. https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/. Zugegriffen: 13. Jan. 2020
ISIS12 (2018) Bayerischer IT-Sicherheitscluster. Handbuch zur effizienten Gestaltung von Informationssicherheit für Kleine und Mittlere Organisationen (KMO). Version 1.9
Johannsen A, Eifert F, Annan T (2020) Der IT-Mittelstand als Wegbereiter für Datengetriebene und kooperative Geschäftsmodelle. Wiss Trifft Prax 13:59–65
Johannsen A, Kant D (2020) IT-Governance, Risiko- und Compliance-Management (IT-GRC) für KMU –Literaturanalyse und Ansatzbildung. http://ibid.th-brandenburg.de. Zugegriffen: 6. Apr. 2020
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. https://www.ingentaconnect.com/content/ist/ei. Zugegriffen: 10. März 2020 (IS&T International Symposium on Electronic Imaging 2020 Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2020. Society for Imaging Science and Technology)
KIW (2020) Mittelstand 4.0 Kompetenzzentrum IT-Wirtschaft. www.it-wirtschaft.de. Zugegriffen: 10. Jan. 2020
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
Leeser DC (2020) Digitalisierung in KMU kompakt, compliance und IT-security. Springer Vieweg, Wiesbaden
Lindner D, Leyh C (2019) Digitalisierung von KMU – Fragestellungen, Handlungsempfehlungen sowie Implikationen für IT-Organisation und IT-Servicemanagement. HMD 56:402–418
Müller K (2018) IT-Sicherheit mit System, 6. Aufl. Springer Vieweg, Wiesbaden
Richter S, Straub T, Lucke C (2018) Information Security Awareness – eine konzeptionelle Neubetrachtung. In: Multikonferenz Wirtschaftsinformatik 2018 Lüneburg, S 1369–1380
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: 5. März 2020