IT-Compliance in KMU – Experteninterviews zum Status quo

Nico Deistler und Christopher Rentrop

Wirtschaftsinformatik & Management 2022 • 14 (1): 10–19
https://doi.org/10.1365/s35764-021-00380-5
Angenommen: 22. November 2021
Online publiziert: 25. Januar 2022

Die digitale Transformation von Geschäftsprozessen und die stärkere Einbindung von IT-Systemen erzeugen bei kleinen und mittelständischen Unternehmen (KMU) Chancen und Risiken zugleich. Risiken, die insbesondere in einer fehlenden IT-Compliance resultieren können. Wie Studien zeigen, sind KMU in Bezug auf IT-Compliance-Maßnahmen im Vergleich zu kapitalmarktorientierten Unternehmen jedoch im Rückstand [1]. Im Beitrag wird mithilfe von Experteninterviews und einer qualitativen Datenanalyse der Frage nachgegangen, welcher Status quo an Maßnahmen aktuell implementiert und wie der empfundene Compliance-Reifegrad ist. Weiterhin werden die Gründe und Motive erörtert, die zu diesem Zustand geführt haben. Letztlich sind Treiber identifiziert worden, die zu einem höheren Bewusstsein in der Zukunft führen können. Die Arbeit zeigt interessante Erkenntnisse aus der Praxis, da die Experteninterviews Einblicke in den aktuellen Status quo in Bezug auf IT-Compliance liefern.

Status quo in KMU

Die dynamischen Themenbereiche rund um Digitalisierung und deren Auswirkungen werden in der Wissenschaft und Praxis kontrovers diskutiert und zeigen auf, dass es zu Veränderungen in den Geschäftsprozessen und der IT-Landschaft kommen wird [1]. Die Bereitschaft, aktiv Maßnahmen zur IT-Compliance und IT-Sicherheit anzugehen, ist trotz einer steigenden Risikowahrnehmung weiterhin gering [2]. Eine aktuelle Studie des Branchenverbandes Bitkom aus dem Jahr 2018 kam zu dem Ergebnis, dass 73 % der KMU bereits von Datendiebstahl oder Cyberspionage betroffen waren [3]. Dies zeigt, dass gerade mittelständische Unternehmen, die mit ihrer Innovationskraft und Wertschöpfung die Wirtschaft vorantreiben, eine effiziente IT-Compliance nicht vernachlässigen sollten. In der vorliegenden Arbeit sollen daher die folgenden Fragen beantwortet werden:

- Frage 1: Wie wird der Begriff IT-Compliance in KMU verstanden?
- Frage 2: Welche IT-Compliance-Maßnahmen werden aktuell in KMU durchgeführt?
- Frage 3: Welche Gründe und Motive haben den Zustand für IT-Compliance getrieben?
- Frage 4: Welche Faktoren treiben aktuell und zukünftig IT-Compliance-Maßnahmen?

Durchführung der Datenerhebung

Zur Beantwortung der oben definierten Fragen bietet sich das Experteninterview an. Mithilfe dessen wird ein breites Fachwissen, das die Experten aus ihrer beruflichen Praxis erworben haben, abgefragt und repräsentativ dargestellt. Die Fragen sind offen gestellt und haben einen explorativen Charakter. Die Erhebung erfolgt mit einem leitfadengesteuerten Interview und einer qualitativen Methodik zur Auswertung [4].

Die Interviewpartner wurden danach ausgewählt, dass sie entweder in Compliance relevanten Positionen in mittelständischen Unternehmen oder als Wissenschaftler oder Berater im Umfeld der Wirtschaftsinformatik tä-

Nico Deistler M. Sc. [1] (✉)
ist Prokurist in einer Unternehmensberatung, Doktorand an der HTWG in Konstanz und lehrt an der Hochschule Worms im Fachbereich Informatik.
nico.deistler@online.de

Prof. Dr. Christopher Rentrop [1] (✉)
Professor für Wirtschaftsinformatik, Direktor Konstanzer Institut für Prozesssteuerung (kips) und Gründer der BITCO3 GmbH.
rentrop@htwg-konstanz.de

[1] *Fakultät Informatik, HTWG Konstanz, Konstanz, Deutschland*

Zusammenfassung

- Keine zielgerichtete Verortung und Verantwortlichkeit von IT-Compliance in der Organisation, aufgrund von fehlendem Begriffsverständnis und Bewusstsein von Risiken
- Fehlender ganzheitlicher IT-Compliance-Ansatz, es werden lediglich einzelne technologische Maßnahmen umgesetzt
- Schwerpunkt liegt auf Kosten, anstelle einer langfristigen Kostenverringerung durch sichere und stabile Geschäftsprozesse

tig sind. Im Rahmen dieser Tätigkeit sollten sie sich mit IT-Compliance beschäftigen oder in der Vergangenheit bereits befasst haben. Das Ziel war zudem, unterschiedliche Branchen, von IT-Dienstleistern über Unternehmen, deren Geschäftstätigkeit nicht in direktem Zusammenhang mit IT steht, abzubilden, um eine möglichst breite Datenbasis zu erhalten. Aufgrund der mittelständischen Organisationsstrukturen handelte es sich bei den Befragten oftmals um Geschäftsführer, in deren Verantwortung die IT sowie Compliance liegen, und die über eine interne Sicht auf das Thema verfügen. Die externe Sicht wurde von den Wissenschaftlern und Beratern abgedeckt, die eine Vielzahl von mittelständischen Unternehmen betreut haben. Für die Teilnahme am Interview wurden zwölf Experten angefragt, von denen zehn zugesagt haben.

Alle Interviewpartner verfügen über mehrjährige Berufserfahrung (> 5 Jahre). Die Interviews wurden alle telefonisch durchgeführt und dauerten zwischen 45 und 60 min. Auf der Basis der definierten Fragen wurden zwölf Interviewfragen abgeleitet, auf die in der Darstellung der Ergebnisse eingegangen wird.

Die qualitative Methode zur Auswertung umfasst eine händische Transkription der Interviews und den Import der Daten in Microsoft Excel. Im Anschluss wurde eine qualitative Codierung [5] durchgeführt, mit der die Daten in mehreren Iterationen Codes zugeordnet werden. Als grober Bezugsrahmen dienten dabei die Interviewfragen, die zu Beginn schon feststehende Codes haben. Die weiteren Codes entwickelten sich durch eine offene iterative Codierung und wurden von einem Forscher so lange durchgeführt, bis die finalen Codes feststanden. Diese wurden im Anschluss von einem weiteren Forscher einem Review unterzogen und weiter angepasst.

Im Folgenden werden die Ergebnisse der beschriebenen Datenanalyse dargestellt. Beginnend mit dem Begriff der IT-Compliance, folgt danach der Ist-Zustand der Maßnahmen sowie der empfundene Compliance-Reifegrad in KMU. Der dritte Abschnitt stellt die Gründe und Motive dar, welche zum Status quo geführt haben, und zeigt primär die retrospektive Sicht. Danach folgt die Einschätzung welche Faktoren IT-Compliance-Maßnahmen in der Zukunft treiben.

Wie wird der Begriff IT-Compliance in KMU verstanden?

Der Begriff IT-Compliance wurde bei den Interviewpartnern sehr konträr aufgefasst. Bedingt durch die Einführung der EU-Datenschutzgrundverordnung (EU-DSGVO) im Jahre 2018 wurde dieses Schlagwort von nahezu allen Befragten mit IT-Compliance assoziiert. Dies kann zum einen auf die Aktualität zurückzuführen sein, zum anderen war die Umstellung sehr zeit- und kostenintensiv, die mit größeren Projekten und externem Know-how einhergegangen ist. „Die DSGVO mag den Konsumenten im Fokus haben und diesen schützen wollen, insbesondere vor großen Konzernen, zu deren Geschäftstätigkeit das Datensammeln gehört, aber die Auswirkungen der notwendigen Umstellungen in KMU, um eine Konformität zu erreichen, wurden für den Mittelstand nicht ausreichend bedacht“, so der Befragte I3.

Weitere genannte Begriffe sind gesetzliche Vorgaben, hier wurden insbesondere die Anforderungen nach AO, HGB und GoBD genannt sowie die Einhaltung gesetzlicher Vorgaben, die überwiegend durch Steuerberater und Wirtschaftsprüfer benannt und überprüft werden. Die Einhaltung von Normen und Standards sowie Unternehmensrichtlinien wurden nur von einzelnen Befragten erwähnt. Sechs Interviewpartner nannten Themen, die der IT-Sicherheit zuzuordnen sind. I10: „Für uns als Logistik-Unternehmen ist von Relevanz, dass unsere IT einwandfrei funktioniert und gegenüber externen Angriffen bestmöglich gesichert ist, um einen Ausfall, der mit Lieferverzögerungen einhergeht, zu vermeiden. Das ist meine Anforderung seitens der Geschäftsführung an eine IT, die compliant ist“ (**Tab. 1**).

Welche IT-Compliance-Maßnahmen werden aktuell in KMU durchgeführt?

In diesem Abschnitt soll eruiert werden, wie der Status quo in Bezug auf IT-Compliance aus Sicht der Befragten ist. Im ersten Schritt soll die Frage beantwortet werden, ob in Unternehmen eine gesonderte Betrachtung von Compliance und IT-Compliance stattfindet.

Die Ergebnisse der Befragten zeigen, dass in nur wenigen Fällen eine gesonderte Betrachtung von IT-Compliance stattfindet. Dies ist abhängig von der Unternehmensgröße und -branche. Die Unternehmen, die über eine IT-Compliance-Abteilung verfügen, sind beispielsweise Unternehmen, deren Geschäftstätigkeit primär in der IT stattfindet und die damit auch ein anderes Bewusstsein besitzen. „Wir als (Fach-)Abteilung Delivery haben das Thema IT-Compliance bei uns verankert, da ein Großteil der Prozesse auch hier stattfindet, und tragen es in die Organisation. Dies hat für uns den Vorteil, dass wir selbstständig agieren und zeitnah reagieren können, jedoch leidet darunter die Durchdringung in das gesamte Unternehmen“, I9, Leiter IT-Delivery eines IT-Dienstleisters. Insgesamt lässt sich jedoch feststellen, dass dies drei von zehn Befragten äußerten und damit überwiegend keine gesonderte Betrachtung durchgeführt wird.

Weiterhin wurde gefragt, ob es einen IT-Compliance-Verantwortlichen beziehungsweise eine -Abteilung gibt, und wenn ja, wo dies(er) in der Organisation angesiedelt ist. Fünf der Befragten gaben an, dass diese Aufgabe von der Geschäftsführung an den Leiter IT delegiert wurde. Vom Leiter IT wird diese Aufgabe neben den Tätigkeiten das Tagesgeschäftes durchge-

Kernthese 1

Die Treiber werden die Notwendigkeit von IT-Compliance-Maßnahmen weiter erhöhen

Tab. 1 Interviewfragen und Zusammenfassung der Ergebnisse

Interviewfragen	Zusammenfassende Antworten
Was verstehen Sie unter dem Begriff IT-Compliance?	Datenschutz (EU-DSGVO)
	Gesetzliche Vorgaben
	Normen und Standards
	Unternehmensethik/-richtlinien
	IT-Sicherheit

führt und gegebenenfalls an einzelne Mitarbeiter ausgelagert. Ein regelmäßiger Prozess ist nicht implementiert, vielmehr werden bei Bedarf, wie beispielsweise Einführung der EU-DSGVO, Projekte aufgesetzt. „Da wir keine gesonderte Betrachtung von IT-Compliance durchführen, unterliegt auch die Verantwortung der Compliance der Geschäftsführung. Sollten IT-relevante Themen im Rahmen unserer Risikoanalysen identifiziert werden, haben wir einen fähigen Mitarbeiter, der mit der IT vertraut ist und sich diesen annimmt", die Aussage des Geschäftsführers I1. Bei größeren KMU, die gleichzeitig IT-Dienstleister sind, gaben die externen Befragten (Berater und Professor) an, dass IT-Compliance-Verantwortliche vereinzelt vorhanden und dem Leiter IT unterstellt sind.

Die nächste Frage zielt darauf ab, ob es Kommunikation im Unternehmen über die Anforderungen der IT-Compliance gibt. Sechs der Befragten äußerten, dass eine regelmäßige Kommunikation von compliancenahen Themen stattfindet. Dies geschieht in Form von Newslettern, Sensibilisierung bezüglich Passwortkomplexitäten, durch Schulungsangebote für Neueinsteiger sowie einen regelmäßigen (halbjährlichen) Austausch zwischen Management und Mitarbeitern bezüglich sicherheitsrelevanter Vorfälle. Weiterhin wurde genannt, dass eine anlassbezogene Kommunikation stattfindet, wie beispielsweise Kommunikation in Bezug auf Viren oder andere akute Sicherheitsbedrohungen. Von dem externen Befragten I7 wurde geäußert, dass „IT-Sicherheitsvorfälle auf Mitarbeiterebene oftmals falsch klassifiziert und dadurch in der Hierarchie nach oben nicht kommuniziert werden". So beschreibt I8: „Die Mitarbeiter sehen die Kommunikation als lästig an, da ständig erweiterte Passwortkomplexitätskriterien und Betriebssystemvorfälle die Arbeit gefühlt behindern". Zudem wurde genannt, dass eine zielgerichtete Kommunikation seitens der Geschäftsführung in Bezug auf IT-Compliance-Themen nicht stattfindet.

Kernthese 2

Rahmenwerke schaffen einen Leitfaden und dienen als Orientierung

In der nächsten Fragestellung wurde explizit danach gefragt, ob die Anforderungen und Gesetze bekannt sind, die in Bezug auf IT-Compliance gelten und wo diese beschafft werden. Sieben Befragte gaben an, dass die Anforderungen und gesetzlichen Bestimmungen im Rahmen der Jahresabschlussprüfung durch Wirtschaftsprüfer, Steuerberater oder Unternehmensjuristen bekannt und dadurch übermittelt werden. Vier weitere Befragte sagten, dass sie die Informationen über die IHK, Interessenvertretungen oder Foren (passiv) beschaffen. Alle Befragten gaben an, dass die Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) und andere Anforderungen oder Rahmenwerke bekannt sind. Eine weitere Iteration der Antworten ergab, dass bei sieben Befragten die Anforderungen nach BSI-Grundschutz, bei drei Befragten COBIT (Control Objectives for Information and Related Technology) und bei zwei Befragten ISMS (Information Security Management System) und ITIL (Information Technology Infrastructure Library) bekannt sind. „BSI-Grundschutz ist zwar bekannt, wird aber nicht vollumfänglich umgesetzt, da die Umsetzung aller Anforderungen den Geschäftsbetrieb behindern würde", I5, Leiter IT eines Unternehmens mit 150 Mitarbeitern. Der Leiter IT und Compliance des Unterneh-

mens mit 400 Mitarbeitern: „Wir sind aktuell mit unserem externen Berater dabei, ein ISMS aufzubauen. BSI-Grundschutz erfüllen wir bereits, andere gängige Rahmenwerke wie COBIT oder ITIL-Prozesse haben wir abhängig vom Anwendungsbezug für einzelne Bereiche umgesetzt".

Dies führt zu der Frage, welche Ansätze oder Rahmenwerke tatsächlich eingesetzt werden. Die Antworten sind hierzu sehr heterogen. Vier der Befragten gaben an, die Anforderungen nach BSI-Grundschutz einzuhalten, weitere drei ein IT-Sicherheitskonzept zu haben, ausgewählte ITIL-Prozesse und ISO-Normen haben vorwiegend IT-Dienstleister genannt. Fünf Befragte sagten jedoch aus, keine Rahmenwerke zu nutzen. „Rahmenwerke sind zu generisch und nicht anpassungsfähig an unser Unternehmen. Zudem stehen sie nicht im Verhältnis zum tatsächlichen Nutzen", I1. Sinngemäß gaben diese Aussage alle Befragten, die keine Rahmenwerke einsetzen. Zudem wurde thematisiert, dass „die Kosten zur Delegation von Mitarbeitern, die dieses ‚(Compliance-)System' pflegen, zu hoch sind", I5. Acht der Befragten äußerten, dass Einzellösungen, wie Berechtigungskonzept, technisches 4-Augen-Prinzip, Firewall, Passwortkomplexitäten, E-Mail-Verschlüsselungen und Backup-Prozeduren eingesetzt werden.

Im letzten Abschnitt dieses Kapitel wurden die Befragten nach der Einschätzung des Compliance-Reifegrades ihrer Compliance-Maßnahmen gefragt. Aufgrund der im vorigen Absatz festgestellten Einzellösungen nannten auch hier sechs Befragte, dass dedizierte technische Maßnahmen ohne ganzheitliche Betrachtung genutzt werden. „Richtlinien werden erstellt, aber nicht in der Form kommuniziert und die Vorteile daraus dargestellt, dass diese auch angewendet werden", I3. Dazu ergänzt I4: „Der Reifegrad der implementierten Prozesse ist im Verhältnis zum Risiko bisher ausreichend, wir haben jedoch Aufholbedarf im Bereich Cybersicherheit und Cloud-Anwendungen". Weitere drei Befragte nannten den Reifegrad in der Entwicklungsphase als ausbaufähig. Die externen Berater äußern: „Nur wenige auf IT fokussierte und stark von IT abhängige Geschäftsmodelle haben Compliance-Maßnahmen im notwenigen Reifegrad umgesetzt", so I7, und sollte das der Fall sein, nennt I8: „Da eine regelmäßige jährliche Attestierung durch einen Wirtschaftsprüfer erfolgt, haben diese Prozesse zwei, drei Jahre nach Einführung einen hohen Reifegrad erreicht. Oftmals sind es dann aber

nur diese Prozesse, die beispielsweise für Kunden von Relevanz sind, andere interne Maßnahmen, die nicht Bestandteil der Attestierung sind, sind nicht wirksam“ (**Tab. 2**).

Welche Gründe und Motive haben den Zustand für IT-Compliance getrieben?

Der dritte Abschnitt geht auf die Gründe und Motive ein, welche zum Status quo geführt haben, und zeigt primär die retrospektive Sicht. Alle Befragten nannten zu hohe Kosten als einen wesentlichen Grund für den Status quo. So äußert I2: „Hohe Kosten sowohl durch externes Know-how als auch durch die Einstellung von Mitarbeitern mit diesen Kompetenzen“. Dazu ergänzt I2: „Cloud-Applikationen werden verstärkt genutzt, wodurch es zu einer Veränderung von Prozessen kommt. Der Aufbau von Kompetenz ist kostenintensiv.“ Weiter meint I10: „Wir haben limitierte Ressourcen. Mitarbeiter können nicht für IT-Compliance über einen längeren Zeitraum freigestellt werden“. Und I4 fasst zusammen: „Der Schwerpunkt liegt bei den meisten Unternehmen auf den Kosten, anstelle einer langfristigen Kostenverringerung, beispielsweise durch sichere und stabile Geschäftsprozesse“. Vier weitere Befragte nannten fehlende Kompetenzen, da es sich um gut ausgebildete IT-Fachkräfte handelt, die am Arbeitsmarkt schwer für KMU zu bekommen sind. Zudem wurde genannt, dass teilweise Prozesse vorhanden sind, jedoch ein Bewusstsein für Compliance-Maßnahmen im Generellen fehlt. Auch wird der „Tone from the top“ nicht kommuniziert und die IT nicht als Bestanteil des Kerngeschäftes gesehen. Bestimmte Risiken, die bewusst in Kauf genommen werden, wurden nicht geäußert. Es wurden jedoch mehrfach fehlende IT-Sicherheitsmaßnahmen als ausbaufähig gekennzeichnet. Die Angst vor Cyberspionage und Datendiebstahl ist bei den Befragten verbreitet. Auch wenn sie nicht direkt betroffen sind, gaben die Befragten an, ein Unternehmen zu kennen, welches schon einmal betroffen war. Dies führe dann zu einzelnen technologischen Maßnahmen. Zudem

Kernthese 3

Klare Verantwortlichkeiten mit Berichterstattung an das Management definieren

Tab. 2 Interviewfragen und Zusammenfassung der Ergebnisse

Interviewfragen	Zusammenfassende Antworten
Erfolgt im Unternehmen eine gesonderte Betrachtung von IT-Compliance und Compliance?	Gesonderte Betrachtung von IT-Compliance, abhängig von Unternehmensgröße und -branche
Gibt es einen (IT-)Compliance-Verantwortlichen/eine -Abteilung bzw. wo sind diese in der Organisation angesiedelt?	Geschäftsführung und Leiter IT übernehmen überwiegend IT-Compliance-Aufgaben
Ist bekannt, welche Anforderungen/Gesetze in Bezug auf IT-Compliance gelten? Wo werden die Informationen beschafft?	Anforderungen/Gesetzliche Bestimmungen werden aus der Jahresabschlussprüfung beschafft Informationsbeschaffung via IHK/Interessenvertretungen/Foren
Werden Ansätze oder Rahmenwerke zur Einhaltung von IT-Compliance eingesetzt?	Operative Fehler im Umgang (zum Beispiel falsche Klassifizierung von Vorfällen) Dedizierte technische Maßnahmen ohne ganzheitliche Betrachtung; einseitiger Fokus
Gibt es Kommunikation im Unternehmen (an das Management und die Benutzer) über die Anforderungen der Compliance?	Anlassbezogene Kommunikation findet statt BSI u. a. Anforderungen/Rahmenwerke sind bekannt, jedoch keine vollumfängliche Anwendung
Wie bewerten Sie den Reifegrad der Maßnahmen?	Rahmenwerke nur marginal anwendbar, daher geringe Anwendung

passen die Rahmenwerke nicht zu den Strukturen in KMU, gaben nahezu alle übereinstimmend an.

Zu der Frage, ob es wesentliche Treiber in den letzten Jahren gab, die den Reifegrad erhöht haben, nannten neun der Befragten, dass die Einführung der EU-DSGVO zu einem höheren Bewusstsein geführt hat und IT-Compliance seitdem bei der Geschäftsführung einen höheren Stellenwert einnimmt. Auch wurden Cyberangriffe, Datenverlust und Cloud-Anwendungen von fünf Befragten genannt (**Tab. 3**).

Welche Faktoren treiben aktuell und zukünftig IT-Compliance-Maßnahmen?

Die Interviewfragen bezogen sich zum einen auf die Treiber, denen eine spürbare Aufmerksamkeit zukommen wird, und zum anderen darauf, ob sich die Relevanz von IT-Compliance in den nächsten Jahren verändern wird. Als aktuellen Treiber nannten alle Befragten die Auslagerung von IT-Systemen in Cloud-Anwendungen und damit einhergehend die Datensouveränität. Dazu I7: „Unternehmen werden nur noch die wichtigsten geschäftsrelevanten Daten selbst vorhalten, andere Anwendungen in Cloud Applikationen wandern. Cloud-Provider wiederum werden sich in stärkerem Wettbewerb befinden, Compliance-Prozesse zertifizieren lassen und damit IT-Compliance ein Wettbewerbsvorteil sein“. Damit könnten Unternehmen einen Teil der Maßnahmen auslagern, was aber nicht dazu führen wird, dass das Unternehmen keine weiteren Maßnahmen implementieren muss. Acht Befragte nannten Themen zu Cybersicherheit als weiteren Treiber. „Kommt es vermehrt zu Vorfällen und davon ist bei dem aktuellen Trend auszugehen, wird die Relevanz zwangsweise bei jedem Vorfall erhöht werden. Das Bekanntwerden von Cyberangriffen führte bei uns zur Einfüh-

Tab. 3 Interviewfragen und Zusammenfassung der Ergebnisse

Interviewfragen	Zusammenfassende Antworten
Werden bestimmte (Compliance-)Risiken bewusst in Kauf genommen? Wenn ja, welche Gründe und Motive liegen hierfür vor?	Hohe Kosten der Umsetzung
Was sind wesentliche Gründe für den Status quo in Bezug auf IT-Compliance?	Limitierte Mitarbeiterressourcen, fehlende Kompetenz Rahmenwerke zu generisch Mangelndes Bewusstsein für IT-Compliance-Risiken
Gab es wesentliche Treiber in den letzten Jahren, die den Reifegrad erhöht haben?	Einführung der EU-DSGVO Cyberangriffe/Datenverlust Cloud Anwendungen

Tab. 4 Interviewfragen und Zusammenfassung der Ergebnisse

Interviewfragen	Zusammenfassende Antworten
Gibt es Faktoren, die IT-Compliance-Maßnahmen in Ihrem Unternehmen eine spürbare Aufmerksamkeit zukommen lassen? Wie glauben Sie, wird sich die Relevanz von IT-Compliance in den nächsten Jahren verändern?	Cloud-Anwendungen und Datensouveränität Cybersicherheit Digitalisierung EU-DSGVO Mobile Sicherheit Kundenanforderungen (Zertifizierungen/Attestierungen)

Handlungsempfehlung

- Analyse der Adaptierung von bereits vorhandenen Rahmenwerken auf die Strukturen von KMU
- Veränderungen der Geschäftsprozesse, die aus der Digitalisierung, EU-DSGVO, Cloud-Anwendungen und Cybersicherheit resultieren, sollten in der Analyse ausreichend berücksichtigt werden
- Bewusstsein von Risiken schärfen

rung von zusätzlichen Firewalls und IDS-Systemen." Weitere sechs Befragte gaben übereinstimmend an, dass die Digitalisierung der Geschäftsprozesse dazu führen wird, dass die IT und damit auch die IT-Compliance einen immer wichtigeren Stellenwert einnehmen wird. Weitere genannte Punkte sind die EU-DSGVO bei fünf Befragten. Zudem hat insbesondere ein IT-Dienstleister erwähnt: „Größere Kunden erwarten von uns die Einhaltung bestimmter branchenüblicher Standards sowie die regelmäßige Attestierung dieser Prozesse. Für uns war die Implementierung mit einem hohen initialen Aufwand verbunden, der jedoch das Bewusstsein bei den Mitarbeitern gestärkt und unsere Prozesse standardisiert und automatisiert hat", so der Leiter IT und Compliance, I6 (**Tab. 4**).Fazit und Ausblick

Die Ergebnisse der Befragungen zeigen, dass IT-Compliance in KMU ein sehr dynamisches Umfeld ist und die Digitalisierung, EU-DSGVO, Cloud-Anwendungen und Cybersicherheit bereits eine große Rolle als Treiber spielen. Da bei den Verantwortlichen kein klares Begriffsverständnis von IT-Compliance vorhanden ist sowie das Bewusstsein noch nicht in der notwendigen Form ausgeprägt ist, führt dies dazu, dass die Verantwortlichkeit von IT-Compliance nicht zielgerichtet in der Organisation verortet ist. Dies kann zur Folge haben, dass der so wichtige „Tone from the top" nicht gelebt und im Umkehrschluss Risiken im operativen Umgang mit der IT nicht erkannt oder falsch eingeschätzt werden. Die Ergebnisse zeigen, dass die Gründe für diesen Status quo zu hohe Kosten für IT, limitierte Mitarbeiterressourcen, fehlende Kompetenz und Rahmenwerke sind, die nicht zu den Strukturen in KMU passen. Dies führt dazu, dass die Unternehmen keinen ganzheitlichen Ansatz, sondern lediglich einzelne technologische Maßnahmen umsetzen. Zusammengefasst liegt der Schwerpunkt bei den meisten Unternehmen auf den Kosten, anstelle einer langfristigen Kostenverringerung, beispielsweise durch sichere und stabile Geschäftsprozesse.

Weitere Diskussion zu diesem Thema wären wünschenswert, da die genannten Faktoren die Notwendigkeit von IT-Compliance weiter vorantreiben werden. Daher ist es wichtig, sich zum einen mit der Adaptierung von bereits vorhandenen Rahmenwerken auf die Strukturen von KMU auseinanderzusetzen. Zum anderen sollten die sich verändernden Geschäftsprozesse, die aus der Digitalisierung und Cloud-Anwendungen resultieren, darin berücksichtigt werden.

Funding. Open Access funding enabled and organized by Projekt DEAL..

Literatur

[1] Deistler, N., & Rentrop, C. (2020). IT-Compliance in KMU—State of the art. *HMD*, *57*, 1047–1057.

[2] 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: 28. Nov. 2020.

[3] Bitkom (2018). Bitkom-Mittelstandsbericht 2018. Studie. https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Mittelstandsbericht-2018.html. Zugegriffen: 20. Nov. 2020.

[4] Meuser, M., & Nagel, U. (2009). Das Experteninterview – konzeptionelle Grundlagen und methodische Anlage. In S. Pickel, G. Pickel, H.-J. Lauth & D. Jahn (Hrsg.), *Methoden der vergleichenden Politik- und Sozialwissenschaft. Neue Entwicklungen und Anwendungen* (S. 465–479). Wiesbaden: VS.

[5] Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: techniques and procedures for developing grounded theory*. Thousand Oaks: SAGE.