



The Future of Controls
IKS-Transformation im
Versicherungsumfeld

Über diese Studie

Die Deloitte-Studie zum Thema „Future of Controls“ analysiert die aktuellen Herausforderungen von deutschen Versicherungsunternehmen im Hinblick auf das IKS (Interne Kontrollsystem). Darüber hinaus werden die Elemente und Eigenschaften eines modernen IKS in Bezug auf (1) Organisation und Betriebsmodell sowie (2) Technologieeinsatz diskutiert.

Insbesondere werden (3) der Mehrwert eines modernen IKS und (4) dessen Beitrag zur Unternehmenssteuerung dargestellt. Aufbauend auf den Studienergebnissen geben wir einen Ausblick auf strategieorientierte Transformations- und Steuerungsmöglichkeiten eines IKS im Versicherungsumfeld.

Methodik

Die vorliegende Studie basiert auf systematisierten Experteninterviews. Befragt wurden leitende IKS-Verantwortliche von deutschen Versicherungsunternehmen sowie internationale IKS-Experten von Deloitte. Aufgrund ihres Wissens und ihrer Erfahrung in Bezug auf die IKS-Optimierung gelten die befragten Personen als ausgewiesene Experten auf

diesem Gebiet. Die Befragung wurde per Videokonferenz durchgeführt und im Rahmen einer qualitativen Inhaltsanalyse nach Mayring ausgewertet.

Executive Summary	4
1. Aktuelle Herausforderungen von Versicherungsunternehmen im Hinblick auf das IKS	6
2. Studienergebnisse	14
3. Strategieorientierte Transformations-und Steuerungsmöglichkeiten eines IKS	26
Fazit und Ausblick	29
Literatur und Quellen	30

Executive Summary

Viele Versicherungsunternehmen überschätzen die Wirksamkeit und Effizienz ihres bestehenden IKS. Dies liegt zum einen daran, dass die Herausforderungen im Kontext des IKS oftmals nicht vollständig erkannt und demzufolge keine adäquaten Gegenmaßnahmen getroffen werden. Auf der anderen Seite wird der zusätzliche Nutzen, den das IKS als ganzheitliches Steuerungsinstrument bieten kann, von Unternehmen noch zu wenig erkannt: Denn in seiner steuernden Funktion kann das IKS erheblich zur Erfüllung von strategischen Unternehmenszielen beitragen und somit einen erheblichen Mehrwert darstellen. Das vorliegende White Paper untersucht daher die folgenden Kernfragen: Welchen Herausforderungen stehen Versicherungsunternehmen gegenüber? Wie sieht ein IKS der Zukunft aus? Welche Anforderungen müssen diesbezüglich erfüllt werden? Welche Ansätze gibt es, um zu einem modernen IKS zu kommen und dieses als Steuerungswerkzeug einzusetzen?

Der erste Teil des White Papers identifiziert die aktuellen Herausforderungen, die sich für Versicherungsunternehmen im Zusammenhang mit dem IKS ergeben. Insbesondere können (i) regulatorische Anforderungen, (ii) digitale Transformationsprozesse, (iii) Dynamiken im Innovations- und Wettbewerbsumfeld, (iv) inkonsistente Risiko- und Kontrollsysteme sowie (v) eine mangelnde Ausrichtung an Unternehmenszielen zur Unwirksamkeit und Ineffizienz des IKS führen. Aufgrund der damit einhergehenden Kontrollschwächen (z.B. falsches Verständnis und Sicherheitsgefühl in Bezug auf die Einhaltung von Geschäftsrisiken, hoher Ressourcenverbrauch durch manuelle Kontrollausführungen oder der mangelnde Einsatz technologischer Möglichkeiten) sollten bestehende Kontrollsysteme kritisch hinterfragt werden. Denn oftmals beruhen Risiken und Kontrollen lediglich auf Erfahrungswerten oder allgemein gefassten

Risiko- und Kontrollkatalogen und sind darüber hinaus nur pauschal beschrieben. Für die Modernisierung und Transformation des IKS bedarf es daher eines ganzheitlichen Ansatzes, welcher in der Versicherungspraxis in ausgereifter Form noch nicht vollumfänglich etabliert ist.

Im zweiten Teil des White Papers werden verschiedene Ansatzmöglichkeiten für die Ausgestaltung eines modernen IKS erörtert. Grundlage hierfür ist eine qualitative Befragung unter IKS-Verantwortlichen von deutschen Versicherungsunternehmen sowie internationalen IKS-Experten von Deloitte. Im Speziellen werden die Elemente und Eigenschaften eines modernen IKS in Bezug auf (1) Organisation und Betriebsmodell sowie (2) Technologieeinsatz diskutiert. Insbesondere werden (3) der Mehrwert eines modernen IKS und (4) dessen Beitrag zur Unternehmenssteuerung dargestellt. Zusammenfassend sollte ein modernes IKS einen (1) hohen Grad an Standardisierung aufweisen (z.B. Prozess-, Risiko- und Kontrolltaxonomie; Risiko- und Kontrollbewertungsverfahren). Ferner ermöglicht die (2) Automatisierung eine Effizienzsteigerung des IKS und gleichzeitig eine Kostensenkung, indem kostenintensive, zeitaufwendige manuelle Tätigkeiten rationalisiert werden. Darüber hinaus sind die (3) Vernetzung der eingesetzten Technologien über programmierte Schnittstellen oder RPA sowie eine Vernetzung der Rollen im IKS durch eine verbesserte Kommunikation und klare Aufgabendefinition zu empfehlen. Durch die (4) Fokussierung auf strategische Prozessziele und die Ausrichtung der Kontrollen auf die Zielerreichung generiert das IKS zudem einen echten Mehrwert für die Unternehmensführung. Die Standardisierung, Automatisierung, Vernetzung und strategische Ausrichtung eines IKS schaffen wiederum eine (5) hohe Transparenz (z.B. über potenzielle Risiken im Unternehmensumfeld)

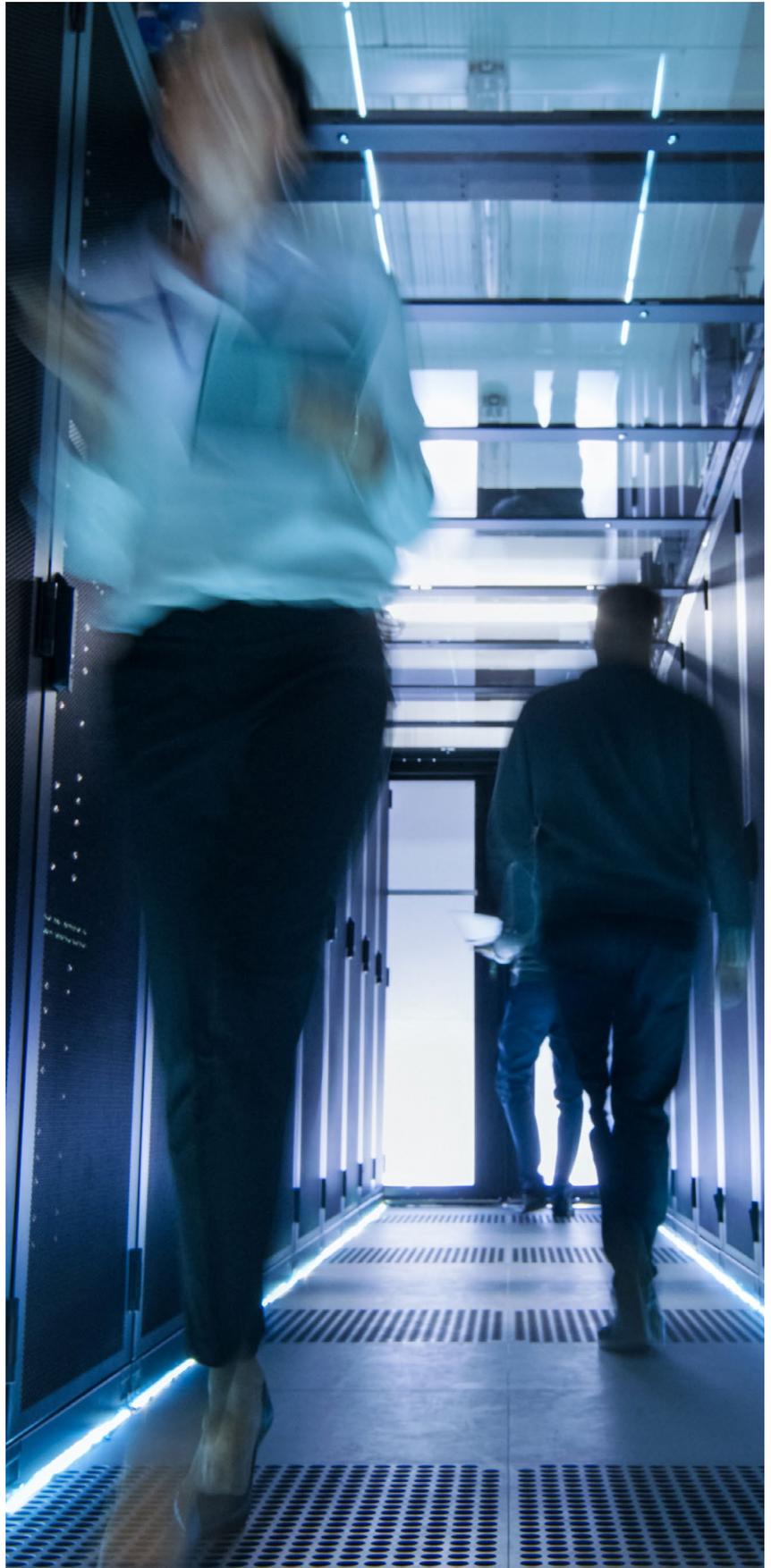
und ermöglichen zugleich eine (6) Rationalisierung von redundanten Prozessen und Kontrollen. Zusätzlich bietet eine erhöhte Transparenz eine Grundlage zur Schaffung einer verbesserten Risikokultur und Wahrnehmung im Unternehmen im Sinne von „Steuerung“ statt „Verhinderung“.

Der Weg hin zu einem modernen IKS kann insbesondere durch die Aktivierung von drei Transformationshebeln gelingen. Die (1) Umgestaltung des Betriebsmodells sollte durch die Optimierung von Strukturen und Systemen erfolgen (z.B. Implementierung eines Chief Control Officer (CCO), Aufbau eines Kompetenzzentrums für Kontrollen (CCoE)). Durch (2) Technologie-Enablement kann die Automatisierung von Prozessabläufen vorangetrieben werden. Dies gilt für Prozesse im eigentlichen Sinne, aber auch für die Aufgaben im Rahmen des IKS-Regelkreislaufs (z.B. Kontrollausführung, -test, -überwachung, IKS-Berichterstattung), vor allem im Hinblick auf eine kontinuierliche Risikoüberwachung und -steuerung. (3) Harmonisierung und Rationalisierung von Risiken und Kontrollen können etwa durch die Anwendung des „Test once, use multiple times“-Ansatzes erfolgen, d.h., dass zentral bereitgestellte Controllergebnisinformationen für die unterschiedlichen Verwendungszwecke innerhalb der Three Lines of Defense zur Verfügung stehen. Je mehr Transformationshebel aktiviert werden, desto kosteneffizienter, erkenntnisorientierter und geschäftsförderlicher kann das IKS eingesetzt werden.

Im dritten Teil des White Papers werden die strategierorientierten Transformations- und Steuerungsmöglichkeiten diskutiert. Generell wird die Möglichkeit der steuerbaren Einwirkung von Kontrollen auf die Erfüllung von strategischen Unternehmenszielen in der Versicherungspraxis bisher kaum wahrgenommen. Der zusätzliche Nutzen,

den das IKS als ganzheitliches Steuerungswerkzeug bieten kann, liegt vor allem in der Unterstützung von Entscheidungsprozessen durch eine detaillierte und aktuellere Informationslage zu Risiken sowie Prozess- und Kontrollschwächen im Unternehmen. Durch die direkte Kommunikation von steuerungsrelevanten IKS-Informationen an die Geschäftsleitung profitiert die IKS-Funktion von einer hohen Aufmerksamkeit und erfährt somit eine größere Wertschätzung.

Ein transparentes Bild von Risiken und Prozessschwächen unterstützt nicht nur die Entscheidungsfindung für Investitionen oder Rationalisierungen im Unternehmen, sondern kann darüber hinaus hilfreiche Informationen zur strategischen Ausrichtung im Sinne neuer Produkteinführungen oder der Erschließung neuer Märkte liefern. Daraus resultiert aber auch das Erfordernis zur Skalierbarkeit von Kontrollen, um kontinuierliche Änderungen bzw. Anpassungen von strategischen Zielvorgaben abbilden zu können. Zur flexiblen Steuerung von Risiken und Prozessen – unter Berücksichtigung von Zeit-, Kosten- und Qualitätsfaktoren – bedarf es eines ganzheitlichen, robusten und nachhaltigen Vorgehensmodells, welches im dritten Teil des White Papers schrittweise anhand eines Beispiels aus der Versicherungsbranche beschrieben wird.



1. Aktuelle Herausforderungen von Versicherungsunternehmen im Hinblick auf das IKS

Die voranschreitende Digitalisierung in der Versicherungsbranche führt unter anderem dazu, dass sich Geschäftsmodelle, Systemlandschaften und regulatorische Rahmenbedingungen ändern. Der damit einhergehende stetige Wandel des Risikoumfelds stellt viele Versicherer vor eine große Herausforderung. Zudem müssen strategische Unternehmensziele unter Berücksichtigung von Risiken und Kostendruck umgesetzt werden. Ein zentrales und wertstiftendes Element ist die Integration von IKS und Risikomanagement zur einheitlichen Identifikation und adäquaten Steuerung sowie Überwachung von Risiken. Um den aufsichtsrechtlichen Anforderungen gerecht zu werden sowie mit den technologischen Entwicklungen Schritt zu halten, ist ein wirksames IKS daher unerlässlich. Allerdings gibt es einige Herausforderungen, welche die Wirksamkeit und Effizienz eines IKS beeinflussen¹:



Digitaler Transformationsprozess

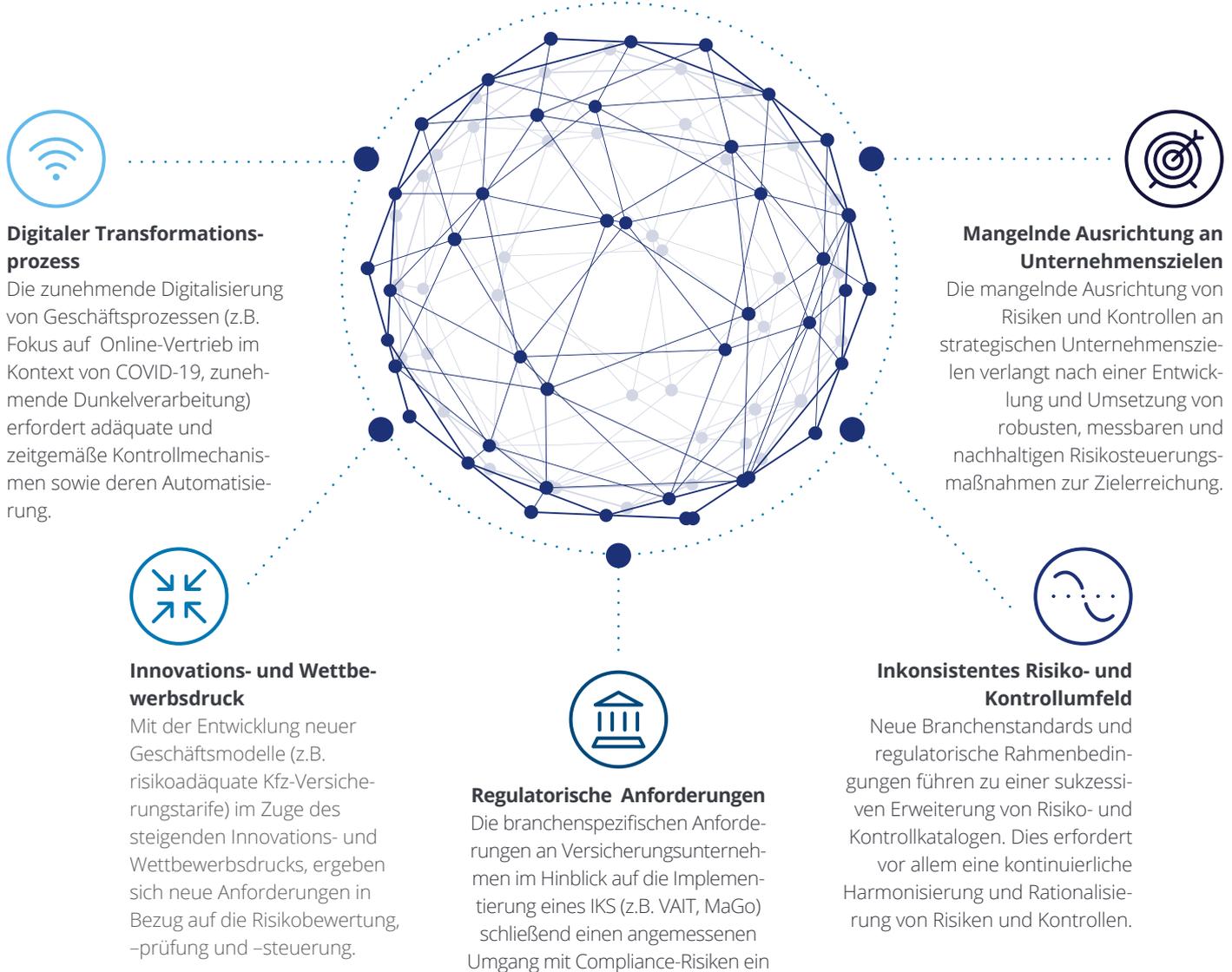
Die anhaltende digitale Transformation von Geschäftsprozessen wirkt sich zum Teil erheblich auf ein bestehendes IKS aus: Denn viele Versicherungsunternehmen haben ihre klassischen Vertriebsansätze (z.B. Ausschließlichkeitsvertrieb) um digitale Vertriebswege (z.B. Smartphone-Apps) erweitert, um dem Kundenverhalten gerecht zu werden. Aus Kundenperspektive wird dabei ein integriertes und kanalübergreifendes Ökosystem erwartet, welches den gesamten Wertschöpfungsprozess begleitet, und zwar vom Erstkontakt über das Beratungs- und Verkaufsgespräch bis hin zur Schadenabwicklung. Zudem haben die Kontaktbeschränkungen im Zuge der COVID-19-Pandemie deutlich gezeigt, dass Versicherungsgesellschaften das persönliche Serviceangebot im Rahmen von klassischen Vertriebsansätzen, wie Außendienst oder Callcenter, um ein breites Spektrum an digitalen Medien und Services erweitern müssen, um langfristig wettbewerbsfähig zu bleiben. Zugleich sind Versicherer bemüht, Dunkelverarbeitungsquoten zu

erhöhen. Dennoch gehen mit digitalen Versicherungsangeboten und der Verlagerung von Geschäftsprozessen neuartige Risiken einher (z.B. Verlängerung der Prozesse zum Kunden via Smartphone), denen Versicherungsunternehmen mit adäquaten und zeitgemäßen Kontrollmechanismen begegnen sollten.

Darüber hinaus kann sich ein IKS als äußerst unwirksam und ineffizient erweisen, wenn mit den technologischen Entwicklungen nicht Schritt gehalten wird. Insbesondere die unzureichende Nutzung von technologischen Möglichkeiten bei der Kontrollausführung, den Kontrolltests und der Überwachung von Risiken und Kontrollen schränkt die Wirksamkeit und Effizienz eines IKS stark ein. Insofern sollten im Zuge der Digitalisierung nicht nur die operativen Kernaktivitäten von Geschäftsprozessen angepasst bzw. neu modelliert, sondern auch die Automatisierung von Kontrollmechanismen entsprechend vorangetrieben werden.

Die digitale Transformation von Geschäftsprozessen erfordert adäquate und zeitgemäße Kontrollmechanismen des IKS.

Abb. 1 – Herausforderungen für Versicherungsunternehmen im Hinblick auf das IKS





Innovations- und Wettbewerbsdruck

Technologische Innovationen haben zugleich einen maßgeblichen Einfluss auf bestehende Marktstrukturen. Die fortschreitende Digitalisierung ist unter anderem dafür verantwortlich, dass Markteintrittsbarrieren sinken und neue Wettbewerber in die Versicherungsbranche drängen (z.B. Telematik-Start-ups). Vor allem für den konservativ ausgerichteten Versicherungsmarkt stellt dieser Trend eine große Herausforderung dar. Durch den Eintritt neuer Marktteilnehmer mit disruptiven Geschäftsmodellen ändert sich auch die Erwartungshaltung des Kunden an das Produktportfolio eines Versicherers.

Der verstärkte Fokus auf den Onlinevertrieb erfordert transparente Versicherungsprodukte mit einer geringen Komplexität, aber auch die Möglichkeit einer risikoadäquaten Tarifoption gewinnt zunehmend an Bedeutung. Die Konzeption eines risikoindividuellen Tarifs steht dabei im Kontrast zu bisherigen Tarifierungsgrundsätzen, wonach gleichartige Risiken (z.B. Alter, Schadenhistorie) kollektiv zusammengefasst werden. Zwar bieten risikoadäquate Tarife für Versicherer weiterreichende Chancen (z.B. Reduzierung von Schadenauszahlungen²), dennoch ergeben sich grundlegende Anforderungen in Bezug auf die Risikobewertung, -prüfung und -steuerung. Beispielsweise stellt sich die Frage, ob ein hinreichend geringes Individualrisiko unter Kosten-Nutzen-Abwägung überhaupt einer Kontrolle bedarf. Weiterhin würde eine „Echtzeit-Bepreisung“ (z.B. „Pay how you drive“-Kfz-Tarif) auf der Grundlage einer kontinuierlichen Datenerlieferung des jeweiligen Geschäftsvorfalles auch eine entsprechende „Echtzeit-Steuerung“ der Produktrisiken im IKS ermöglichen. Aus Risikomanagementsicht bedarf es hierfür vor allem innovativer und moderner IKS-Lösungsansätze.



Regulatorische Anforderungen

Ein IKS umfasst alle Grundsätze, Verfahren und Maßnahmen, die der Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftsprozesse (Operations), der Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung (Financial Reporting) und der Einhaltung relevanter rechtlicher Vorschriften (Compliance) dienen. Die verpflichtende Implementierung eines IKS kann auf verschiedenen gesetzlichen Grundlagen beruhen. Neben Anforderungen an ein IKS mit internationalen Auswirkungen (z.B. Sarbanes-Oxley Act für an US-Börsen gelistete Versicherer) existieren ebenso nationale Anforderungen. So interpretiert das Institut der Wirtschaftsprüfer in Deutschland (IDW) die allgemeine Leitungspflicht (§ 76 Abs. 1 AktG) und die Sorgfaltspflicht des Vorstandes (§ 93 Abs. 1 AktG) insoweit, dass Unternehmen verpflichtet sind, ein IKS einzurichten, welches Fehlentwicklungen aufdecken und die Grundlage für entgegensteuernde Maßnahmen bieten kann.

Aus branchenspezifischer Sicht verlangen die Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) eine explizite Berücksichtigung des Risikoprofils des Versicherers bei der Ausgestaltung des IKS sowie eine fortlaufende Überwachung der Angemessenheit und Wirksamkeit der internen Kontrollen. Weiterhin fordern die Versicherungsaufsichtsrechtlichen Anforderungen an die IT (VAIT) spezifische Kontrollmaßnahmen in der IT-Umgebung. Im Speziellen definieren die VAIT mit der Durchführung von Risikoanalysen (z.B. in Bezug auf die bestehenden Systeme) und Tests von Änderungen (z.B. hinsichtlich möglicher Inkompatibilitäten) zusätzliche Kontrollanforderungen zur sicheren Umsetzung von IT-Änderungen. Aus regulatorischer Perspektive verpflichten sich

Versicherungsunternehmen also nicht nur zur Einführung eines IKS, sondern auch zur Bereitstellung von angemessenen IT-Systemen und -Strukturen (s. VAG § 29 Abs. 3). Die regulatorischen Anforderungen an Versicherungsunternehmen steigen somit stetig und die aktuellen Prüfungen der BaFin zeigen zudem, dass diese auch ernst zu nehmen sind.



Inkonsistenzen in Bezug auf das Risiko- und Kontrollumfeld

Trotz zunehmender aufsichtsrechtlicher Anforderungen sind Interne Kontrollsysteme in vielen Versicherungsunternehmen lediglich hinsichtlich der Finanzberichterstattung ausgereift und nehmen in den operativen Bereichen eine eher untergeordnete Rolle ein. Oftmals werden Interne Kontrollsysteme erst dann von der Unternehmensführung priorisiert, wenn sich diese als unwirksam herausgestellt haben – eine Optimierung der Kontrollfunktion erfolgt, wenn überhaupt, erst nach Risikoeintritt. Dieses Vorgehen lässt jedoch nur reaktive Handlungsoptionen zu und führt mitunter zu hohen Kosten. Vor diesem Hintergrund ist es ratsam, die aktuelle Situation zu überdenken und bestehende IKS zu transformieren.

Zu den größten Hürden hierbei zählen die überwiegend unstrukturierten Risiko- und Kontrollkataloge auf Unternehmensebene. Ein wesentlicher Grund hierfür ist, dass Risiko- und Kontrollkataloge im Zeitverlauf immer umfangreicher werden. So haben neue Branchenstandards (z.B. DSGVO-konforme Einwilligungserklärung) und regulatorische Rahmenbedingungen (z.B. Cloud-Computing Framework) im Zuge der Digitalisierung in den vergangenen Jahren zu einer erheblichen Erweiterung von potenziellen Risikofaktoren geführt. Vor allem die Zunahme von nichtfinanziellen Risiken (z.B. Cyber-Risiken) hat zu einer sukzessiven Erweiterung von Risikotaxonomien geführt. Aufgrund des hohen Zeitdrucks bei der Umsetzung wurden in der Folge zahlreiche redundante und/oder doppelte Kontrollen eingeführt, die zu einem hohen Verbrauch finanzieller und zeitlicher Ressourcen geführt haben. Aber auch die Verlagerung von Risiken an andere Stellen im Prozess (oder in andere Prozesse) spielt in diesem Zusammenhang

eine wichtige Rolle. Insofern erfordert die zunehmende operative, regulatorische und finanzielle Komplexität einen umfassenden und vollständigen Überblick über alle existierenden Risiken und Kontrollen. Harmonisierung und Rationalisierung von Risiken können beispielsweise durch einen strukturierten Risikokatalog gelingen, auf dessen Grundlage die jeweiligen Risiken in den Prozessen angepasst werden.





Ausrichtung an Unternehmenszielen und -strukturen

Die Wirksamkeit und damit auch der Mehrwert eines IKS können aus Unternehmenssicht nicht nur durch ein uneinheitliches Verständnis von Risiko- und Kontrolldefinitionen beschränkt sein, sondern auch durch eine fehlende oder mangelnde Ausrichtung der Risiken und Kontrollen an den Unternehmenszielen. Dies führt mitunter zu einer Verlangsamung von Geschäftsprozessen und vermittelt oftmals ein falsches Verständnis und Sicherheitsgefühl in Bezug auf die Einhaltung von regulatorischen Anforderungen. Bedeutsamerweise sieht das international anerkannte Rahmenwerk, das sog. COSO II „Enterprise Risk Management – Integrated Framework“, eine klare strategische Ausrichtung des IKS anhand von Unternehmenszielen vor. Neben Zielen der Berichterstattung (Kommunikation von Finanzinformationen) und Regeleinhaltung (Einhaltung von gültigen Gesetzen und Vorschriften) existieren ebenso betriebliche (Effektivität und Effizienz der operativen Geschäftstätigkeit) und strategische Ziele (Unterstützung der Unternehmensstrategie). Die Zielfestlegung ist gewissermaßen die Voraussetzung für die anschließende Risikobeurteilung und -steuerung. Allerdings nutzen bisher wenige Unternehmen die Möglichkeit der steuerbaren Einwirkung von Risiken und Kontrollen auf die Erfüllung von Prozess- und Unternehmenszielen, doch Kontrollsysteme könnten erheblich zu einer besseren Entscheidungsfindung beitragen. Eine der größten Herausforderungen in diesem Zusammenhang ist die Entwicklung und Anwendung von robusten, messbaren und nachhaltigen Risikosteuerungsmaßnahmen zur Zielerreichung. Insofern werden die Chancen, die das IKS als ganzheitliches Steuerungswerkzeug bietet, von den Versicherungsunternehmen insgesamt noch zu wenig wahrgenommen.

Die Erfüllung von strategischen Unternehmenszielen im Rahmen des IKS erfordert robuste, messbare und nachhaltige Risikosteuerungsmaßnahmen.

Neben geeigneten Steuerungswerkzeugen als Beitrag zur Unternehmenssteuerung bedarf es auch einer optimalen Ausrichtung von Unternehmensstrukturen hinsichtlich der Überwachung von IKS-Aktivitäten. Als Organisationsmodell für ein funktionsfähiges, internes Überwachungssystem wird vielfach das „Three-Line-of-Defense-Modell“ verwendet. Jedoch kommt es in der Praxis gelegentlich zu Unstimmigkeiten bzw. Unklarheiten innerhalb der drei Verteidigungslinien. Häufig mangelt es beispielsweise an einem einheitlichen Konzept für die Überwachung von IKS-Aktivitäten oder es existieren unterschiedliche Risikosichtweisen und -bereitschaften innerhalb eines Unternehmens. Beispielsweise können eine ungemessene Rollenverteilung oder Inkompetenzen einem effizienten und effektiven IKS entgegenstehen. Außerdem kann sich eine abteilungsbezogene Sichtweise des IKS als unproduktiv herausstellen (d.h. keine End-to-End-Betrachtung). Als Reaktion darauf wäre die prozessuale Ausrichtung an Organisationsstrukturen i.S.e. Gesamtrisikobetrachtung eine weitere Herausforderung. Um eine schnellere und fundiertere Entscheidungsfindung im Kontext des Risikomanagements und der Organisationsgestaltung zu ermöglichen, sollte das Überwachungssystem daher optimiert und angepasst werden.

Abb. 2 – Gegenwärtige Kontrollschwächen im Rahmen des IKS





Der Status quo interner Kontrollsysteme birgt weitere Herausforderungen

Oftmals kämpfen Unternehmen auch an internen Fronten: So sind die unterschiedlichen Risikoarten, welche die Kontrolllandschaft nachhaltig prägen (v.a. Operational Risk, IT Risk, Cyber Risk, 3rd Party Risk, Strategic Risk), oftmals nicht harmonisiert. Dies betrifft insbesondere Taxonomien, Aufbau- und Ablauforganisationen, internes und externes Reporting, Datenbanken und IT-Systeme sowie Risikoidentifikations- und Risikobewertungsinstrumente. Es bedarf daher eines neuen und standardisierten Kontrollsteuerungsmodells und -systems sowie einer besseren Integration zwischen den am Risikomanagement beteiligten Unternehmensbereichen. Darüber hinaus bleiben technische Möglichkeiten oftmals ungenutzt, auch bei weniger digitalisierten Prozessen (s. Abb. 2). Die Digitalisierung eröffnet Unternehmen neue Möglichkeiten, insbesondere im Hinblick auf die Nutzung von Daten zur Schaffung von Transparenz. Beispielsweise können somit Risiken zielgerichteter bearbeitet werden. Auch werden bestehende Kontrollsysteme häufig nicht kritisch hinterfragt: So beruhen Risiken und Kontrollen oftmals nur auf Erfahrungswerten, allgemein gefassten Risiko- und Kontrollkatalogen oder sind zu „pauschal“ beschrieben. Unter Berücksichtigung der genannten Aspekte besteht die Gefahr, dass die Leistungsfähigkeit des IKS überschätzt wird.





2. Studienergebnisse

Im Rahmen der qualitativen Studie wurden leitende IKS-Verantwortliche von deutschen Versicherungsunternehmen sowie IKS-Experten von globalen Deloitte-Gesellschaften befragt. Um den beschriebenen Herausforderungen für Versicherungsunternehmen zu begegnen, werden die Elemente und Eigenschaften eines modernen IKS in Bezug auf (1) Organisation und Betriebsmodell sowie (2) Technologieeinsatz erörtert. Insbesondere werden (3) der Mehrwert eines modernen IKS und (4) dessen Beitrag zur Unternehmenssteuerung dargelegt.

1) Organisation und Betriebsmodell eines modernen IKS

Integration von IKS und Risikomanagement

Bezugnehmend auf die Notwendigkeit einer integrierten IKS- und Risikomanagementfunktion nannten die Experten unterschiedliche Gründe:

- Sicherstellung eines ordnungsgemäßen Prozessablaufs zur Erreichung von Unternehmenszielen.
- Die Identifikation und Priorisierung von Risiken durch das Risikomanagement ist Grundvoraussetzung für die Gestaltung effektiver Kontrollen im Rahmen des IKS.
- Die Integration beider Funktionen ermöglicht eine ganzheitliche, prozessübergreifende Betrachtung von Unternehmensrisiken und somit auch eine proaktive Reaktion auf den möglichen Risikoeintritt.

Framework zur Ausgestaltung eines IKS

Die zweite Frage widmet sich den Rahmenwerken und Prüfungsstandards hinsichtlich der Ausgestaltung eines IKS:

- Das COSO II ERM Framework (s. Abb. 3)³ gilt unter den Experten als maßgebend, da es eine umfassende und verständliche

Als zentraler IKS-Verantwortlicher stellt der Chief Controls Officer die effektive Zusammenarbeit zwischen den drei Verteidigungslinien sicher.

Grundlage für das IKS darstellt. Das Rahmenwerk ist für die Gestaltung eines IKS besonders empfehlenswert, da es für alle Risikokategorien innerhalb eines Unternehmens weitestgehend anwendbar ist, auch unabhängig davon, welche Technologien im IKS eingesetzt werden. Gleichzeitig ermöglicht der Technologieeinsatz eine bessere Umsetzung der insgesamt 17 COSO-Prinzipien. Dennoch weisen die Experten deutlich darauf hin, dass die Elemente des Rahmenwerks individuell an die Anforderungen eines IKS und die Risikobereitschaft eines Unternehmens anzupassen sind.

- Für die Ausgestaltung eines IKS im deutschen Versicherungsumfeld wurden das COBIT-Rahmenwerk sowie die MaGo und VAIT als zusätzliche Orientierung angeführt. Die beiden IDW-Prüfungsstandards PS 981 und PS 982/951 wurden ergänzend als Referenzen für das Risikomanagement und IKS im deutschen Versicherungskontext genannt.

Rollen und Verantwortlichkeiten innerhalb des IKS-Betriebsmodells

Die dritte Fragestellung adressiert die verschiedenen Rollen und Verantwortlichkeiten eines effektiven IKS-Betriebsmodells. Ergänzend zum Three-Lines-of-Defense Modell erachten die Experten die Einfüh-

rung eines Chief Controls Officer (CCO) sowie eines Controls Center of Excellence (CCoE) als äußerst sinnvoll:

- Der CCO unterstützt zum einen die 1st LoD (z.B. Schließung von Wissenslücken) und agiert zum anderen als Führungskraft der kontroll- und risikoüberwachenden Einheit der 2nd LoD. Der CCO ist dem Chief Operating Officer (COO) oder Chief Risk Officer (CRO) unterstellt.
- Die Tätigkeiten eines CCO umfassen je nach Einordnung des CCO in die 1st oder 2nd LoD (i) die Sicherstellung der Aufgabenerfüllung der 1st und der 2nd LoD im Rahmen des IKS sowie (ii) die Unterstützung der 1st LoD bei IKS-bezogenen Aufgaben als Teil von dieser. Als Führungskraft der IKS-unterstützenden Einheit der 2LoD kann ein CCO auch für (iii) die Richtigkeit der Inhalte des Kontroll-Rahmens verantwortlich sein oder (iv) für die zielführende Ausrichtung von IKS-Prüfprogrammen auf mögliche Schwachstellen im IKS und Risikomanagement durch die 3LoD.
- Als zentrale Experteneinheit für IKS-Themen agiert ein CCoE entweder (i) innerhalb der 2nd LoD (als methodikgebende und unterstützende Einheit), (ii) als unabhängige Stabseinheit oder (iii)

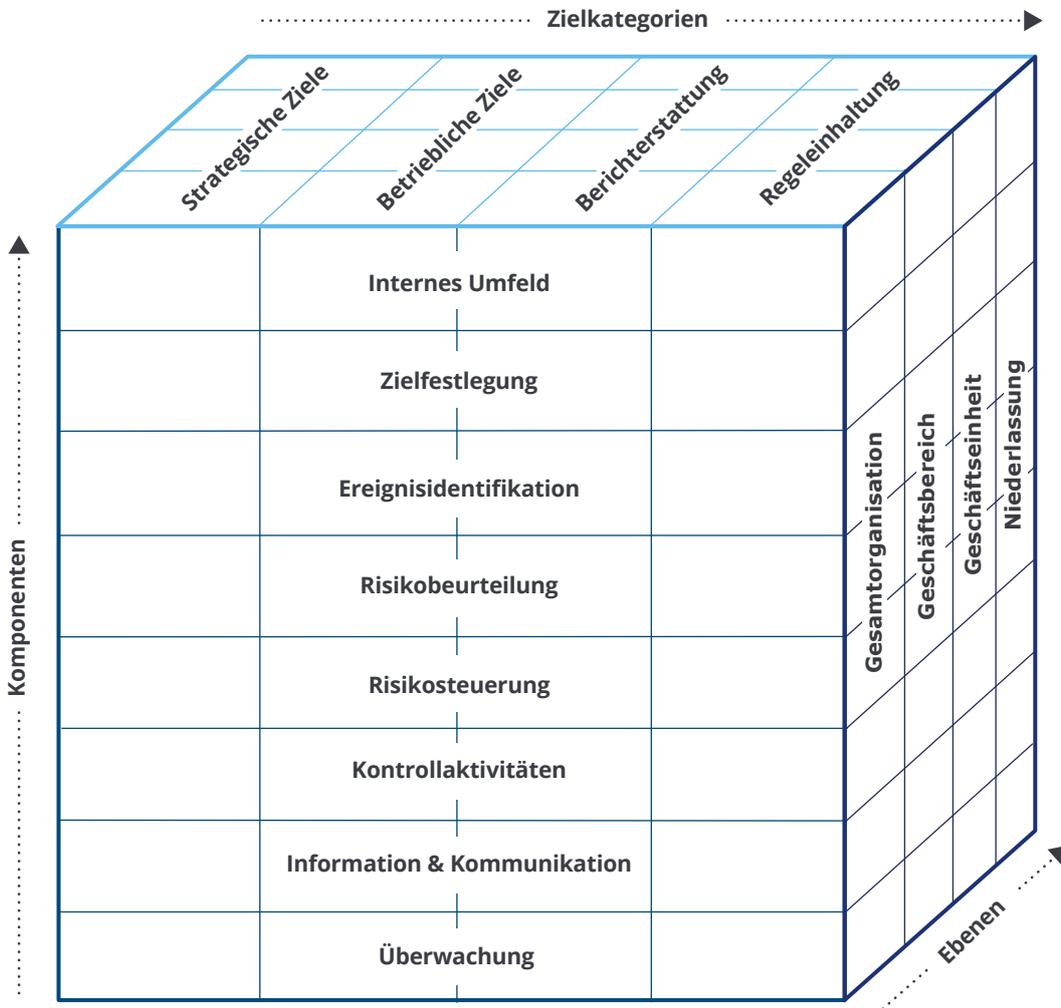


sogar als ausgelagertes Servicecenter. Die Zusammenarbeit des CCoE mit anderen IKS-Rollen sowie Art und Umfang der vom CCoE in Anspruch genommenen Beratungsleistungen sollten hinreichend definiert sein.

- Die Aufgaben eines CCoE umfassen die Unterstützung und Beratung der (i) 1st LoD bei der Gestaltung und Dokumentation von Kontrollen, (ii) der 2nd LoD beim Einsatz von Kontrollüberwachungs- und Berichterstattungsmethoden und (iii) des Managements bei der Behandlung von Kontrollschwächen und -eskalationsprozessen. Weitere Aufgaben beinhalten die (iv) Standardisierung der Methodik hinsichtlich Kontrollüberwachung bzw. Berichterstattung und Kontrollbewertungsverfahren sowie (v) die Prüfung der Einhaltung dieser Methodik. Ferner (vi) unterstützt das CCoE bei der Rationalisierung und Automatisierung von Kontrollen und (vii) treibt den Technologieeinsatz im IKS voran.

Die Nutzenpotenziale eines CCoE liegen vor allem in der erhöhten Standardisierung, Effizienz und Qualität der Kontrollen und Regelprozesse des IKS.

Abb. 3 – Aufbau eines IKS gemäß COSO II ERM Framework



Das COSO II ERM Framework dient als grundlegende Referenz für die Entwicklung eines effektiven und effizienten IKS, muss aber stets auf die jeweilige Risikoumgebung eines Unternehmens angepasst werden.

Kommunikation von IKS-Ergebnissen an die Geschäftsleitung

Die IKS-Berichterstattung an die Geschäftsleitung obliegt hauptsächlich der zweiten Verteidigungslinie (2nd LoD):

- Als Eigentümer von Prozessen, Kontrollen und Risiken in den operativen Bereichen ist die 1st LoD für die IKS-bezogene Berichterstattung an die 2nd LoD zuständig.
- In ihrer kontrollüberwachenden und berichterstattenden Funktion prüft die 2nd LoD die IKS-bezogene Berichterstattung der 1st LoD und aggregiert diese, um an die Geschäftsleitung zu berichten.
- Für eine Erhöhung der Wertschätzung des IKS befürworten die Experten eine direkte Berichterstattung der Bereichsleiter (Prozesseigentümer) an die Geschäftsleitung bzw. an den CCO, sofern dieser Teil der 1st Line ist, sowie der Risikobeauftragten an die unabhängige Risikocontrolling-Funktion der 2nd LoD bzw. an den CCO, sofern dieser Teil der 2nd Line ist.

Schaffung eines unternehmenseinheitlichen Verständnisses im Umgang mit Risiken und Kontrollen

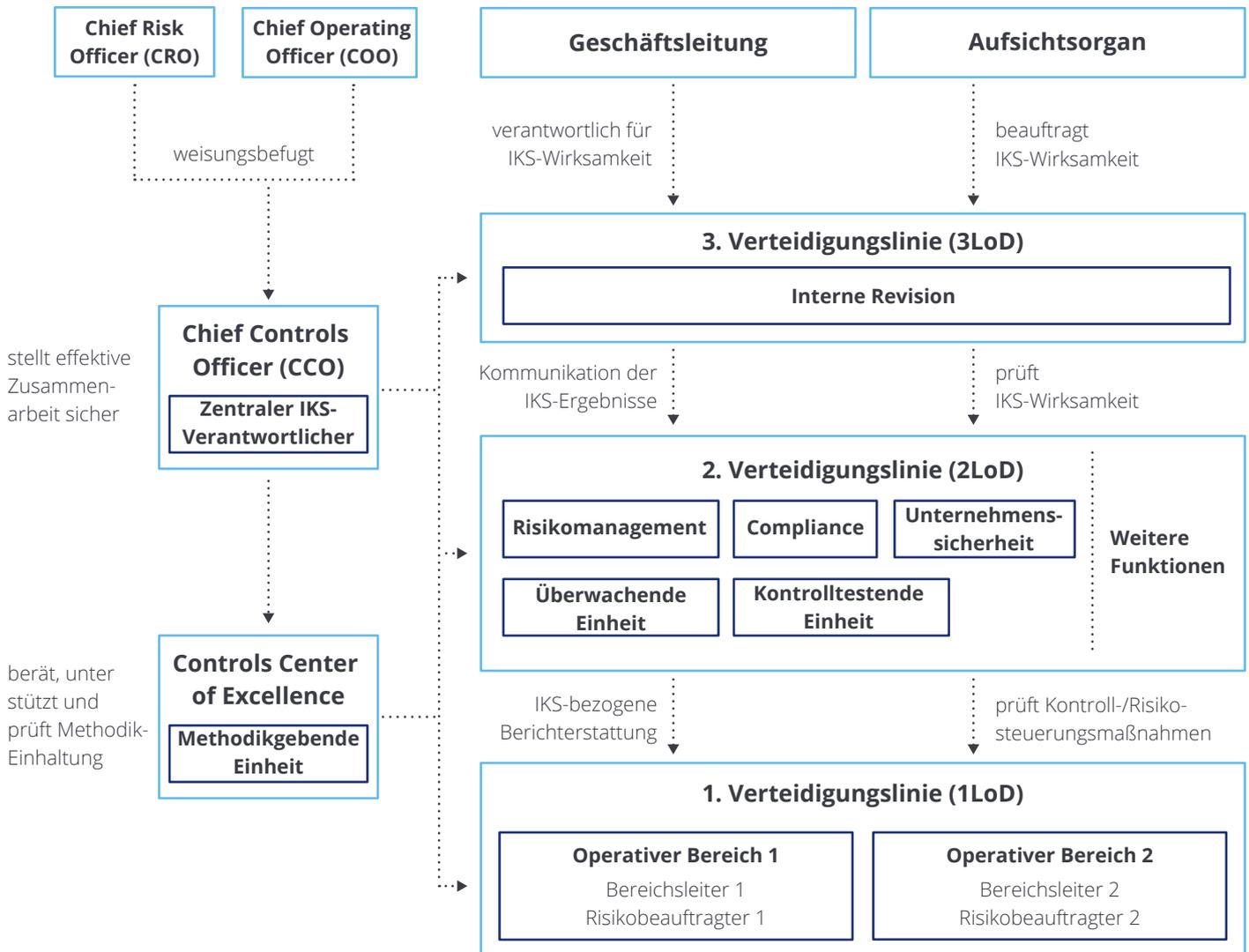
- Die Experten befürworten eine unternehmenseinheitliche, mit der Prozessmethodik abgestimmte Risiko- und Kontrolltaxonomie:
- Konzipierung und regelmäßige Aktualisierung einer gemeinsamen Risiko- und Kontrolltaxonomie (d.h. Strukturierung durch Gruppen- und Kategorienbildung) sowie die Erstellung einer standardisierten Kontrollbibliothek (d.h. Muster-Kontrollbeschreibungen) können zu einem konsistenten Verständnis von Risiken und Kontrollen beitragen.
- Ferner sollten die angewendeten Risiko- und Kontrollbewertungsmethoden der einzelnen Verteidigungslinien standardisiert oder zumindest vergleichbar gemacht werden.
- Die Vorteile der standardisierten IKS-Dokumentation und aggregierten Berichterstattung liegen darin, dass (i) mögliche Dokumentationsmängel ein-

zelner operativer Bereiche aufgedeckt und (ii) die Bedeutung der verschiedenen IKS-Berichte für die Geschäftsleitung besser einschätzbar und vergleichbar gemacht werden können.

- Zur Sensibilisierung des Unternehmens im Umgang mit Risiken ist zudem ein regelmäßiger Austausch hinsichtlich der IKS-Methodik unabdingbar, idealerweise zwischen allen beteiligten IKS-Rollen und -Verantwortlichkeiten.

Die Dokumentation von Standards für Risiken und Kontrollen ist essenziell, um über alle Unternehmensbereiche hinweg ein konsistentes Verständnis von und einen adäquaten Umgang mit diesen zu ermöglichen. In der Folge ergibt sich eine bessere Vergleichbarkeit von IKS-Berichten.

Abb. 4 – Betriebsmodell eines modernen IKS



2) Technologieeinsatz im Rahmen eines modernen IKS

Technologische Entwicklungen

Es wurde erörtert, welche Technologien im Bereich Prozess- und Datenmanagement zukünftig den größten Einfluss auf ein IKS haben werden:

- Technologische Möglichkeiten im Rahmen des IKS sollten für die (i) Automatisierung, (ii) Datenanalyse und Mustererkennung sowie (iii) Datenhaltung besser nutzbar gemacht werden.

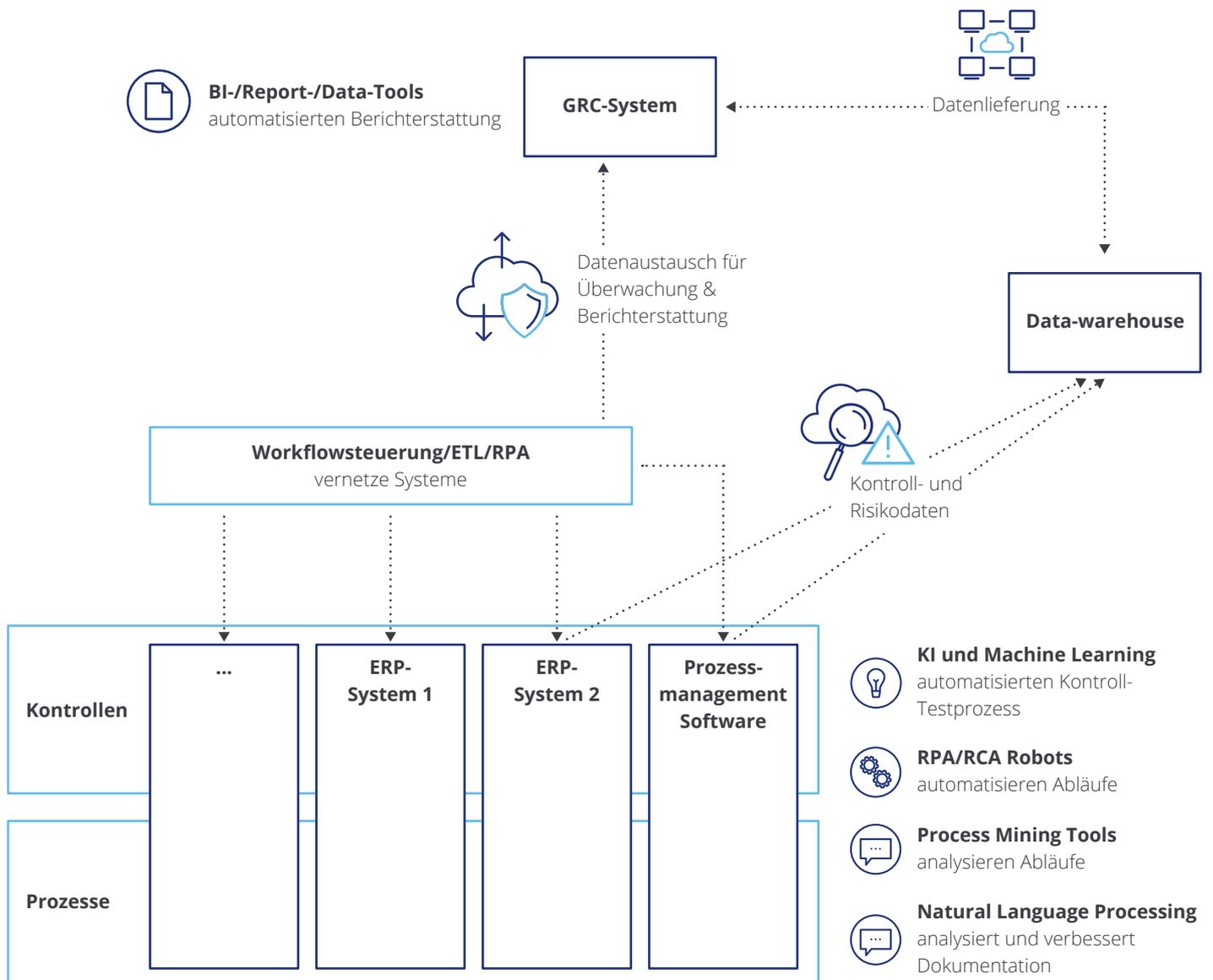
- Automatisierungstools (z.B. Robotics Process Automation (RPA), Robotic Cognitive Automation (RCA)) können den manuellen Aufwand für sich wiederholende und regelbasierte Aufgaben reduzieren und somit die Effizienz des IKS erhöhen.

- Mittels Datenanalyse (z.B. Data und Process Mining) können IKS-relevante Daten wesentlich schneller und umfassender ausgewertet werden. Korrelationen zwischen Risiken und Kontrollen können zudem mittels Software zur Mustererkennung (z.B. Machine Learning, Optical Character Recognition (OCR), Künstliche Intelligenz (KI)) aufgedeckt werden, um mögliche Ursachen eines Risikoeintritts zu identifizieren.

- Ferner werden Technologien zur Datenhaltung (z.B. Cloudservice, Data as a Service, Datawarehouse) die Arbeitsweise eines modernen IKS künftig prägen. Entsprechende Technologien sind auch als Standardlösungen zu beziehen und damit vergleichsweise günstig und einfach im IKS zu implementieren.

Mit einer verstärkten Automatisierung von Kontrollen liegt der Fokus künftig auch auf der Sicherstellung von Qualität und ordnungsmäßiger Funktionsweise der eingesetzten Technologien.

Abb. 5 – Technologie-Architektur eines modernen IKS



Kontrollausführung und -testprozess

Die Experten sprechen sich für eine intensivere Datennutzung für die Automatisierung der Kontrollausführungs- und -testprozesse aus:

- Während RPA sich vor allem zur Automatisierung von regelbasierten, einfachen Kontrollen oder Kontrolltests eignet, können komplexe fachliche Kontrollen oder Kontrolltests nur durch die Kombination mit intelligenten Automatisierungstechnologien wie RCA, KI oder Machine Learning automatisiert werden.
- Voraussetzung für eine Automatisierung von Kontrollausführungs- und -testprozessen ist eine hohe Transparenz bezüglich (i) der für die Kontrollausführungs- und -testprozesse benötigten Kontrolldaten, (ii) der Herkunft dieser Daten sowie (iii) der im Kontrolltestprozess verwendeten Bewertungsmethoden.
- Vorteile einer automatisierten Kontrollausführung liegen (i) in der besseren Nutzungsmöglichkeit von Mitarbeiterkapazitäten durch den Wegfall manueller Arbeitsschritte und (ii) in der höheren Verfügbarkeit von dokumentierten Kontrolldaten, die im Rahmen des Kontrolltestprozesses verwertet werden können.
- Vorteile eines automatisierten Kontrolltestprozesses liegen zum einen (i) in der vollständigen Bewertung der Grundgesamtheit aller Kontrollausführungen und der damit verbundenen Aussagekraft bezüglich der Wirksamkeit der Kontrolle. Zum anderen (ii) können Kontrollschwächen und negative Kontrollergebnisse schneller erkannt werden, sodass sich die kontrolltestende Einheit der 2nd LoD stärker auf deren Bewertung und Behebung fokussieren kann.
- Für eine selbstständige Implementierung der Kontrolltests und deren Beurteilung ist laut Expertenmeinung eine entsprechende Ausbildung im Umgang mit den Automatisierungstechnologien essenziell.

- Weiteres Einsatzpotenzial zur Automatisierung besteht in der Prüfung bzw. Sicherstellung der Qualität der IKS-Dokumentation: Natural-Language-Processing-Tools (NLP) könnten z.B. zur automatischen Erstellung von Kontrollbeschreibungen oder -abläufen verwendet werden. Ferner könnte in die automatisierte Auswertung der Kontrollbewertungen durch das GRC-System im Rahmen der IKS-Berichterstattung auch eine Prüfungslogik eingebaut werden, die bspw. eine fehlerhafte oder nicht den Anforderungen entsprechende Dokumentation der Funktionsprüfung von Kontrollen aufdeckt.

Outsourcing des Kontrolltestprozesses

Die Experten erachten eine teilweise oder vollständige Auslagerung des Kontrolltestprozesses unter gewissen Voraussetzungen als sinnvoll:

- Ein Unternehmen sollte eine Auslagerung insbesondere dann in Betracht ziehen, wenn es keine eigenen Kompetenzen oder Ressourcen zur Automatisierung von Kontrolltests besitzt.
- Die Auslagerung kann entweder an externe Dienstleister oder i.S.e. unternehmensgruppeninternen Auslagerung erfolgen (z.B. Mutter-/Tochtergesellschaften; gruppeninternes CCoE).
- Voraussetzungen für eine Auslagerung an Dienstleister sind vor allem Transparenz und Dokumentation bezüglich (i) der Art und des Detaillierungsgrads der eingesetzten Kontrollen, der (ii) kontrollrelevanten Daten sowie (iii) der Verwendung der Kontrollergebnisse durch die drei Verteidigungslinien.
- Dienstleister sollten wiederum über ein entsprechendes Fachwissen hinsichtlich der Geschäftssektoren und Branche des auslagernden Unternehmens verfügen, um die Kontrollen möglichst effektiv testen zu können.

- Vorteile für das auslagernde Unternehmen liegen in der möglichen (i) Kosteneinsparung und (ii) Qualitätssteigerung des Kontrolltestprozesses durch das Know-how des Dienstleisters (z.B. effektive Gestaltung; Automatisierung des Kontrolltestverfahrens).

Kontrollüberwachung und -steuerung

Den Einsatz von Technologien zur Kontrollüberwachung und -steuerung erachten die Experten als notwendig:

- Die Kontrollüberwachung umfasst nach Expertenmeinung nicht nur die Überwachung der Kontrollausführung, sondern auch die Überwachung der Ergebnisse des Kontrolltestprozesses.
- Die Überwachung der Kontrollausführung kann durch den Einsatz von RPA oder KI automatisch erfolgen. Ferner eignet sich Process Mining zur Analyse des automatisierten Kontrollablaufs sowie zur Aufdeckung der darin enthaltenen Fehler oder Ineffizienzen.
- Zur Überwachung des Kontrolltestprozesses können Datenanalyse-Tools verwendet werden. Für die Identifikation von Risikoanomalien, Handlungsmustern oder Kontrollschwächen eignen sich zudem Machine Learning und KI.
- Die erhobenen Daten sollten anschließend in ein Governance-Risk-Compliance-Tool (GRC-Tool) eingespielt werden. Als zentrales Überwachungssystem stellt dieses nicht nur die Verbindung zwischen den im IKS eingesetzten Technologie-Tools und den an der Kontrollausführung beteiligten Anwendungssystemen dar, sondern bildet auch die technologische Datenbasis für die IKS-bezogene Berichterstattung.
- Als Teil des GRC-Systems (oder damit verknüpft) können Workflowsteuerungs-Tools eine Verbindung zwischen den Prozessen der Kontrollausführung, den Kontrolltests und der Kontrollauswertung sowie der Berichterstattung herstellen.

- Wesentliche Vorteile einer technologieunterstützten bzw. automatisierten Kontrollüberwachung sind eine (i) schnellere Verfügbarkeit der Berichterstattung zur Kontrollwirksamkeit, (ii) bessere Nachvollziehbarkeit der Prüfungsaktivitäten sowie (iii) reversionssichere Dokumentation der Prüfungsergebnisse.

Datenerfassung und -auswertung

Die Erfassung und Auswertung von IKS-relevanten Daten sollte nach Expertenmeinung durch ein zentrales System erfolgen:

- Der Prozess der Datenerfassung und -auswertung beginnt üblicherweise in den Anwendungssystemen der operativen Bereiche, wo unternehmensbezogene Transaktionen bzw. Geschäftsprozesse erfasst und automatische Kontrollen durchgeführt werden.
- Durch Anwendungsschnittstellen und Übertragungsprozesse wie sogenannte ETL-Prozesse (Extract Transform Load) können kontrollrelevante Daten automatisch aus den Anwendungssystemen extrahiert und in ein zentrales GRC-System überführt werden. Die Ablage der zugehörigen kontrollrelevanten Datensätze sowie der Prozess-, Risiko- und Kontrolldokumentationen erfolgt idealerweise in einem zentralen Datawarehouse, auf das das GRC-System zurückgreifen kann.
- Die Daten im GRC-System sind die Basis für die automatische Erstellung von IKS-Berichten unter Verwendung bestimmter Tools zur Business-Intelligence-(BI-)Berichterstattung (z.B. Cognos, Breor), Visualisierung (z.B. Tableau, PowerBI) und Analyse (z.B. Ark, SPSS).
- Die Vorteile einer automatisierten Übertragung von kontrollrelevanten Daten an das GRC-System liegen in der (i) kontinuierlichen Überwachung von Risiken und Kontrollen, (ii) Echtzeit-Berichterstattung über die Wirksamkeit von Kontrollen und (iii) Warnung bezüglich der Überschreitung von Grenzwerten, Zeiträumen oder dem Eintritt von Kontrollschwächen.

3) Substanzieller Mehrwert eines modernen IKS

Quantitativer und qualitativer Mehrwert

Die IKS-Transformation bietet für Versicherungsunternehmen einen vielseitigen Mehrwert:

- Der quantitative Mehrwert spiegelt sich in Kostensenkungspotenzialen wider, die durch Automatisierung von Kontrollen, Testverfahren und Berichterstattungen realisiert werden können. Neben der Reduzierung von Durchlaufzeiten und Prüfungsfeststellungen (z.B. Interne Revision) können zudem etwaige, mit Bußgeldern versehene Compliance-Verstöße vermieden werden.

- Der qualitative Mehrwert liegt in der schnellen und umfangreichen Berichterstattung zu Risiko- und Kontrollinformationen. Hiervon profitieren Geschäftsführung und operatives Management (1st LoD) gleichermaßen, da die Erfüllung von Unternehmens- und Kontrollzielen besser bewertet werden kann. Das IKS trägt daher nicht nur zur strategischen Zielerreichung bei, sondern auch zur Einhaltung von Sorgfaltspflichten gegenüber Dritten. Ein weiterer Vorteil ist die ganzheitliche und aktuelle Sicht auf die globale Risikolandschaft. Somit können potenzielle Risiken oder unbewusste Veränderungen in Prozessabläufen frühzeitig erkannt und Steuerungsmaßnahmen einleitet werden (s. Kap. 4).

Die Transformation des IKS generiert für Unternehmen sowohl quantitative (z.B. Kostensenkung) als auch qualitative Nutzensvorteile (z.B. schnellere und umfangreichere Berichterstattung).

Ermittlung des quantitativen und qualitativen Nutzens

Der quantitative und qualitative Nutzen eines IKS lässt sich anhand bestimmter Kennzahlen und Methoden ermitteln:

- Der quantitative Nutzen ist nur schwer messbar, da dessen Gegenteil oftmals erst durch den finanziellen Schaden bei Risikoeintritt (z.B. Strafzahlung) erkennbar wird. Leichter zu berechnen sind hingegen Kosteneinsparungen, die auf einer projektbasierten IKS-Optimierung beruhen (z.B. Kapitalwert der geschätzten zukünftigen Einsparungen, Break-Even-Analyse).
- Der qualitative Nutzen lässt sich anhand eines Soll-Ist-Vergleichs ermitteln. So könnte der Nutzen eines IKS für die Prozessqualität z.B. auf Basis der Prozessfehleranzahl oder der Kundenzufriedenheit bewertet werden. Weiterhin könnte der Nutzen für Risikomanagement und Compliance auf Basis von erhöhter Kontrollzielerreichung und vermiedenen Regelverstößen gemessen werden.

4) Beitrag eines modernen IKS zur Unternehmenssteuerung

Risikosteuerung im Rahmen des IKS

Die Steuerung von Risiken ist elementarer IKS-Bestandteil gemäß den Anforderungen des COSO II ERM Framework:

- Als Instrument der Datenanalyse/-bereitstellung ermöglicht das IKS eine Aussage über die Wirksamkeit von risikomitigierenden Kontrollen: Jede Kontrolle fungiert als Datenpunkt, welcher sowohl Informationen über Kontrollschwächen als auch deren mögliche Ursachen innerhalb der Prozessumgebung erhebt. In der Folge können effektive Korrekturmaßnahmen zur Risikosteuerung abgeleitet werden.
- Eine schnelle Reaktion auf Risiken kann sich als Wettbewerbsvorteil für Unternehmen erweisen: Auf Basis detaillierter Informationen zu aktuellen Prozess- und Kontrollschwächen können notwendige Investitionsentscheidungen zu Prozessen und Technologien hinreichend begründet werden.
- Entscheidungen zur strategischen Unternehmensausrichtung können durch IKS-bezogene Berichterstattungen unterstützt werden: Beispielsweise kann die Entscheidung hinsichtlich einer Produkteinführung auf der Grundlage der aktuellen Risikosituation des Unternehmens oder der Fähigkeit zur IKS-Skalierung getroffen werden.
- Der Einblick in die Geschäftsprozesse durch Kontrollen und Risikoanalysen offenbart Steuerungsimpulse für Entscheidungen zur Automatisierung oder Rationalisierung von Prozessen und Kontrollen. Die Grundlage für Rationalisierungsentscheidungen stellt dabei immer eine Gegenüberstellung der Kontrollkosten und des Schadens bei Risikoeintritt dar.

Steuerungsmaßnahmen des IKS

Die Risikosteuerung beinhaltet Mechanismen und Maßnahmen zur Beeinflussung der Risikosituation:

- Die frühzeitige Erkennung von Risiken und Prozessschwächen kann durch präventive Steuerungsmaßnahmen gelingen, die Folgendes voraussetzen:
 - Kontinuierliche Identifikation und Beurteilung von Risiken durch die 1st LoD: Die Bewertung von Prozessrisiken wird mit Datenanalyse-Tools vorgenommen und mit der bestehenden Risikobereitschaft abgeglichen. Dies ermöglicht eine frühzeitige Erkennung des Risikoeintritts und die Einleitung notwendiger Risikosteuerungsmaßnahmen.
 - Befähigung zur Automatisierung und Datensammlung/-verarbeitung: Das IKS sollte in der Lage sein, negative Kontrollergebnisse in den Prozessen in Echtzeit zu identifizieren, um eventuelle Korrektur- oder Eskalationsmaßnahmen möglichst schnell in die Wege zu leiten.
- Eine alternative Maßnahme zur Echtzeitüberwachung von detektiven Kontrollen (z.B. 4-Augen-Prinzip) ist die Implementierung von präventiven Kontrollen (z.B. Funktionstrennung), die den Risikoeintritt bereits zum Zeitpunkt der Datenerfassung, d.h. präventiv, verhindern sollen. Allerdings lassen sich nicht alle detektiven Kontrollen durch eine präventive Kontrolle ersetzen bzw. das Ersetzen würde keinen substantziellen Mehrwert generieren. Daher empfehlen die Experten eine Kombination beider Kontrollarten.

Die frühzeitige Erkennung von Risiken und Prozessschwächen kann durch den Einsatz von präventiven Steuerungsmaßnahmen gelingen.



3. Strategieorientierte Transformations- und Steuerungsmöglichkeiten eines IKS

1) Elemente und Eigenschaften eines modernen IKS

Das vorliegende White Paper hat die Elemente und Eigenschaften eines modernen IKS auf der Grundlage von qualitativen Experteninterviews erörtert, welche im Folgenden zusammengefasst dargestellt werden:

- **Standardisierung:** Ein modernes IKS sollte einen hohen Grad an Standardisierung aufweisen. Dies reicht von standardisierten Prozess-, Risiko- und Kontrolltaxonomien über einheitliche Risiko- und Kontrollbewertungsverfahren bis hin zur Standardisierung von eingesetzten Technologien.
- **Automatisierung:** Die Automatisierung ermöglicht eine Effizienzsteigerung des IKS und eine gleichzeitige Kostensenkung, indem teure, zeitaufwendige manuelle Tätigkeiten rationalisiert werden.
- **Vernetzung:** Eine weitere Eigenschaft ist die Vernetzung der eingesetzten Technologien über programmierte Schnittstellen oder RPA sowie eine Vernetzung der Rollen im IKS durch eine verbesserte Kommunikation und klare Aufgabendefinition.
- **Strategische Ausrichtung:** Die Fokussierung auf strategische Prozessziele sowie die Ausrichtung der Kontrollen auf die Zielerreichung generieren einen Mehrwert für die Unternehmensführung und eine hohe Aufmerksamkeit für die IKS-Funktion.
- **Transparenz:** Standardisierung, Automatisierung und Vernetzung können erheblich zur Transparenz beitragen, und zwar hinsichtlich potenzieller Risiken im Unter-

Standardisierung, Automatisierung, Vernetzung und strategische Ausrichtung eines IKS schaffen hohe Transparenz und ermöglichen eine Rationalisierung.

nehmensumfeld sowie der Wirksamkeit von risikomitigierenden Maßnahmen. Zudem eröffnen sich neue Chancen in Bezug auf die aktive Prozessgestaltung, sprich die Verlagerung in operative Prozesse (d.h. risikoindividuell statt im Kollektiv). Zusätzlich bietet eine erhöhte Transparenz eine Grundlage zur Schaffung einer verbesserten Risikokultur und Wahrnehmung im Unternehmen im Sinne von „Steuerung“ statt „Verhinderung“.

- **Rationalisierung:** Mit entsprechender Transparenz kann letztendlich die Rationalisierung von redundanten Prozessen und Kontrollen gelingen. Die Rationalisierung sollte unter Berücksichtigung einer Kosten-/Nutzen-Abwägung (Kontrollkosten vs. Schaden bei Risikoeintritt) und risikoeffizienter Steuerung durch Optimierung von Qualität, Zeit und Kosten erfolgen. Das Reporting der Zielerreichung (z.B. über KPIs) stellt für das Management einen weiteren Mehrwert dar.

Auf dem Weg zu einem modernen IKS gibt es verschiedene Transformationshebel

Je mehr Hebel aktiviert werden, desto größer der Mehrwert, der mit einem IKS realisiert werden kann:

1. Umgestaltung des Betriebsmodells: Dies kann zum einen durch die Optimierung von Strukturen und Systemen mittels CCO und eine einheitliche bzw. aktuelle Risikotaxonomie gelingen oder durch den Aufbau eines CCoE. Eine weitere Möglichkeit besteht in der Adaption des IIA-Drei-Linien-Modells⁴, welches mehr Flexibilität im Design bietet. Der Fokus liegt dabei stärker auf dem Management von Risiken, indem die 2nd LoD nicht als „Verhinderer“ fungiert, sondern vielmehr als „Enabler“. Der Fokus liegt dabei auf der Erreichung von Geschäftszielen, wobei die Risiken in einem akzeptablen Bereich bleiben.

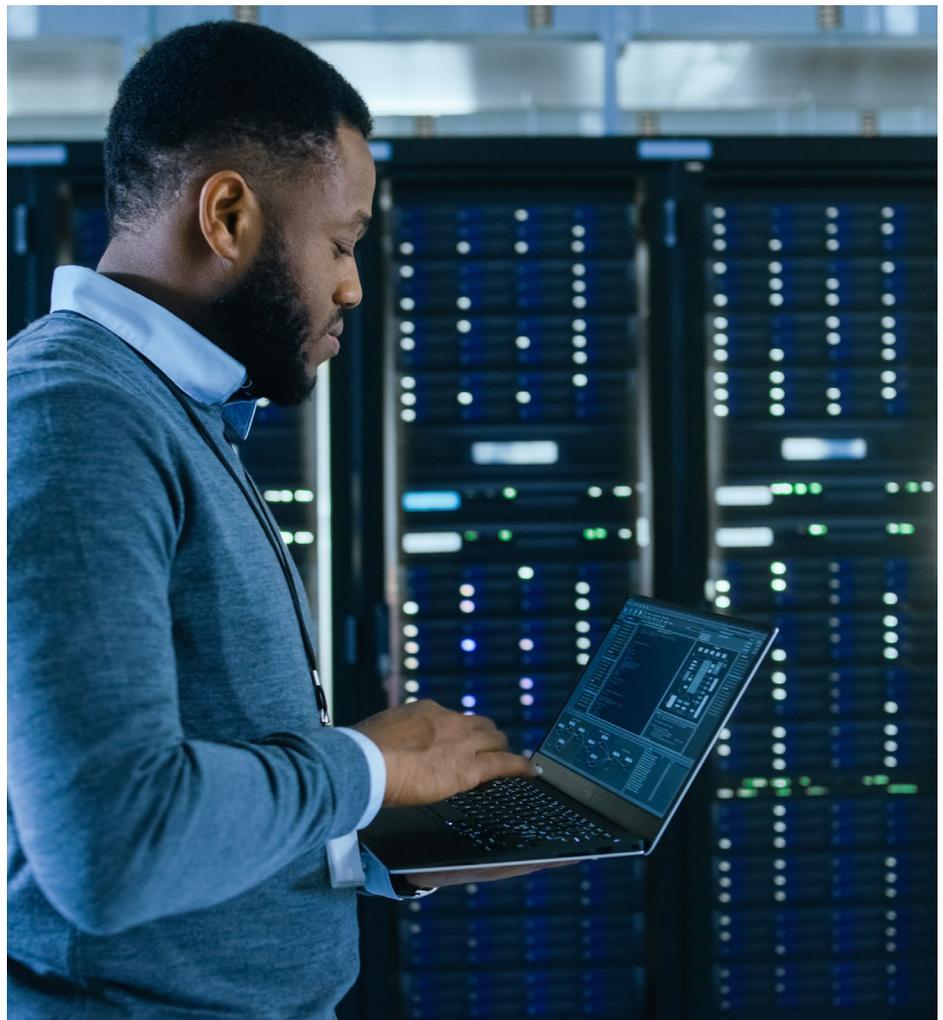
2. Technologie-Enablement: Dadurch kann die Automatisierung von Prozessabläufen vorangetrieben werden. Dies gilt für Prozesse im eigentlichen Sinne, aber auch für die Aufgaben im Rahmen des IKS-Regelkreislafs (z.B. Kontrollausführung, -test, -überwachung, IKS-Berichterstattung), vor allem im Hinblick auf eine kontinuierliche Risikoüberwachung und -steuerung.

3. Harmonisierung und Rationalisierung: Dieser Punkt umfasst die Harmonisierung und Rationalisierung von Risiken und Kontrollen innerhalb des Unternehmens und zielt auf eine Verbesserung des Überprüfungsprozesses unter Anwendung des „Test once, use multiple times“-Ansatzes ab.

Zusätzlich bietet eine erhöhte Transparenz eine Grundlage zur Schaffung einer verbesserten Risikokultur und Wahrnehmung im Unternehmen im Sinne einer Mehrwertschaffenden, proaktiven Steuerung von Risiken, statt nur als Kostenfaktor oder Verhinderer von Möglichkeiten gesehen zu werden.

Eine erfolgreiche IKS-Transformation offenbart für Versicherungsunternehmen weitreichende Vorteile

- **Kosteneffizient:** z.B. Beseitigung von Redundanzen; Fokus auf technologische Anpassung oder Verbesserung von zentralen Prüfverfahren
- **Erkenntnisorientiert:** z.B. Bereitstellung von risikospezifischen, intelligenten Informationen oder Kausalzusammenhängen und Korrelationen zwischen Risiken und Ereignissen
- **Geschäftsförderlich:** z.B. Integration von Kontrollen in „Business-as-usual-Prozesse (BAU)“ führt zur besseren User Experience und ermöglicht eine schnelle Lösung für Sonderfälle und Probleme.



2) Vom Kostenfaktor zum strategieorientierten Steuerungsinstrument

Trotz vielversprechender Transformativonsmöglichkeiten haben Versicherer den zusätzlichen Nutzen, den ein IKS als ganzheitliches Steuerungswerkzeug bieten kann, noch nicht erkannt: Denn das IKS kann erheblich zur Erfüllung von strategischen Zielen beitragen und dem Management einen echten Mehrwert bieten. Die Unterstützung der Unternehmensstrategie in Form der entsprechenden Zielvorgabe auf höchster Ebene geht ursprünglich auf das COSO II ERM Framework zurück. Der Beitrag, den ein modernes IKS zur Unternehmenssteuerung leisten kann, liegt vor allem in der Unterstützung von Entscheidungsprozessen durch eine detaillierte und aktuellere Informationslage zu Risiken sowie Prozess- und Kontrollschwächen. Durch die direkte Kommunikation von steuerungsrelevanten IKS-Informationen an die Geschäftsleitung profitiert die IKS-Funktion von einer hohen Aufmerksamkeit und erfährt somit eine größere Wertschätzung. Ein transparentes Bild der Risiken und Prozessschwächen unterstützt nicht nur die Entscheidungsfindung für Investitionen oder Rationalisierungen im Unternehmen, sondern kann darüber hinaus hilfreiche Informationen zur strategischen Ausrichtung im Sinne neuer Produkteinführungen oder Erschließung neuer Märkte liefern. Dies wird zukünftig besonders relevant sein, da Unternehmensorganisationen einem stetigen Wandel unterliegen, beispielsweise durch neue Vertriebswege oder Produkte. Daraus resultiert aber auch eine kontinuierliche Änderung bzw. Anpassung von strategischen Zielvorgaben, die sich aus regulatorischen und technologischen Anforderungen ergeben.

Letztendlich ermöglicht ein modernes IKS, von einer reaktiven zu einer schnelleren und vorausschauenden Risikosteuerung zu gelangen, indem mögliche Kontrollschwächen oder unerwünschte Kontrollergebnisse unmittelbar identifiziert und entsprechende Korrekturmaßnahmen zeitnah eingeleitet werden. Dies würde den Schaden im Falle eines Risikoeintritts abwenden oder zumindest begrenzen. Allerdings wird die Möglichkeit der steuerbaren Einwirkung von Kontrollen auf die Erfüllung von strategischen Unternehmenszielen in der

Versicherungspraxis bisher kaum genutzt. Daraus resultiert zudem das Erfordernis zur Skalierbarkeit von Kontrollen, um kontinuierliche Änderungen bzw. Anpassungen von strategischen Zielvorgaben abbilden zu können. Zur flexiblen Steuerung von Risiken und Prozessen – unter Berücksichtigung von Zeit-, Kosten-, und Qualitätsfaktoren – bedarf es eines ganzheitlichen, robusten und nachhaltigen Ansatzes. Der Weg des IKS vom Kostenfaktor hin zu einem strategieorientierten Steuerungsinstrument beschreiben wir beispielhaft anhand eines Schaden-/Leistungsprozesses aus der Versicherungsbranche:

1. Strategische Unternehmensziele analysieren und Prozesse strategisch gewichten:

Als strategische Unternehmensziele hat sich das Versicherungsunternehmen bspw. die folgenden strategischen Ziele mithilfe der Zielperspektiven einer Balanced Scorecard gesetzt:

- **Finanzperspektive:** z.B. Profitabilität steigern
- **Kundenperspektive:** z.B. Kundenzufriedenheit erhöhen
- **Prozessperspektive:** z.B. Prozesskosten reduzieren
- **Interne Perspektive:** z.B. Mitarbeiterbindung erhöhen

Ausgehend davon identifiziert und priorisiert der Prozessverantwortliche diejenigen Prozessgruppen bzw. Hauptprozesse, die zur Erreichung der strategischen Unternehmensziele wichtig sind. Als Input stehen unterschiedliche Informationen zur Verfügung (z.B. Prozesslandkarte, Prozessabläufe, Auswertungen).

In unserem Beispiel eines Schaden-/Leistungsprozesses ist der Prozess vor allem von den strategischen Zielen „Kundenzufriedenheit erhöhen“ und „Prozesskosten reduzieren“ betroffen bzw. kann zu diesen strategischen Unternehmenszielen einen wichtigen Beitrag leisten.

2. Ableitung von strategischen Prozesszielen:

Nach Priorisierung der Prozessgrup-

pen bzw. Hauptprozesse auf Basis der strategischen Ziele werden die strategischen Prozessziele formuliert. Für den Schaden-/Leistungsprozess leitet der Prozessverantwortliche die beiden Ziele „Prozesskosten reduzieren durch Vermeidung von Nacharbeiten“ und „Kundenzufriedenheit erhöhen durch schnellere Leistungsauszahlung“ aus den für seinen Prozess relevanten strategischen Unternehmenszielen ab.

3. Ableitung von operativen Prozesszielen:

Die Ableitung von operativen Prozesszielen orientiert sich in der Regel immer an den drei Faktoren Zeit, Qualität und Kosten:

- **Zeitfokus:** z.B. Verringerung von Responsezeiten durch einen integrierten Multi-Channel-Ansatz
- **Qualitätsführerschaft:** z.B. Fehlervermeidung durch die Minimierung von unabsichtlichen und absichtlichen Fehlern
- **Kostenführerschaft:** z.B. Minimierung von Prozesskosten durch effizientere Bearbeitung

Da diese drei Faktoren grundsätzlich in einem Zielkonflikt stehen (s. Punkt 9), sind diese entsprechend zu gewichten.

- In unserem Beispiel wurde unter anderem aus dem strategischen Prozessziel „Prozesskosten reduzieren durch das Vermeiden von Nacharbeiten“ das operative Prozessziel „Minimierung von unabsichtlichen und absichtlichen Bearbeitungsfehlern“ abgeleitet.

Die Formulierung von operativen Prozesszielen erfolgt anhand der SMART-Formel, wie beispielhaft beschrieben:

- **Spezifisch:** Minimierung von unabsichtlichen (d.h. Fehlerrisiko) und absichtlichen Bearbeitungsfehlern (d.h. Fraud-Risiko)
- **Messbar:** Messung anhand spezifischer Kennzahlen (z.B. Korrekturquote)
- **Ableitbar:** Aus dem strategischen Ziel „Qualitätsführerschaft“

- **Realistisch:** Es sollte klar sein, welche Methodik, Verfahren und Ressourcen verwendet werden.
- **Terminierung:** Das operative Ziel muss einen Zeitbezug haben, sodass man dieses zu einem bestimmten Wiedervorlage-termin überprüfen kann (z.B. zum Ende der Woche).

4. Messung von operativen Prozesszielen: Anhand geeigneter Prozesskennzahlen wird anschließend die Erreichung von operativen Prozesszielen vorangetrieben, die im Folgenden beispielhaft beschrieben werden:

- **Kennzahlen in Bezug auf Durchlaufzeiten:** z.B. Dauer der Durchlaufzeit eines Teilprozesses
- **Kennzahlen in Bezug auf Mengen:** z.B. Anzahl der Prozessdurchläufe
- **Kennzahlen in Bezug auf Entscheidungen:** z.B. Korrekturquote
- **Kennzahlen für Kapazitäten:** z.B. Arbeitsaufwand für bestimmte Aktivitäten
- **Kennzahlen in Bezug auf Kosten:** z.B. Personalkosten eines Prozesses pro Jahr

In unserem Beispiel ist hier besonders die Kennzahl der Korrekturquote, d.h. die Messung, wie viele der Leistungsauszahlungen im Prozessverlauf korrigiert werden müssen, relevant für eine Steuerung des Prozessziels der Fehlervermeidung.

5. Ableitung von Risiken: Anhand der operativen Prozessziele werden für eine bestimmte Aktivität mögliche Risiken identifiziert, die die Erreichung des Prozessziels beeinträchtigen können:

- **Prozessaktivität:** Auszahlung anstoßen (d.h. Leistungsauszahlung an den Versicherungsnehmer)
- **Risiken:** Auszahlung der Höhe und im Grunde nach falsch; interner Betrug bei Leistungsauszahlungen

6. Ableitung von Kontrollzielen: Neben operativen Prozesszielen können auch Kontrollziele aus den strategischen Prozesszielen abgeleitet werden. Dabei wird zunächst ein abstraktes Hauptkontrollziel abgeleitet, welches anschließend in Kontrollteilziele zerlegt wird, deren Einhaltung auch operativ überprüft werden kann:

- **Hauptkontrollziel:** z.B. Verhinderung von Leistungsauszahlungen in ungerechtfertigter Höhe
- **Erstes Kontrollteilziel:** z.B. Verhinderung des Fehlerrisikos von unabsichtlichen Leistungsauszahlungen
- **Zweites Kontrollteilziel:** z.B. Verhinderung des Fraud-Risikos von vorsätzlichen Leistungsauszahlungen

7. Kontrolldesign: Zur Erfüllung der Kontrollziele werden geeignete Kontrollen etabliert:

- **Kontrollart:** Stichprobenhafte Identifikation von einzelnen Leistungsauszahlungsfällen, die geprüft werden sollen; Qualitätskontrolle von einzelnen Leistungsauszahlungen im Rahmen einer Zweitfreigabe; Funktionstrennung der Benutzerberechtigungen im Bestandsführungssystem von Mitarbeitern in der Schadenerfassung und Leistungsauszahlung
- **Kontrollausführung:** manuell; (teil)automatisch
- **Kontrollfrequenz:** anlassbezogen mehrfach täglich

8. Messung von Kontrollzielen: Um Kontrollziele zu messen und den Zielerfüllungsgrad zu beurteilen, bedarf es eines verlässlichen, robusten und nachhaltigen Kennzahlensystems. Ein etablierter Ansatz zur Spezifizierung von effizienten und effektiven Kontrollprozessen ist der Return on Control Process Investment (RCPI):

- **Return on Control Process Investment (RCPI):** Mithilfe des aktivitätsbasierten Quantifizierungsverfahrens können Kon-

trollaktivitäten ökonomisch bewertet und entsprechend ihrer Kontrollziele optimiert werden. Basierend auf diesen Kontrollzielen wird der jährliche Schadenerwartungswert auf der Grundlage von Schadenpotenzialen (z.B. Geldbußen bei Nichteinhaltung eines Gesetzes) und Schadeneintrittswahrscheinlichkeiten (z.B. auf Basis von Vergangenheitsdaten) ermittelt. Im Anschluss erfolgt die Konkretisierung einzelner Kontrollaktivitäten anhand von:

- **Zeitfaktoren** (z.B. Dauer der Kontrollaktivität)
- **Qualitätsfaktoren** (z.B. Fehler-Entdeckungswahrscheinlichkeit)
- **Kostenfaktoren**⁵ (z.B. Kosten der Kontrollaktivität)

Abschließend erfolgt die Ermittlung des RCPI je Kontrollaktivität unter Berücksichtigung von Wechselwirkungseffekten der drei Faktoren. Aus der Menge der für die Einhaltung des jeweiligen Kontrollhauptziels geeigneten Kontrollkombinationen sollte theoretisch diejenige ausgewählt werden, die den größten ökonomischen Wert bzw. RCPI realisiert. Allerdings besteht in der Praxis ein klassischer Zielkonflikt zwischen Zeit, Qualität und Kosten eines IKS.

9. Maßnahmen zur Steuerung des IKS:

Im Folgenden werden die Maßnahmen zur Steuerung des IKS dargestellt und auf den Zielkonflikt zwischen Zeit, Kosten und Qualität sowie auf das Erfordernis zur Skalierbarkeit von Kontrollen eingegangen:

- **Zielkonflikt zwischen Zeit, Kosten und Qualität:** Kontrollaktivitäten sollten hinsichtlich ihres Kosten-/Nutzenaufwands geprüft werden. So wäre die Existenz einer Kontrolle nicht zu rechtfertigen, wenn die entsprechenden Kontrollkosten den potenziellen Schaden des Risikoeintritts übersteigen. Darüber hinaus sollte im Zuge einer Risikobeurteilung insbesondere der Zielkonflikt zwischen Zeit, Qualität und Kosten gemanagt werden. Anhand eines Leistungsauszahlungsprozesses, in dem 5 Prozent aller manuell bearbeiteten Leistungsfälle durch einen manuelle

Zweitprüfung kontrolliert werden, soll dieser Zielkonflikt erläutert werden. Abbildung 6

zeigt, dass die gleichzeitige Erfüllung aller drei Ziele (d.h. kürzeste Zeit, geringe Kosten und höchste Qualität) oftmals ein Optimierungsproblem darstellt: Soll beispielsweise die (1) Durchführungsdauer des Leistungsauszahlungsprozesses möglichst gering sein, müssen dafür u.U. hohe Kosten (z.B. Prozessschritte automatisieren) bzw. eine niedrige Qualität (z.B. weniger als 5% der Leistungsfallbearbeitungen erneut prüfen) in Kauf genommen werden. Sollen wiederum die (2) Kosten für die Zweitprüfung der Leistungsfallbearbeitungen möglichst gering sein, würde dies u.U. zu einem Zeitverzug (z.B. Aushilfen einsetzen) oder zu einer niedrigen Qualität (z.B. weniger Zweitprüfungen) führen. Die Gewährleistung einer (3) hohen Qualität ist hingegen oftmals mit hohen Kosten und einem Zeitverzug verbunden (z.B. 100% der Leistungsfallbearbeitungen prüfen oder ausschließlich Spezialisten für die Zweitprüfung einsetzen).

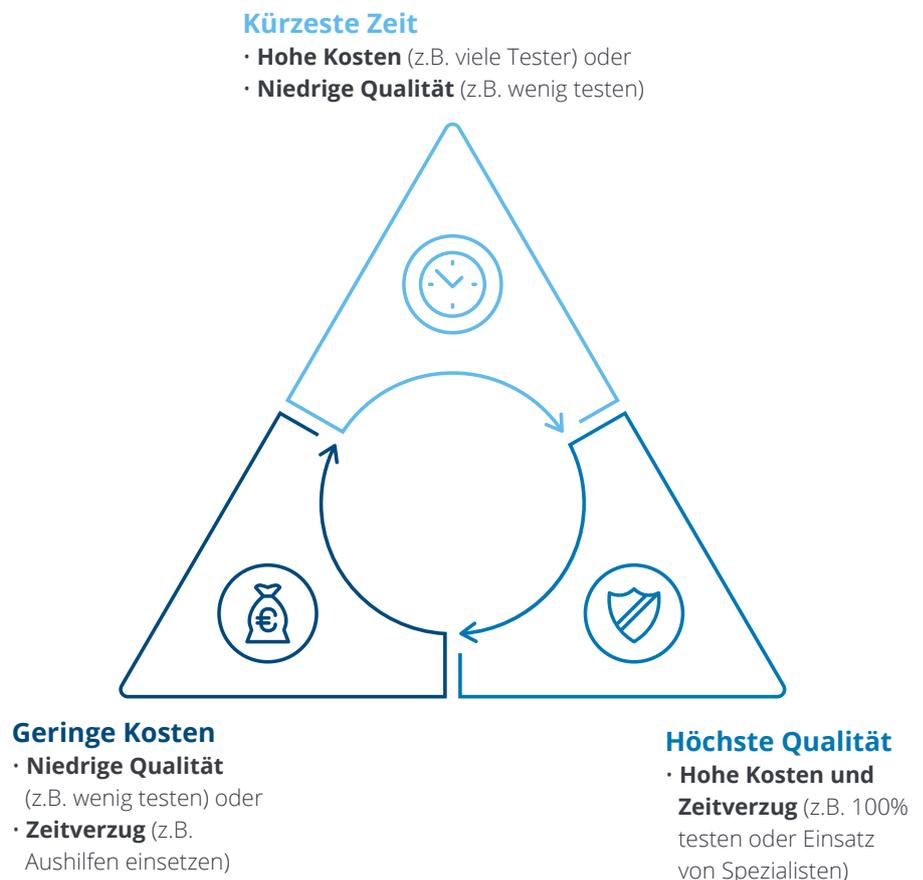
- **Skalierbarkeit von Kontrollen:** Die kontinuierliche Anpassung an sich ändernde strategische Zielvorgaben erfordert insbesondere die Skalierbarkeit von Kontrollen, um situativ zu handeln und den Anforderungen gerecht zu werden (z.B. regulatorische, technologische, kundenseitige Anforderungen). Daraus kann ein weiteres Optimierungsproblem resultieren: Beispielsweise möchte ein Krankenversicherer das bestehende Leistungsversprechen (z.B. Leistungsanträge werden innerhalb von 48 Stunden bearbeitet) trotz einer kurzfristig erhöhten Anzahl an Leistungsanträgen einhalten. Dabei erfolgt die Bearbeitung der Leistungsanträge weitestgehend in Form der Dunkelverarbeitung und eine manuelle Prüfung der bearbeiteten Leistungsanträge erst ab einer gewissen Leistungshöhe. Das Leistungsversprechen würde das „Zeitziel“ des Krankenversicherers in Form der schnellen Leistungsauszahlung aber nur erfüllen, wenn es dabei nicht zu Kapazitätsengpässen kommt. Da in der Regel die Arbeitskapazitäten kurzfristig nicht erhöht werden können, setzt der Krankenversicherer den Schwellenwert für die Leistungshöhe, ab

welcher manuelle Prüfungen erfolgen, herauf. Durch eine solche Reduzierung der Kontrollmaßnahmen können Kapazitätsengpässe reduziert werden. Dabei werden jedoch Nacharbeiten oder ungegerechtfertigte Auszahlungen in einem gewissen Maß in Kauf genommen. Das Beispiel zeigt, dass die variable Gestaltung der Kontrollen eine Skalierbarkeit ermöglicht. Auf diese Weise kann ein potenzieller Reputationsschaden vermieden werden, indem höhere Schadenaufwände in Kauf genommen werden (Trade-off: Reputationsschaden vs. finanzieller Schaden).

- **Automatisierung:** Eine Herangehensweise, um dem Optimierungsproblem zu begegnen, ist die Automatisierung von Prozess- und Kontrollaktivitäten. Wie im zweiten Kapitel des Papers beschrieben, kann die Automatisierung zu einer signi-

fikanten Qualitätssteigerung führen. Der Einsatz moderner Technologien wie RPA erhöht nicht nur die Fehlerentdeckungswahrscheinlichkeit von Kontrollaktivitäten, sondern ermöglicht darüber hinaus eine vollständige Bewertung aller Kontrollausführungen. Ferner trägt die automatisierte Kontrollüberwachung zu einer schnellen und reversionssicheren Dokumentation von Prüfungsergebnissen bei. Zudem reduzieren Automatisierungstools den manuellen Aufwand für sich wiederholende, regelbasierte Aufgaben und setzen dadurch zusätzliche Mitarbeiterkapazitäten für wertstiftende Tätigkeiten frei (z.B. Data Analytics). Nachdem die Implementierungskosten für entsprechende Technologien amortisiert werden, können Automatisierungstools zu einer signifikanten Kosteneinsparung im Vergleich zu manuellen Kontrolltätigkeiten führen.

Abb. 6 – Zielkonflikt zwischen Zeit, Kosten und Qualität



Fazit und Ausblick

Das vorliegende White Paper hat die aktuellen Herausforderungen für Versicherungsunternehmen im Hinblick auf bestehende IKS identifiziert. In erster Linie sollten (1) regulatorische Anforderungen, (2) digitale Transformationsprozesse, (3) Dynamiken im Innovations- und Wettbewerbsumfeld, (4) inkonsistente Risiko- und Kontrollsysteme sowie (5) eine mangelnde Ausrichtung an Unternehmenszielen zu einem Umdenken hinsichtlich des IKS-Betriebs führen. Die mit den Herausforderungen einhergehenden Kontrollschwächen bestehender IKS (z.B. falsches Verständnis und Sicherheitsgefühl in Bezug auf die Einhaltung von Compliance-Anforderungen, hoher Ressourcenverbrauch durch manuelle Kontrollausführungen oder der mangelnde Einsatz technologischer Möglichkeiten) sollten Versicherungsunternehmen daher zum aktiven Handeln bewegen. Die Transformation des IKS hin zu einem effizienten und effektiven Instrument kann insbesondere durch die Standardisierung, Automatisierung, Vernetzung sowie Ausrichtung auf strategische Unternehmensziele gelingen. Dies erhöht wiederum die Transparenz eines IKS, was vor dem Hintergrund immer komplexer werdender Geschäftsprozesse essenziell ist. Mit einer entsprechenden Transparenz kann letztendlich auch die Rationalisierung von redundanten Prozessen und Kontrollen gelingen. Die Praxisbeispiele aus der Versicherungsbranche haben aufgezeigt, wie das IKS vom Kostenfaktor („Verhinderer“) zum strategieorientierten Steuerungsinstrument („Steuerer“) transformiert werden kann. Vor allem durch Standardisierung, Automatisierung, Vernetzung und Transparenz kann das IKS für die Steuerung nutzbar gemacht werden. Zur flexiblen Steuerung von Risiken – unter Berücksichtigung von Zeit-, Kosten- und Qualitätsfaktoren – wurde ein konkretes Vorgehensmodell

vorgelegt, welches in der Versicherungsbranche in ausgereifter Form noch nicht vollumfänglich etabliert ist. Dieses stellt die Messbarkeit des Erfolges – d.h. die erfolgreiche Umsetzung einer Strategie durch KPIs – in den Mittelpunkt der Betrachtung.

Der neue Steuerungscharakter des IKS stellt ein klares Differenzierungsmerkmal im Hinblick auf eine effiziente Prozessgestaltung der Zukunft dar. Durch den Einsatz geeigneter Technologien können Unternehmen dem generellen Optimierungsproblem zwischen Zeit, Kosten und Qualität langfristig begegnen. Durch die zunehmend einfachere Anwendbarkeit von Künstlicher Intelligenz und die größere Verfügbarkeit von kontrollrelevanten Informationen eröffnen sich somit neue Möglichkeiten der Steuerung für das IKS. Der Fokus auf die Automatisierung kann auch zu einer signifikanten Qualitätssteigerung von Kontrollaktivitäten führen und gleichzeitig zu einer Reduktion des damit verbundenen Zeitaufwands. Sind die Investitionskosten für entsprechende Technologien erst einmal amortisiert, können zudem enorme Kosteneinsparungen realisiert werden. Für die Weiterentwicklung des IKS zu einem effizienten, effektiven, automatisierten und digitalen Steuerungswerkzeug verfügt Deloitte nicht nur über die notwendigen Kompetenzen (fachlich, rechtlich, methodisch, technisch) und Allianzen (z.B. SAP, IBM, Google, Amazon), sondern auch über weitreichende IKS-Projekterfahrung in unterschiedlichen Branchen. Als Vorreiter in neuen Technologien im Hinblick auf die Kontrollautomatisierung (z.B. RPA, Natural Language Understanding, GRC-Systeme) unterstützt Deloitte Versicherungsunternehmen bei der Transformation zu einem flexiblen und agilen IKS der Zukunft.

Literatur

- Eling und Kilgus (2014): Wirksamkeit und Effizienz der Regulierung in der deutschsprachigen Assekuranz – Eine juristische und ökonomische Analyse, Institut für Versicherungswirtschaft der Universität St. Gallen, S. 1–44.
- Weidner et al. (2017): Telematic Driving Profile Classification in Car Insurance Pricing, *Annals of Actuarial Science*, 11(2), S. 213–236.
- Bungartz (2018): Handbuch Interne Kontrollsysteme – Steuerung und Überwachung von Unternehmen, Erich Schmidt Verlag, S. 55ff.

Quellen

01. Die „Wirksamkeit“ und „Effizienz“ einer Regulierungsmaßnahme sind in der Assekuranz von hoher Bedeutung. Während die „Wirksamkeit“ als Qualitätsindikator hinsichtlich des Erfüllungsgrads der IKS-Ziele gilt, spiegelt sich die „Effizienz“ in dem erzielten ökonomischen Nutzen wider, der den Zeit- und Kostenaufwand übersteigt (Eling und Kilgus 2014).
02. Die jährliche Fahrleistung sinkt bei einem Wechsel in einen „Pay how you drive“-Tarif um durchschnittlich 10%, was wiederum das Unfallrisiko um 12–15% reduziert. Dies kann langfristig gesehen zu einer Verbesserung der Risikostruktur im Kollektiv eines Versicherers führen (Weidner et al. 2017).
03. Quelle der Abbildung: Bungartz (2018), S. 55 ff
04. Siehe Veröffentlichung des Institute of Internal Auditors (IIA) 2020 „The IIA’s Three Line of Defense Model. An Update of the Three Lines of Defense“.
05. Laut der Experten sind die fixen und variablen Hauptkostenfaktoren (i) der Personalaufwand in Vollzeitäquivalenten für Kontrollausführung und -test, (ii) die Implementierungs-, Wartungs- und Lizenzkosten für Software und Hardware der eingesetzten Technologien sowie (iii) der Schulungsaufwand der Mitarbeiter der drei Verteidigungslinien für IKS-Betrieb und IKS-Prüfung, Aufwand für Dokumentation, Formalisierung und andere IKS-bezogene Aufgaben der 2nd LoD.

Ihre Ansprechpartner



Alexander Thoma

Director | Deloitte Insurance Group

Tel: +49 91 12307 4590

athoma@deloitte.de



Tilman Parpart

Manager | Deloitte Insurance Group

Tel: +49 71 11655 47535

tparpart@deloitte.de

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeiterinnen und Mitarbeiter liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die mehr als 345.000 Mitarbeiterinnen und Mitarbeiter von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.