Studie 2021/22

Maturität der Compliance Management Systeme bei Schweizer Versicherungs-gesellschaften

mazars

Zürcher Hochschule für Angewandte Wissenschaften

zh aw School of Management and Law

Management Summary

Im September und Oktober 2021 hat Mazars in Zusammenarbeit mit der ZHAW School of Management and Law eine Umfrage betreffend Maturität von Compliance Management Systemen bei Schweizer Versicherungsgesellschaften durchgeführt.

An der Online-Befragung nahmen insgesamt 24 Versicherungsgesellschaften aus den Aufsichtskategorien 2-5 teil. Die Ergebnisse dieser Umfrage basieren auf den individuellen Einschätzungen der befragten Compliance-Verantwortlichen, die insgesamt 94 Aussagen bewerteten.

Der Reifegrad der Compliance Management Systeme wird insgesamt positiv beurteilt. Insbesondere attestieren die Compliance-Verantwortlichen den Unternehmen eine hohe Compliance-Verpflichtung. Compliance geniesst einen entsprechend hohen Stellenwert.

Besonders erfreulich ist dabei, dass Verwaltungsräte und Geschäftsleitungen gemäss den befragten Compliance-Verantwortlichen mit gutem Beispiel vorangehen und damit einen Schlüsselbeitrag zu einer starken Compliance-Kultur in ihren Gesellschaften leisten.

Lücken verorten die Befragten allerdings in der Implementierung. Dies zeigt sich insbesondere darin, dass direkte Vorgesetzte nicht in jedem Fall sicherstellen, dass die Compliance-Verpflichtungen des Unternehmens in die Prozesse integriert und durch die Mitarbeitenden erfüllt werden. Auch kommt dem Thema «Compliance» im Rahmen der Zielvereinbarungen und den periodisch stattfindenden Gesprächen zur Zielerreichung bisher eine noch eher untergeordnete Bedeutung zu.

Dies birgt die Gefahr, dass die Compliance-Verpflichtungen, denen sich die oberste Geschäftsführung verschrieben hat, nicht wie erwünscht Teil der «DNA» werden. Ein Erklärungsgrund könnte die Einschätzung der Compliance-Verantwortlichen sein, wonach die Geschäftsleitungen den Compliance-Funktionen durchaus noch etwas mehr Ressourcen für die Erfüllung von Compliance-Zielsetzungen zusprechen könnten.

Alle befragten Versicherungsgesellschaften stellen ihren Mitarbeitenden einen Meldekanal zur Verfügung, der intern regelmässig beworben wird.

Die Compliance-Verantwortlichen gehen jedoch davon aus, dass es Mitarbeitende gibt, die beim Erstatten einer Meldung negative Konsequenzen befürchten. Diese Einschätzung wird mit der tiefen Anzahl eingegangener Meldungen im Verlauf des Jahres 2020 pro 100 Mitarbeitende unterstrichen.

Fehlendes Vertrauen der Mitarbeitenden in den Meldekanal der Unternehmen sowie dessen technische Ausgestaltung könnten mögliche Gründe für die tiefe Melderate sein.

Die Compliance-Teams der befragten Versicherungsgesellschaften decken ein breites Spektrum an beruflichen Erfahrungen und Fertigkeiten ab. Insbesondere juristische Kenntnisse sind am meisten verbreitetet. Nur vereinzelt verfügen Versicherer bereits über Fertigkeiten im Bereich von Data & Analytics oder der künstlichen Intelligenz zur Unterstützung von Compliance-Tätigkeiten. Vor dem Hintergrund der technischen Möglichkeiten und des steigenden Bedarfs an automatisierter Erkennung potenzieller Normenverletzungen ist davon auszugehen, dass sowohl Data & Analytics als auch künstliche Intelligenz im Bereich der Compliance eine zunehmend bedeutende Rolle spielen werden.

Die vorliegende Studie zeichnet ein positives Bild der Maturität der Compliance Management Systeme auf. Nach Einschätzung der Compliance-Verantwortlichen sind die Versicherer insbesondere in den Bereichen «Verpflichtung» sowie «Prozesse und Instrumente» bereits weit fortgeschritten. Etwas kritischer stufen die Befragten den Reifegrad bezüglich Schulung, Awareness, Interaktion ein. Das grösste Entwicklungspotential besteht in der Entwicklung und Implementierung von Prozessen, Instrumenten und Praktiken, welche eine Leistungsbeurteilung erlauben.

Eine individuelle Analyse des Reifegrads eines Unternehmens im Vergleich zu den Ergebnissen dieser Umfrage («Benchmarking») ist auf Wunsch möglich. Auch besteht die Möglichkeit, anhand einer anonymen Online-Befragung die Einschätzung der Mitarbeitenden betreffend Compliance Management System einzuholen.

Zürich, Februar 2022

Inhaltsverzeichnis

Methodologie der Umfrage

Maturitätsmodelle zeigen verschiedene Reifegradstufen auf, die eine Unternehmung in Bezug zu ausgewählten Prozessen, Fähigkeiten oder Praktiken durchläuft. Die Stufen basieren häufig auf Standards, internen oder externen Vorgaben. Eine Einschätzung bezüglich Maturität liefert Erkenntnisse zum aktuellen Stand und Entwicklungspotential und bietet auch die Möglichkeit eines Vergleichs («Benchmarkings»).

Im Rahmen dieser Studie wurde ein Maturitätsmodell für die Beurteilung von Compliance Management Systemen entwickelt. Das Modell basiert auf ISO 37301, FINMA-Vorgaben sowie Erkenntnissen aus Expertengesprächen. Insgesamt wurden Teilnehmende zu sechs Bereichen befragt:

1) Grad der Verpflichtung zu Compliance,
2) Art der Umsetzung von Vorgaben,
3) Umfang der Risikobeurteilung,
4) Stand von Schulungen / Awareness / Interaktion,
5) Leistungsbeurteilung sowie
6) Umsetzung von Prozessen und Instrumenten.

Im Rahmen einer Selbstbeurteilung von insgesamt 94 Aussagen resultiert eine Maturitätseinschätzung. Teilnehmende wurden beispielsweise gefragt, inwieweit sie der Aussage zustimmen, dass die «Compliance-Policy ihres Unternehmens mit den Werten, den Zielen und der Strategie der Organisation abgestimmt ist».

Bei einer Selbsteinschätzung zu dieser und weiteren Aussagen «stimme vollständig zu», erfüllt das Unternehmen die Stufe «angemessen». Ein ungewichteter Mittelwert bestimmt in der Summe die Maturitätsstufe pro Bereich. Die Online-Befragung wurde durch Experten getestet und fand vom 13. September bis 25. Oktober 2021 statt.

Teilnehmende Versicherungsgesellschaften

An dieser Umfrage haben insgesamt 24 Schweizer Versicherungsgesellschaften aus den Aufsichtskategorien 2 bis 5 teilgenommen. Die Aufteilung nach Geschäftsfeldern beträgt 12 Lebens- / Sachversicherer, 8 Krankenversicherer sowie 4 Rückversicherungsgesellschaften. Befragt wurden Führungsverantwortliche aus den Compliance-Bereichen.

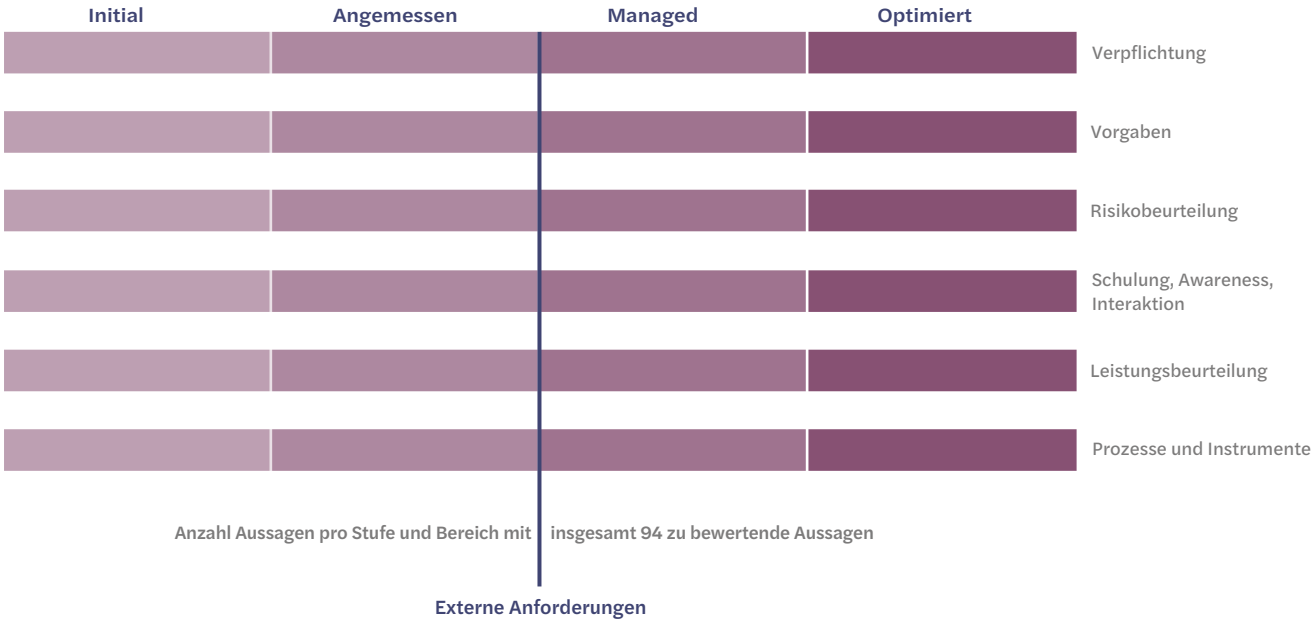
Methodik

Das Modell besteht aus vier Maturitätsstufen, die mittels 94 Aussagen konkretisiert sind. Diese Aussagen werden sechs Bereichen zugeordnet.

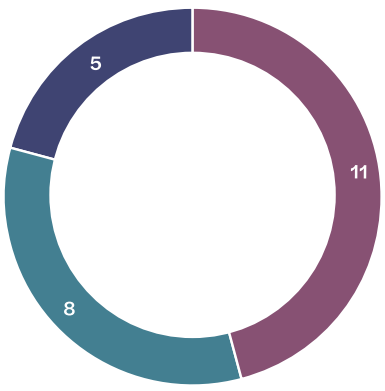
Die Stufen «Initial» und «Angemessen» orientieren sich an externen Anforderungen. Aussagen der Stufen «Managed» und «Optimiert» bauen darauf auf.

Die Teilnehmenden beurteilten, ob die Aussagen vollständig, teilweise oder nicht zutreffen.

Der Maturitätsscore ergibt sich aus der ungewichteten Summe der Mittelwerte pro Stufe.



Lebens- / Sachversicherer
Krankenversicherer
Rückversicherer
n=24



Kategorie 2
Kategorie 3
Kategorie 4
n=24

Kernaussagen

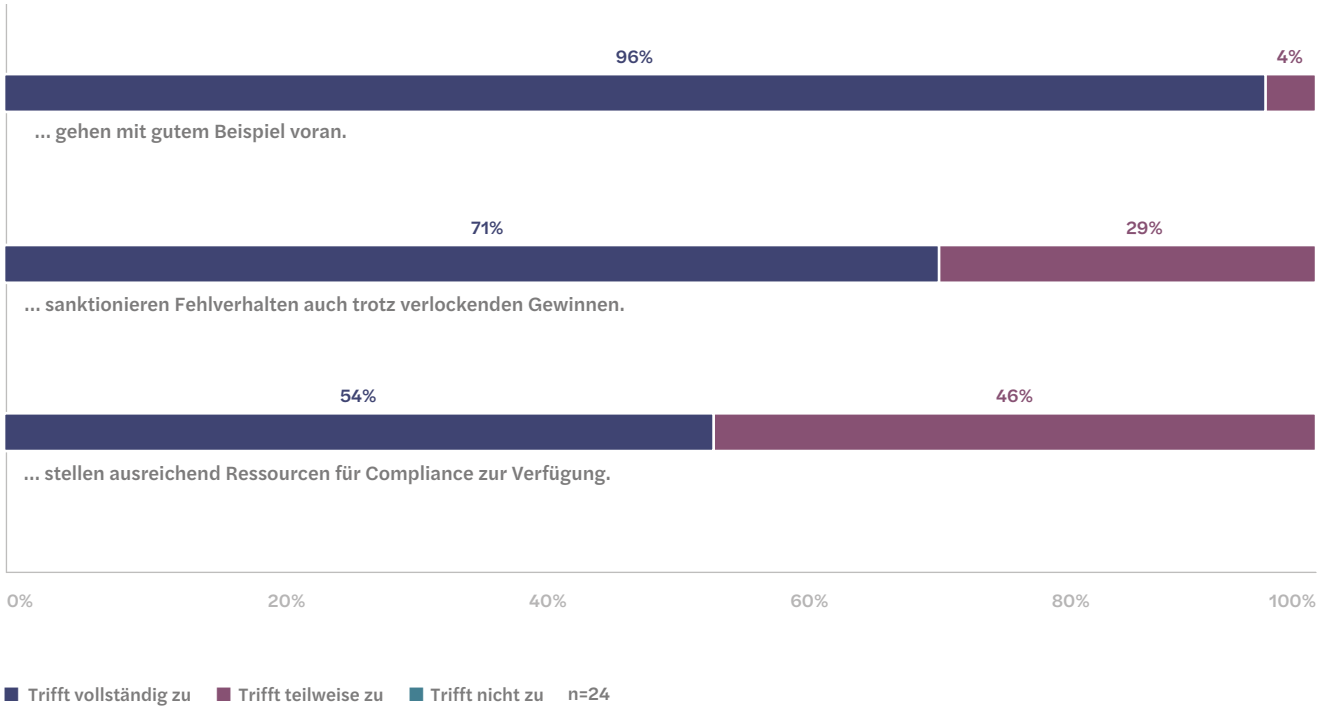
Finanzierung

Während Verwaltungsrat und Geschäftsleitung nach Ansicht der Befragten wesentlich zur Überführung der Compliance-Verpflichtungen in den betrieblichen Alltag beitragen, wird die entsprechende Bereitstellung von Ressourcen kritischer gesehen.

Mit einigen wenigen Ausnahmen trifft es vollständig zu, dass der Verwaltungsrat und die Geschäftsleitung mit gutem Beispiel vorangehen und die vom Unternehmen geforderten Verhaltensnormen selbst auch vorleben. Die Vorbildfunktion des Verwaltungsrates und der Geschäftsleitung ist denn auch einer der bedeutendsten Schlüsselfaktoren zur Beeinflussung der Compliance-Kultur. Damit Compliance-Verantwortliche aber auch erfolgreich die Compliance-Massnahmen umsetzen können, sind die notwendigen Ressourcen für geeignetes Personal, Verfahren oder angemessene Prozesse unabdingbar.

Dass den Compliance-Funktionen ausreichend Ressourcen zugestanden werden, trifft aber nur für wenige Befragte vollständig zu. Die tiefste diesbezügliche Zustimmungsrate weisen die Versicherungsgesellschaften der Aufsichtskategorie 4 auf.

Verwaltungsrat und Geschäftsleitung ...



Verpflichtung zu Compliance

Die Vorbildfunktion des Verwaltungsrates und der Geschäftsleitung hinsichtlich Einhaltung der geforderten Verhaltensnormen wird aus der Sicht der Compliance-Verantwortlichen durchwegs positiv beurteilt. Verbesserungsbedarf besteht auf Stufe der direkten Vorgesetzten, wenn es darum geht, die Compliance-Verpflichtungen des Unternehmens in die Arbeitsprozesse zu integrieren.

Für alle Versicherungen, die an der Umfrage teilgenommen haben, trifft es vollständig oder teilweise zu, dass sich der Verwaltungsrat und die Geschäftsleitung:

- **den Mitarbeitenden gegenüber sichtbar entsprechend den von der Gesellschaft geforderten gemeinsamen Verhaltensnormen verhalten,**
- **zu einem gelebten Compliance Management System verpflichten, indem sie auch bei verlockenden Gewinnaussichten oder guten Ergebnissen unerwünschtes Verhalten nicht tolerieren und sanktionieren,**
- **sich für organisatorische Massnahmen einsetzen, welche die Unabhängigkeit der Compliance-Funktion sicherstellen,**
- **sich dafür einsetzen, dass der direkte Zugang der Compliance-Funktion zum Verwaltungsrat jederzeit und dauerhaft sichergestellt ist.**

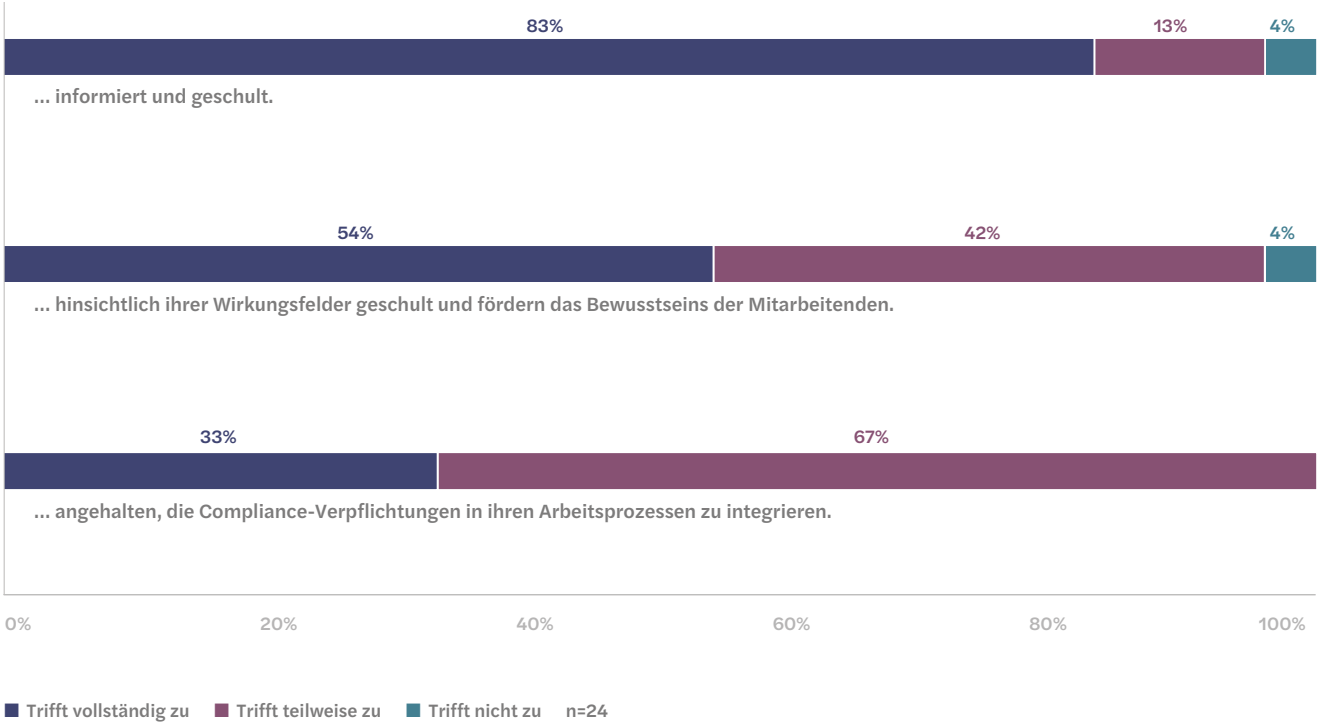
Die hohen Zustimmungswerte verdeutlichen die Bedeutung, welche die Verwaltungsräte und die Geschäftsleitungen der befragten Versicherungsunternehmen dem Thema Compliance beimessen. Nach Einschätzung der Compliance-Verantwortlichen trifft es für fast ausnahmslos alle befragten Versicherungsgesellschaften vollständig oder zumindest teilweise zu, dass Führungskräfte hinsichtlich Compliance informiert und geschult sind.

Richtet man das Augenmerk jedoch darauf, wie die Compliance-Verpflichtungen durch die Versicherungsgesellschaften operationalisiert und in die Prozesse überführt werden, ergab die Umfrage, dass insbesondere bei den Versicherungsgesellschaften der Aufsichtskategorien 3 und 4 mehrheitlich nicht oder nur teilweise festgelegt ist,

- **welche Überwachungsfunktionen durch die Compliance-Funktion überhaupt wahrzunehmen sind, und**
- **über welche organisatorischen Zugänge (Funktionen, Ebenen, Prozesse) die Compliance-Funktion verfügen muss, um ihre Aufgabe mit Bezug auf das Compliance Management System ausführen zu können.**

Weiter trifft für lediglich 33 % der befragten Compliance-Verantwortlichen für die Aufsichtskategorien 2, 3 und 4 vollständig zu, dass die direkten Vorgesetzten auch sicherstellen, dass die Compliance-Verpflichtungen des Unternehmens in den Prozessen integriert sind.

Betreffend Compliance sind die Führungskräfte ...



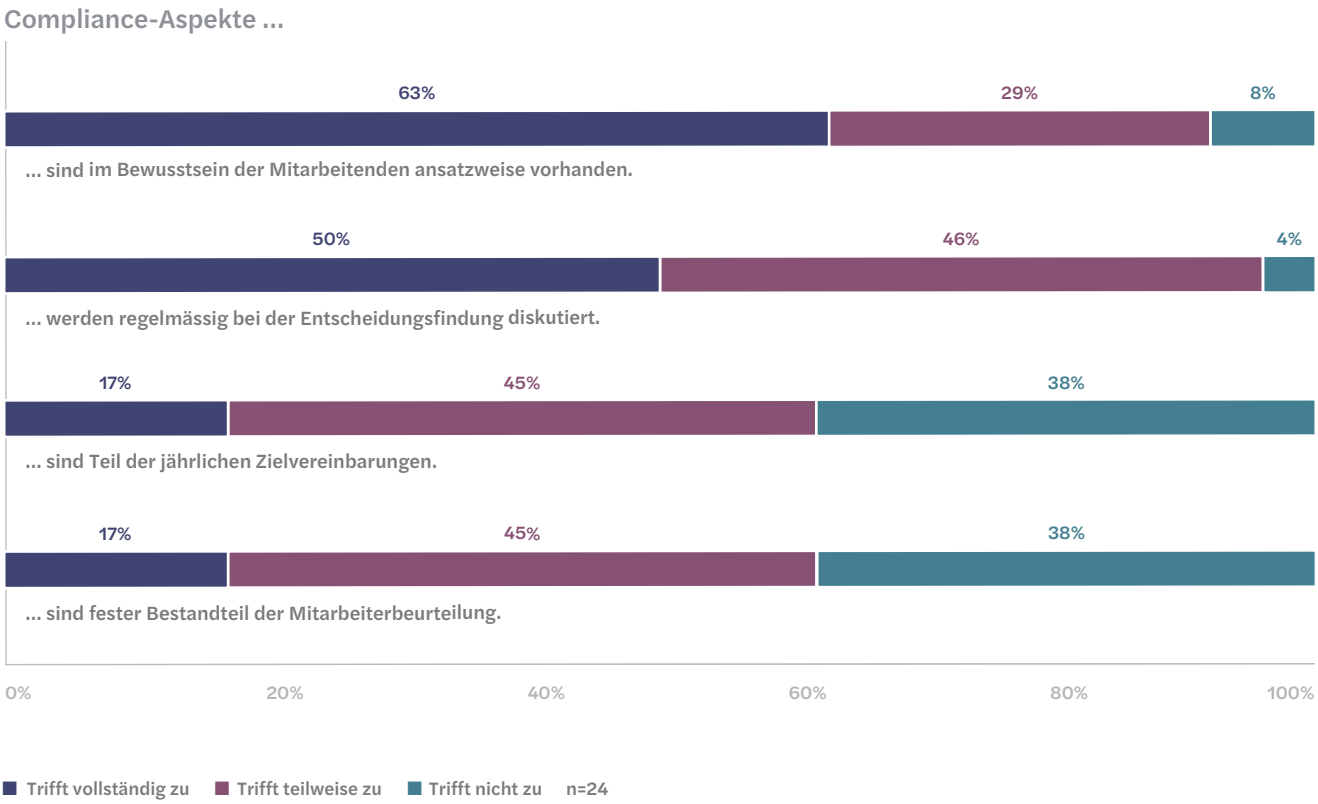
Verankerung von Compliance im Arbeitsalltag der Mitarbeitenden

Die befragten Versicherungsgesellschaften setzen die Instrumente der Zielvereinbarungen und -beurteilungen noch zurückhaltend zur Verankerung des Themas «Compliance» ein.

Für die überwiegende Mehrheit der befragten Compliance-Verantwortlichen trifft es vollständig oder zumindest teilweise zu, dass das Bewusstsein der Mitarbeitenden dem Thema «Compliance» gegenüber zumindest ansatzweise vorhanden ist.

Weiter trifft es aus der Sicht der Befragten vollständig oder teilweise zu, dass Compliance-Aspekte regelmässig bei Entscheidungsfindungen diskutiert werden. Weiter ist positiv, dass gemäss der Mehrheit ein Bewusstsein für die Thematik vorhanden ist.

Als weit weniger gegeben sehen Compliance-Verantwortliche, dass Compliance-Aspekte im Rahmen von Zielerreichungsgesprächen thematisiert werden. Der Aussage, dass Compliance fester Bestandteil der regelmässigen Mitarbeiterbeurteilung (...) ist, stimmen lediglich 17 % der Versicherungsgesellschaften vollständig zu. Für fast 40% der befragten Unternehmen trifft diese Aussagen nicht zu.



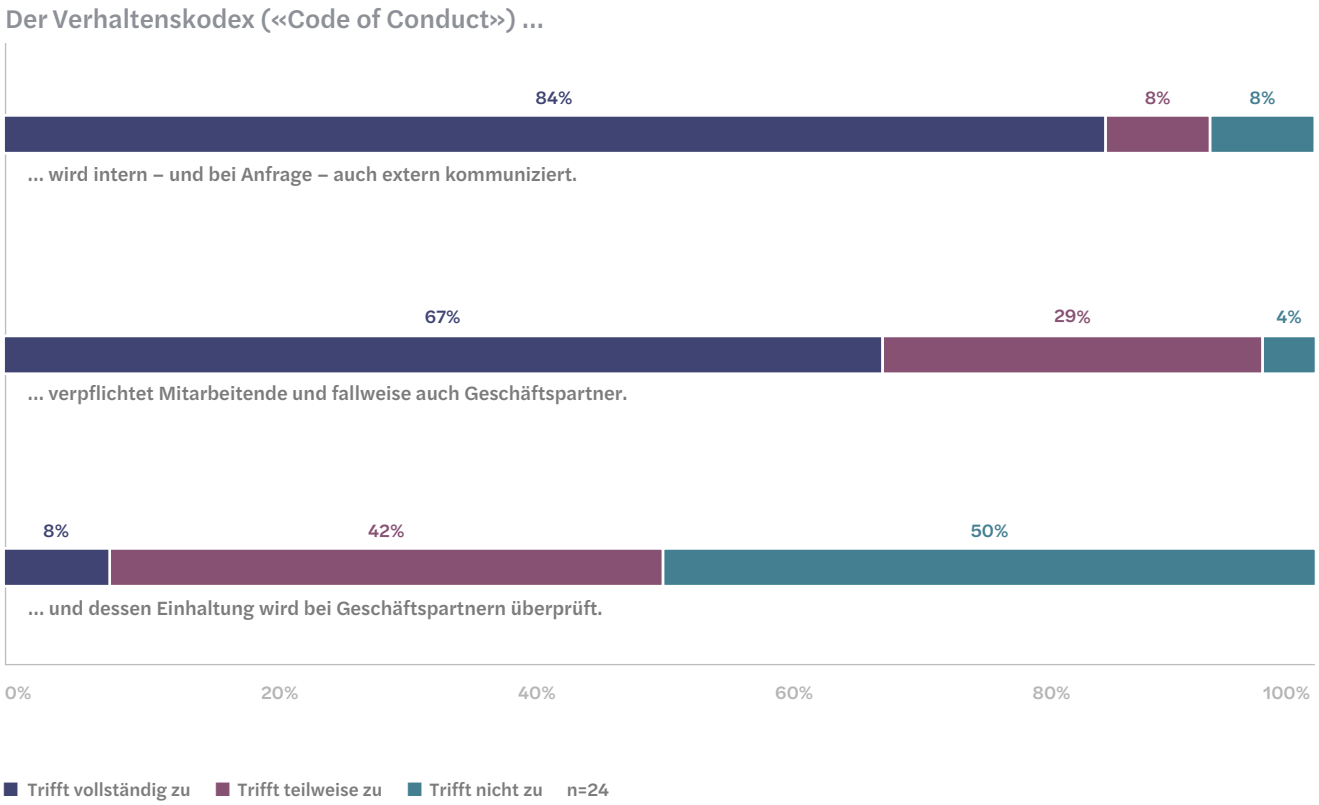
Kommunikation und Überprüfung des Verhaltenskodex bei wesentlichen Geschäftspartnern

Obwohl Versicherungsgesellschaften nicht nur ihre eigenen Mitarbeitenden, sondern auch externe Partner über ihren Verhaltenskodex («Code of Conduct») informieren, überprüft nur eine Minderheit der befragten Unternehmen dessen Einhaltung.

Die überwiegende Mehrheit der befragten Versicherungsgesellschaften stimmt vollständig oder zumindest teilweise zu, dass der unternehmenseigene Verhaltenskodex zusätzlich zu den eigenen Mitarbeitenden auf Anfrage hin auch externen Parteien gegenüber kommuniziert wird. Darüber hinaus bejahen die Teilnehmenden vollständig oder zumindest teilweise, dass der Verhaltenskodex nicht nur die eigenen Mitarbeitenden verpflichtet, die Compliance-Regeln des Unternehmens einzuhalten, sondern fallweise auch die Geschäftspartner.

Im Kontrast dazu stehen die Zustimmungswerte der befragten Versicherungsunternehmen zur Aussage, inwieweit die Einhaltung des Verhaltenskodex bei wichtigen Geschäftspartnern überprüft wird. 50 % der Gesellschaften antworteten zu dieser Aussage, dass die Einhaltung des Code of Conduct bei wesentlichen Geschäftspartnern nicht überprüft wird.

Insbesondere für Versicherungsgesellschaften der Aufsichtskategorien 2 und 4 trifft es nicht zu, dass der Verhaltenscodex Gegenstand von Prüfungen bei wesentlichen Geschäftspartnern ist.



Compliance-Risiken

Die teilnehmenden Versicherungsgesellschaften weisen ähnliche Risiko-Landschaften hinsichtlich Compliance auf. Die Bedeutung einzelner Compliance-Risiken hängt jedoch von der Grösse des Unternehmens ab.

Unabhängig der Grösse stufen die Versicherer folgende Risiken am bedeutendsten ein: Datenschutz, Cyber sowie Risiken im Zusammenhang mit der Informations- und Datensicherheit, Interessenkonflikte, Korruption und Bestechung sowie Risiken in Zusammenhang mit Drittparteien (inkl. Outsourcing). Die hohe Bedeutung des Compliance-Risikos mit Drittparteien steht in Kontrast zur Feststellung, wonach die Einhaltung des Verhaltenscodex bei wichtigen Geschäftspartnern nicht überprüft wird.

Compliance-Risiken hinsichtlich der Verletzung von Vorgaben bezüglich Insiderhandel und Geldwäscherei, Risiken im Zusammenhang mit grenzüberschreitenden Dienstleistungen sowie Risiken betreffend die Verletzung von Melde- und Überwachungspflichten (FATCA / AIA) kommen bei den Versicherungsgesellschaften der Aufsichtskategorie 4 gemäss den Ergebnissen der Umfrage eine eher tiefere Bedeutung zu.

Das «junge» aber bedeutende Compliance-Risiko ESG («Environmental, Social, and Governance») wurde gemäss der Umfrage insbesondere von den Versicherungsgesellschaften der Aufsichtskategorie 2 genannt. Bei den Gesellschaften der Aufsichtskategorie 3 und 4 scheint die Bedeutung dieses Compliance-Risikos derzeit noch tiefer.

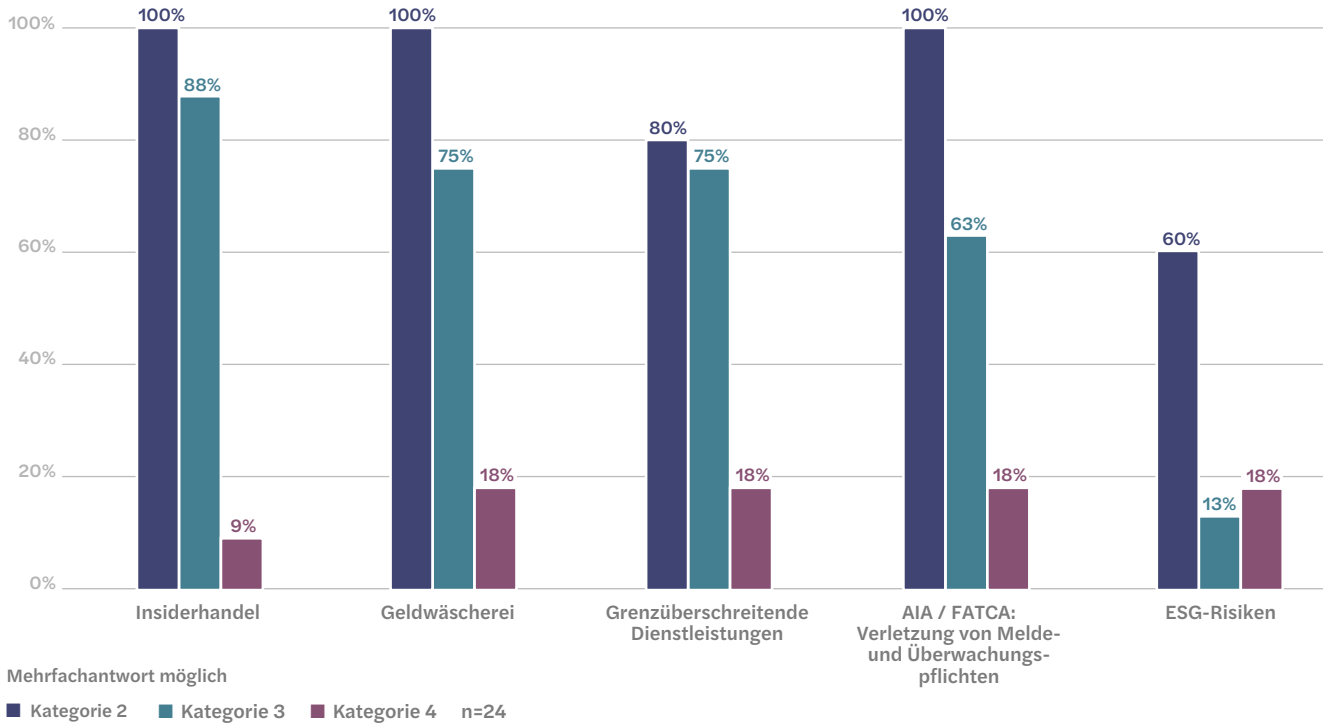
Als weitere Compliance-Risiken wurden von den befragten Unternehmen unter anderen Risiken im Zusammenhang mit dem Verhalten der Mitarbeitenden («Conduct Risk»), das Mithalten mit dem sich laufend und rasch verändernden regulatorischen Umfeld auf nationaler und internationaler Ebene als auch die Risiken im Zusammenhang mit der Aktenaufbewahrung genannt.

Für die Mehrheit der befragten Versicherungsgesellschaften trifft es vollständig zu, dass die Eigner der Compliance-Risiken in den operativ tätigen Fachbereichen («1st Line of Defense») angesiedelt sind. Dies trifft insbesondere für die Versicherer der Aufsichtskategorie 3 zu, weniger jedoch für die Gesellschaften der Aufsichtskategorien 2 und 4.

Dass die Massnahmen zur Adressierung der Compliance-Risiken einheitlich dokumentiert sind, trifft für mehr als die Hälfte der Teilnehmenden nur teilweise oder nicht zu.

Weiter trifft es für knapp 70 % der befragten Compliance-Verantwortlichen nicht oder nur teilweise zu, dass die Effektivität der risikominimierenden Massnahmen im Rahmen des Compliance-Monitorings konsequent erhoben und laufend gemessen werden.

Compliance-Risiken



Abgrenzung von Compliance- zu anderen Unternehmensrisiken

Richtet man den Blick etwas über den Tellerrand der üblicherweise genannten Compliance-Risiken hin zu weiteren Themenfeldern, mit denen ebenfalls umfangreiche gesetzliche, regulatorische und teilweise komplexe Anforderungen und Vorgaben einhergehen, ist zu erkennen, dass diese weit weniger als Compliance-Risiken definiert sind.

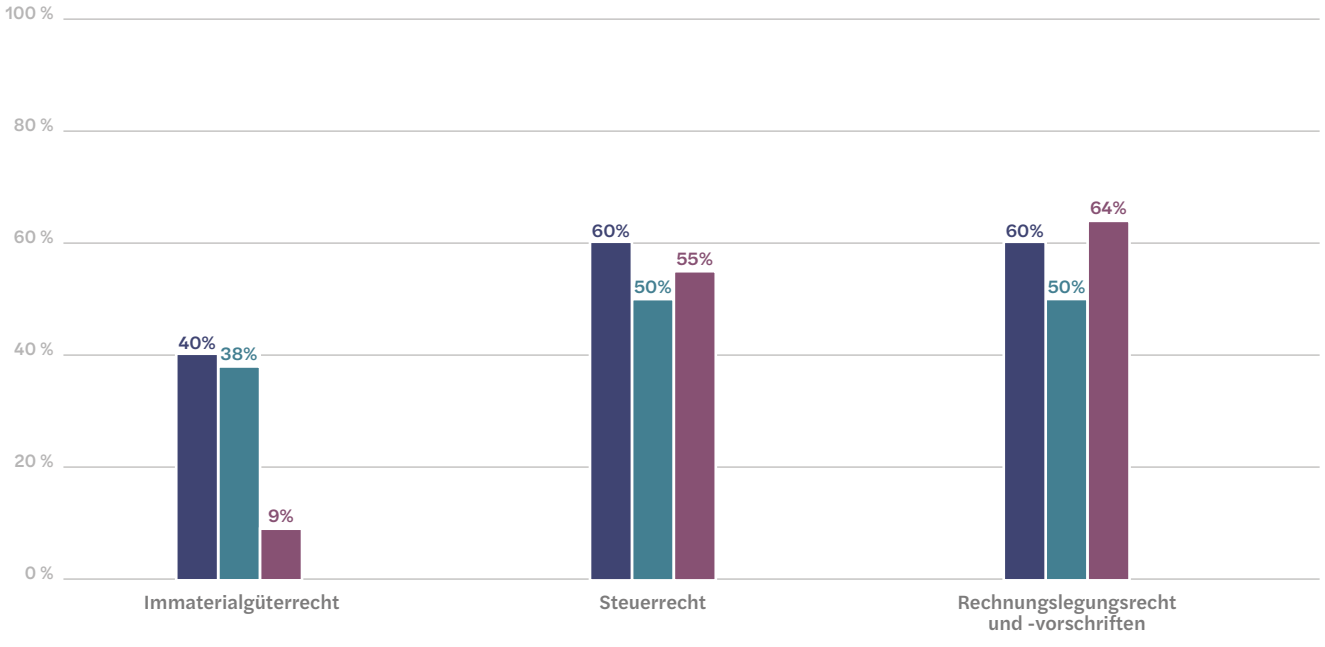
Zu den weiteren wesentlichen Themengebieten gehören die Rechnungslegungsvorschriften, das Steuerrecht, sowie das Immaterialgüterrecht. Knapp etwas mehr als 50 % der befragten Versicherungsunternehmen haben diese Themen als Compliance-Risiken definiert. Unterschiede nach Grösse der Unternehmen sind dabei nicht zu erkennen.

Eine bedeutend geringere Rolle spielt das Kartell- und Wettbewerbsrecht bei den befragten Versicherungsgesellschaften der Aufsichtskategorie 4 im Vergleich zu den Versicherern der Aufsichtskategorien 2 und 3.

Als weitere Themengebiete mit Risikopotential nannten die Befragten unter anderem das Beschwerdemanagement, die Versicherungslizenz-Bestimmungen, die Corporate Governance, die Produktentwicklung sowie den Bereich «Claims & Payouts».

Die Beispiele betreffend Rechnungslegungsvorschriften oder Steuerrecht zeigen eine weitere wesentliche, in der Praxis bisher kaum abschliessend beantwortete Frage im Zusammenhang mit Compliance-Risiken im Allgemeinen auf: Wer im Unternehmen entscheidet (letztendlich) darüber, welche Themenfelder als Compliance-Risiko festgelegt werden? Für jeden Themenbereich, mit welchem gesetzliche, regulatorische, berufsständische oder selbst auferlegte Vorgaben und Anforderungen einhergehen, besteht letztlich das Risiko von Regelverletzungen.

Weitere Compliance-Risiken



Mehrfachantwort möglich

Kategorie 2 Kategorie 3 Kategorie 4 n=24

Einen regelmässigen Austausch zwischen der Compliance-Funktion und anderen Kontrollfunktionen («Assurance Provider») pflegen vor allem Versicherungsunternehmen der Kategorien 2 und 3.

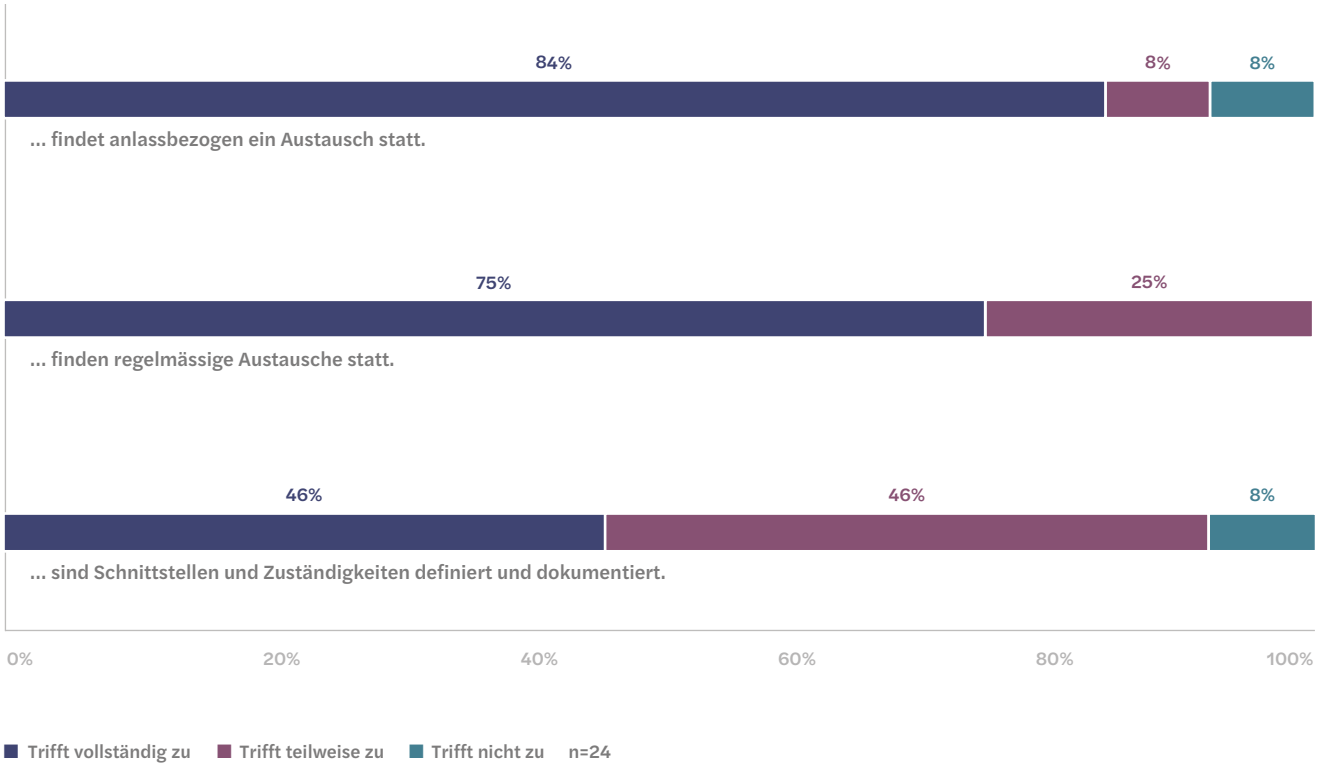
Bei der überwiegenden Mehrheit der befragten Versicherungsgesellschaften trifft es vollständig oder zumindest teilweise zu, dass ein anlassbezogener oder regelmässiger Austausch zwischen der Compliance-Funktion und anderen Kontrollfunktionen stattfindet.

Durch den Austausch zwischen den «Assurance Providern» wird das gegenseitige Verständnis der Tätigkeiten und Aufgaben der jeweiligen Kontrollfunktion gefördert. Dies bildet die Grundlage, wenn es darum geht, in einem weiteren Schritt die Schnittstellen und Zuständigkeiten innerhalb der Gruppe der «Assurance Provider» festzulegen und zu definieren.

Diesbezüglich hat die Umfrage bei den Versicherungsgesellschaften gezeigt, dass sich die Kontrollfunktionen bei nur knapp der Hälfte der Unternehmen gezielt abstimmen und dabei die Schnittstellen und Zuständigkeiten definieren. Für 17 % trifft dies vollständig zu, für 29 % zumindest teilweise, bei 54 % ist dies nicht der Fall.

Ein gezieltes Abstimmen der Schnittstellen und Zuständigkeiten verhindert, dass es zu Überlappungen oder gar ungenügend abgedeckten Risikoexpositionen kommt.

Zwischen Compliance und anderen Kontrollfunktionen ...



Berichterstattung und Tätigkeitsbereich der Compliance-Funktion

Die Betreuung und kontinuierliche Weiterentwicklung des Compliance Management Systems ist Kernaufgabe der Compliance-Funktion. Darüber hinaus werden diverse weitere Aufgaben wahrgenommen. Mehrheitlich berichten die befragten Compliance-Verantwortlichen direkt an den Verwaltungsrat oder alternativ an die/den Chief Executive Officer (CEO) oder General Counsel (GC).

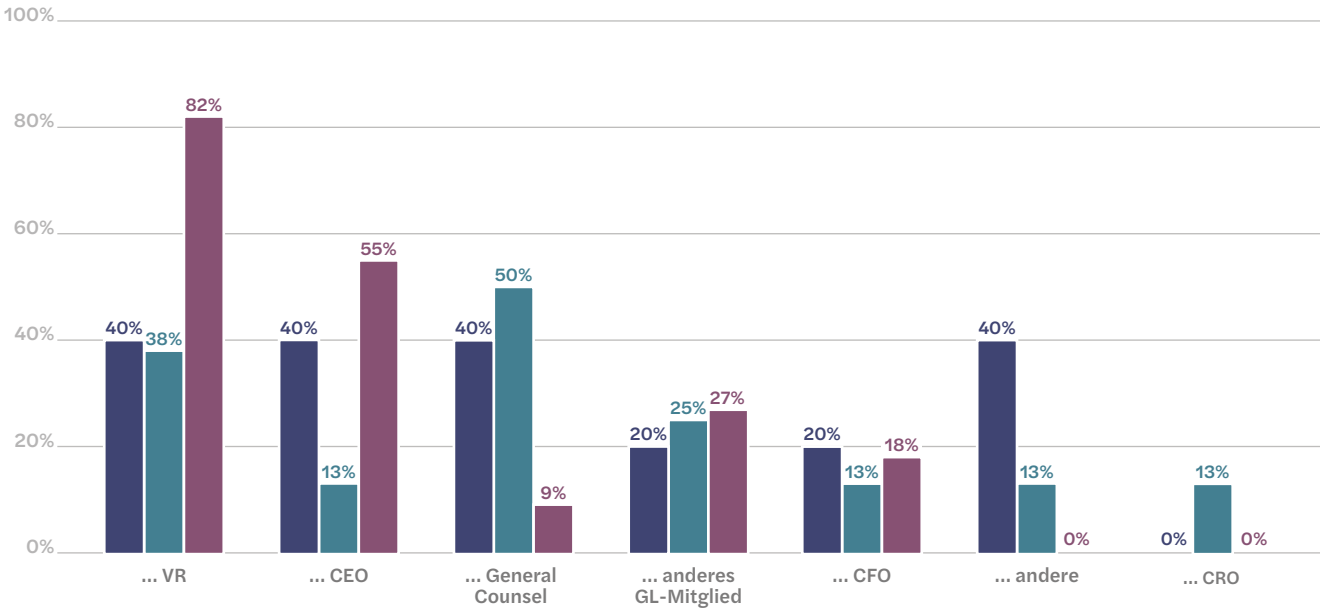
Allerdings wurden Chief Executive Officer (CEO) von Unternehmen der Aufsichtskategorie 3 weniger genannt, demgegenüber ist für die Aufsichtskategorie 4 eine Berichterstattung an den/die General Counsel (GC) weniger häufig.

Vergleichsweise wenig Compliance-Verantwortliche berichten an ein anderes Mitglied der Geschäftsleitung oder an die/den Chief Financial Officer (CFO). Auch selten kommt gemäss den Umfrageergebnissen die Berichterstattung an die/den Chief Risk Officer (CRO) vor.

Hinsichtlich der Frage, welche weiteren Tätigkeiten von der Compliance-Funktion zusätzlich zu ihrer Kernaufgabe, der Betreuung und kontinuierlichen Weiterentwicklung des Compliance Management Systems, wahrgenommen werden, antworteten die befragten Versicherungsgesellschaften, unabhängig ihrer Aufsichtskategorie:

- Beratungen der «1st Line of Defense»
- Fachliche Begleitung von unternehmensinternen Projekten (bspw. Einführung neuer Prozesse)
- Betreuung und Unterhalt des Weisungswesens sowie das Erstellen von Vorgaben (inkl. Verhaltenscodex)
- Compliance-Schulungen
- Betreuung und Unterhalt des Hinweisgebersystems
- Ausübung der Funktion der Datenschutzbeauftragten und des Datenschutzbeauftragten (DPO)
- Durchführung und Überwachung von internen Untersuchungen
- Laufende Überwachung der relevanten Rechtsentwicklung
- Durchführung von Wirksamkeitsprüfungen
- Führen der GwG-Fachstelle

Die Compliance-Funktion berichtet an ...



Mehrfachantwort möglich

Kategorie 2 Kategorie 3 Kategorie 4 n=24

Die Compliance-Teams der befragten Versicherungsgesellschaften verfügen mehrheitlich über juristische Kenntnisse und weniger über Erfahrungen und Kenntnisse im Bereich von Data & Analytics oder gar der künstlichen Intelligenz.

Für die Mehrheit der befragten Versicherungsgesellschaften trifft es vollständig oder teilweise zu, dass die Compliance-Teams zur Mehrheit über juristische Kenntnisse verfügen und sich demzufolge hauptsächlich auf die rechtlichen und regulatorischen Aspekte der Aufgaben einer Compliance-Funktion fokussieren.

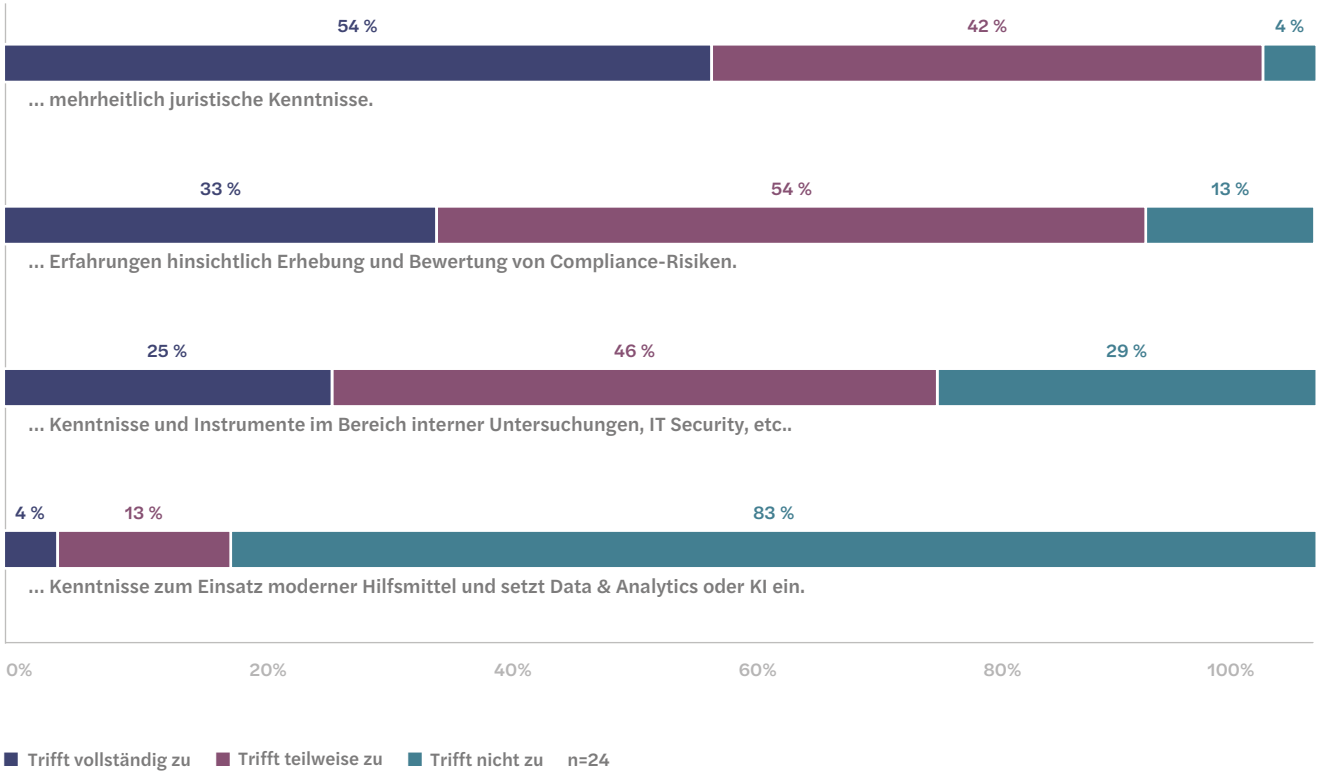
Weiter trifft es vollständig oder teilweise zu, dass die Compliance-Teams auch über Erfahrungen mit dem Erheben und Bewerten von Compliance-Risiken (bspw. auch auf Ebene der Geschäftsprozesse) verfügen und innerhalb der Compliance-Funktion auch auf eigene Fähigkeiten zurückgreifen können, um Stichproben zur Messung der Wirksamkeit von Massnahmen und Kontrollen durchführen zu können.

Weniger Erfahrungen oder Instrumente stehen den Compliance-Funktionen jedoch im Bereich von internen Untersuchungen, IT-Sicherheit, etc. zur Verfügung.

Nur wenige Befragte setzen darüber hinaus Instrumente wie bspw. Data & Analytics oder künstliche Intelligenz (KI) zur Unterstützung ihrer Tätigkeiten ein.

Es ist davon auszugehen, dass sowohl Data & Analytics als auch die künstliche Intelligenz in der Zukunft im Bereich der Compliance eine zunehmend bedeutendere Rolle spielen werden, insbesondere wenn es darum geht, systembasierte Überwachungsinstrumente aufzubauen und zu betreiben, die es erlauben, die Einhaltung der Compliance-Vorgaben und -Weisungen laufend, quasi in Echtzeit, zu überprüfen.

Das Compliance-Team verfügt über ...



Key Performance Indicators («KPI») zur Messung der Compliance-Leistung

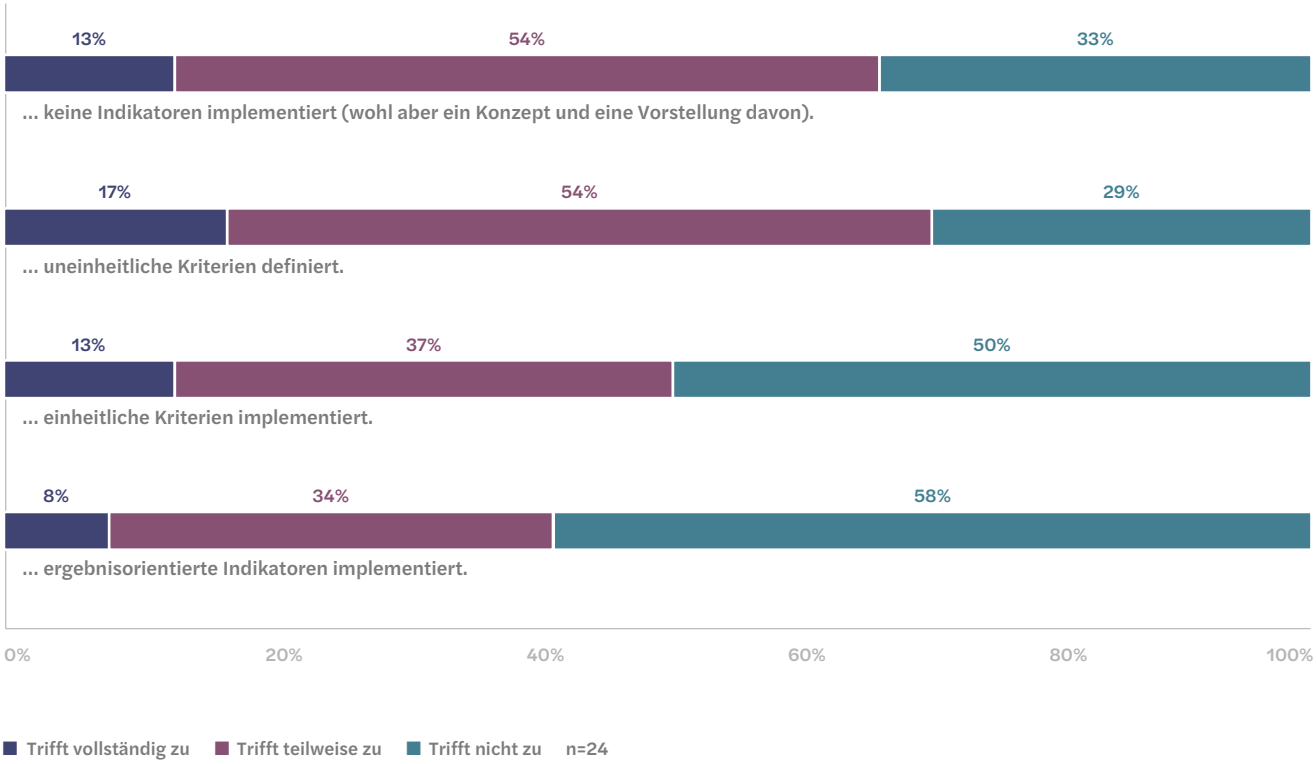
Der Einsatz von konkreten «Key Performance Indicators» zur Messung der Effektivität der Compliance-Massnahmen ist bei den befragten Versicherungsgesellschaften noch wenig verbreitet.

Die Mehrheit der teilnehmenden Gesellschaften hat noch keine oder uneinheitliche Kriterien zur Messung der Compliance-Leistungen definiert. Auch trifft es nur auf eine Minderheit vollständig zu, dass ein Konzept und eine Vorstellung davon vorhanden ist, anhand welcher betriebsspezifischer Indikatoren die Effektivität der Compliance-Massnahmen gemessen werden könnte.

Nur gerade 8% der befragten Versicherungsgesellschaften hat ergebnisorientierte Indikatoren implementiert, bei einem Drittel der Befragten ist dies zumindest teilweise der Fall.

Zu derartigen ergebnisorientierten Indikatoren gehören bspw., ob dank eines Meldekanals Fälle von «non compliance» tendenziell früher aufgedeckt und dadurch Kosten verhindert werden können oder ob die Compliance-Massnahmen dazu führen, dass die Anzahl Konsultationen der Compliance-Funktion laufend zunehmen.

Zur Messung der Compliance-Leistung hat unser Unternehmen ...



Ausgestaltung der Meldestelle («Whistleblowing»)

Das Instrument des E-Mails ist bei den befragten Versicherungsgesellschaften nach wie vor stark als Meldekanal verbreitet.

Das E-Mail, der persönliche Besuch aber auch das Telefon sind bei den befragten Versicherungsgesellschaften die immer noch am weitesten verbreiteten Meldekanäle.

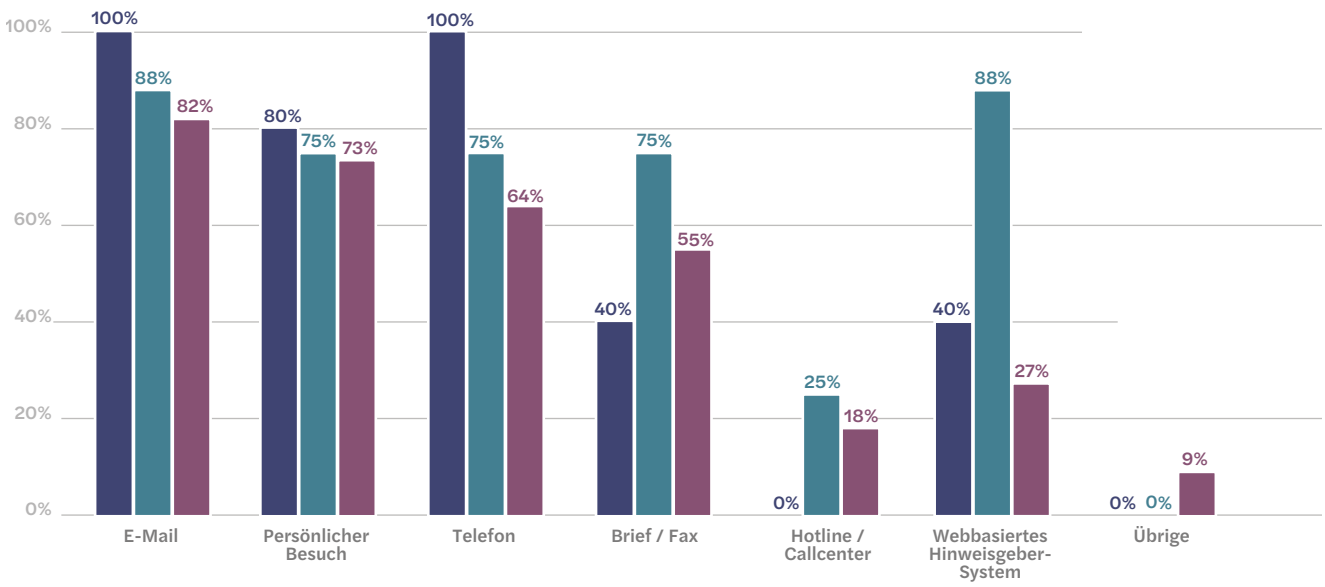
Modernere, d.h. webbasierte Hinweisgeber-Systeme, sind ausser bei Versicherungsgesellschaften der Aufsichtskategorie 3, laut den Ergebnissen der Umfrage noch eher wenig vertreten.

(Noch) gar keine Rolle spielen bei den befragten Versicherungsgesellschaften bspw. Mobile Apps oder Social-Media-Kanäle.

Es kann nur darüber gemutmasst werden, ob auch die in der heutigen Praxis vorherrschend anzutreffenden Formen der Ausgestaltung des Meldekanals, namentlich E-Mails, persönlicher Besuch oder Meldung via Telefon, einen Einfluss auf die (tiefe) Anzahl der eingehenden Meldungen hat.

Es ist anzunehmen, dass Mitarbeitende aus Furcht vor negativen Konsequenzen bei einer Meldung eher die Anonymität suchen. Diesen Schutz bieten die derzeit am weitesten verbreiteten Instrumente allerdings nicht. Dies könnte mitunter ein Grund sein, weshalb Mitarbeitende davon absehen, eine Meldung zu erstatten.

Meldekanäle



Mehrfachantwort möglich

Kategorie 2 Kategorie 3 Kategorie 4 n=24

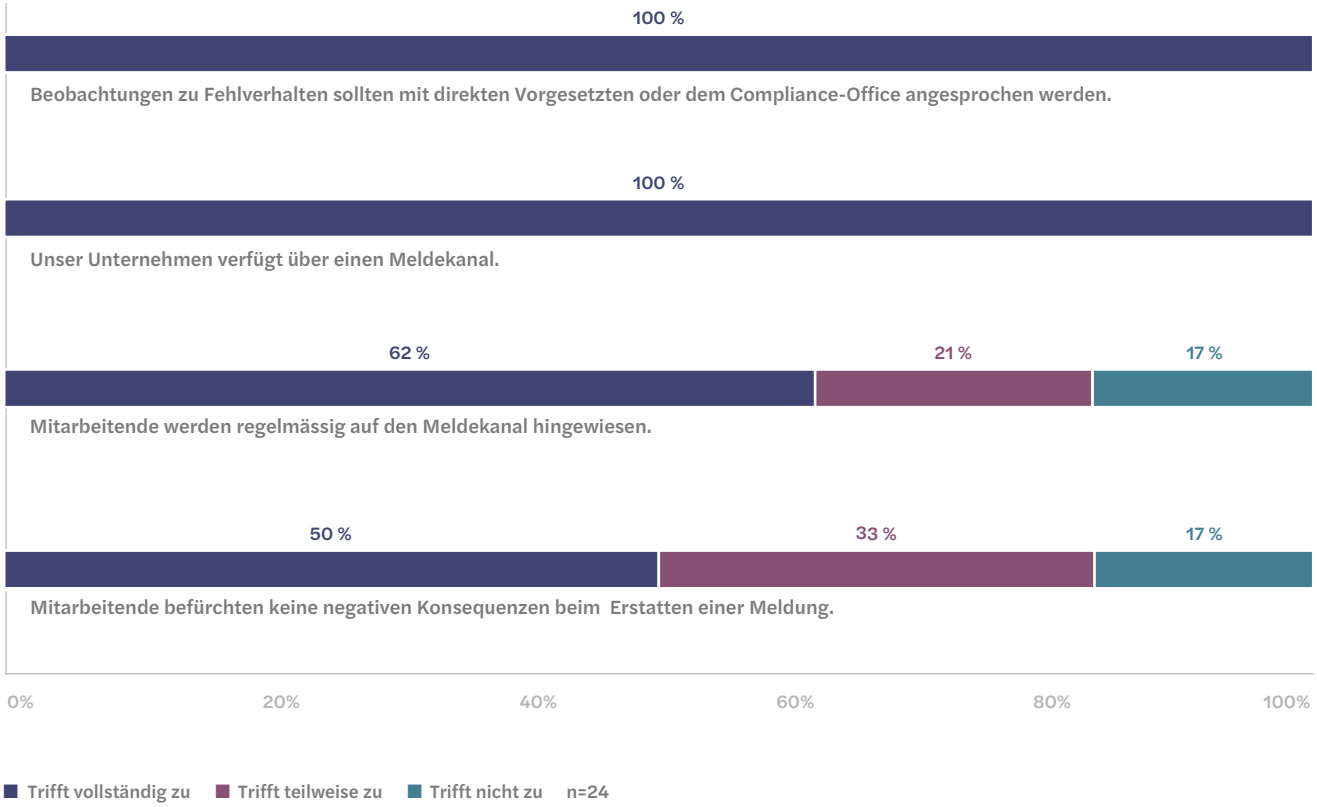
Nutzung des Meldekanals

Die Mitarbeitenden der befragten Versicherungsgesellschaften sind erwartungsgemäss angehalten, Beobachtungen zu Fehlverhalten zu melden. Allerdings gehen die Compliance-Verantwortlichen davon aus, dass Mitarbeitende negative Konsequenzen fürchten könnten.

Alle an der Umfrage teilnehmenden Versicherungsgesellschaften bestätigten, über einen für alle Mitarbeitenden erreich- und kontaktierbaren Meldekanal zu verfügen, über den Beobachtungen zu möglichem Fehlverhalten gemeldet werden können («Whistleblowing»).

Ebenfalls bestätigten alle befragten Versicherungsunternehmen, dass sie ihre Mitarbeitenden dazu anhalten, Beobachtungen zu möglichem Fehlverhalten in einem ersten Schritt mit direkten Vorgesetzten oder mit dem Compliance-Office anzusprechen. Allerdings geben 17 % der an der Umfrage teilnehmenden Gesellschaften an, dass die Mitarbeitenden nicht regelmässig auf das «Whistleblowing» hingewiesen werden.

Dass die Mitarbeitenden aufgrund vergangener Vorfälle davon ausgehen können, dass eine Hinweisgeberin oder ein Hinweisgeber beim Erstatten einer gerechtfertigten Meldung keine negativen Konsequenzen zu befürchten hat (bspw. Entlassung, «shaming and blaming», Ausgrenzung aus dem Team, etc.) sehen die Befragten kritischer. Diese Aussage trifft für 50 % vollständig und für 33 % teilweise zu. Für 17 % trifft diese Aussage nicht zu.



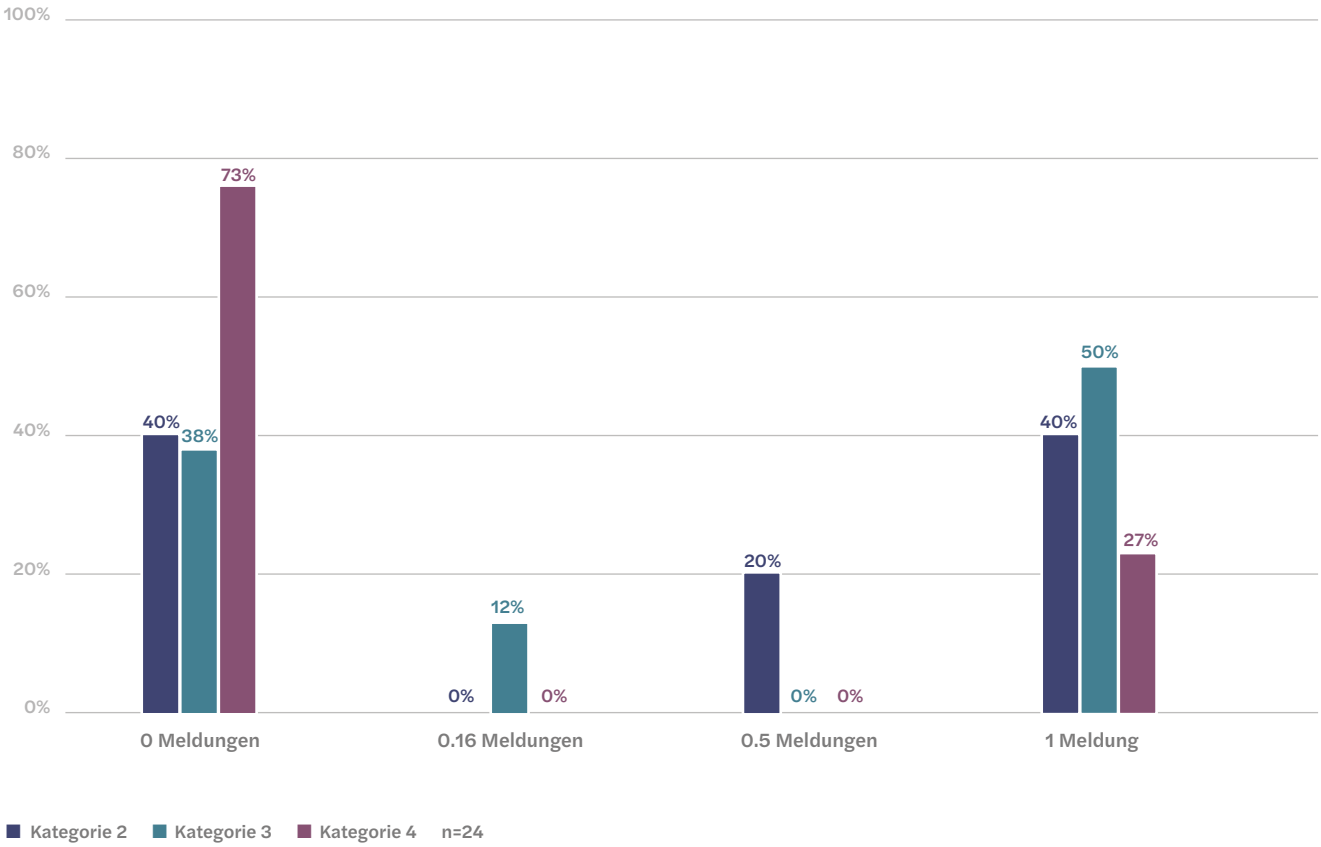
Anzahl Meldungen pro 100 Mitarbeitende

Im Geschäftsjahr 2020 gingen bei 38 % der befragten Gesellschaften rund eine Meldung eines Hinweisgebers pro 100 Mitarbeitende ein.

Bei der Mehrheit der befragten Versicherungsgesellschaften gingen im Verlauf des Jahres 2020 entweder keine Hinweise oder eine Meldung pro 100 Mitarbeitende ein.

Während dem das Bild der Versicherungsgesellschaften der Aufsichtskategorien 2 und 3 ausgeglichen scheint, zeigen sich grössere Abweichungen insbesondere bei den Unternehmen der Aufsichtskategorie 4. Bei 73% der Gesellschaften dieser Aufsichtskategorie gingen im Verlauf des Jahres 2020 keine Hinweise ein.

Diese Werte bei den befragten Versicherungsgesellschaften sind vergleichbar mit Werten aus anderen Umfragen betreffend Hinweisgeber-Systemen in der Schweiz. So berichtet bspw. der «Whistleblowing Report 2021», der die Firma EQS in Zusammenarbeit mit der Fachhochschule Graubünden, herausgab, dass in der Schweiz im Jahr 2020 bei 54 % der befragten Unternehmen unabhängig ihrer Industrie keine Meldungen von Hinweisgebern eingingen.



Befolgte Regelwerke zum Auf- und weiteren Ausbau der Compliance Management Systeme

Die befragten Versicherungsgesellschaften orientieren sich an unterschiedlichen Standards. Wesentlich für die Versicherungsgesellschaften sind aber insbesondere die einschlägigen Vorgaben der FINMA.

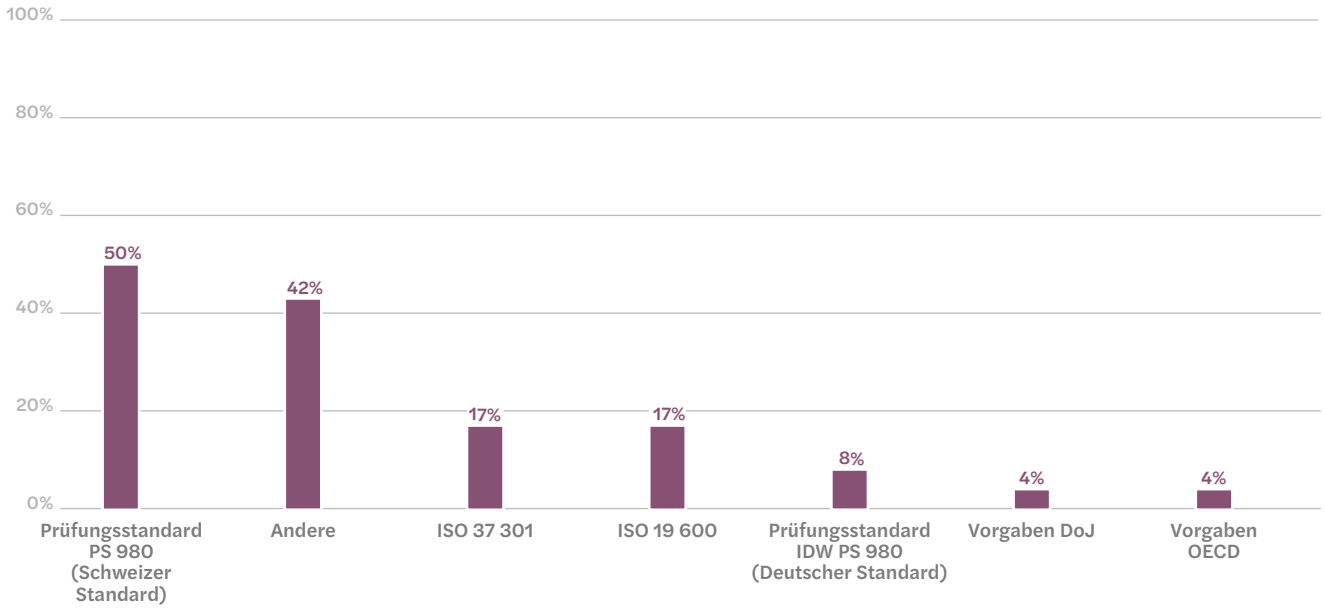
Der Schweizer Prüfungsstandard (PS) 980, «Grundsätze zur Prüfung von Compliance Management Systemen», der sich – mit einigen wenigen Ausnahmen – an dem seit 2013 in Kraft stehenden deutschen Prüfungsstandard IDW PS 980 orientiert, ist bei der Mehrheit der befragten Versicherungsgesellschaften ein wichtiges Regel- und Referenzwerk zum Auf- und weiteren Ausbau ihrer Compliance Management Systeme.

Der erst seit Frühsommer 2021 in Kraft getretene Zertifizierungsstandard ISO Standard 37 301, «Compliance Management Systeme», spielt im Vergleich zum Schweizer Prüfungsstandard (PS) 980 bei den befragen Versicherungsgesellschaften derzeit noch eine untergeordnete Rolle.

Es ist aber davon auszugehen, dass der noch sehr «junge» ISO Standard 37 301 in Zukunft an Verbreitung und demzufolge auch an Bedeutung gewinnen wird.

Ausländisch geprägte Regelwerke wie die «Hallmarks of an Effective Compliance Management System» oder die «Leitlinien für empfehlenswerte Verfahrensweisen in den Bereichen interne Kontrollsysteme, Ethik und Compliance» der OECD spielen bei den befragten Versicherungsgesellschaften eine untergeordnete Rolle.

Vereinzelt wurde von den Versicherungsgesellschaften auch auf den «Swiss Code of Best Practice for Corporate Governance / Grundzüge eines wirksamen Compliance Management Systems» verwiesen.



Mehrfachantwort möglich
n=24

Auswertung gesamt

Die einzelnen Aussagen der teilnehmenden Versicherungsgesellschaften wurden zum Zweck der Konsolidierung der Ergebnisse einer der folgenden Kategorien zugewiesen:

Verpflichtung

Schulung, Awareness, Interaktion

Vorgaben

Leistungsbeurteilung

Risikobeurteilung

Prozesse und Instrumente

Die Gesamtauswertung über alle teilnehmenden Versicherungsgesellschaften hinweg zeigt auf, dass die Maturität der Compliance Management Systeme im Urteil der Compliance-Verantwortlichen hinsichtlich der Aussagen zu Verpflichtung sowie Prozesse und Instrumente jeweils erfreulich hohe Reifegrade aufweisen.

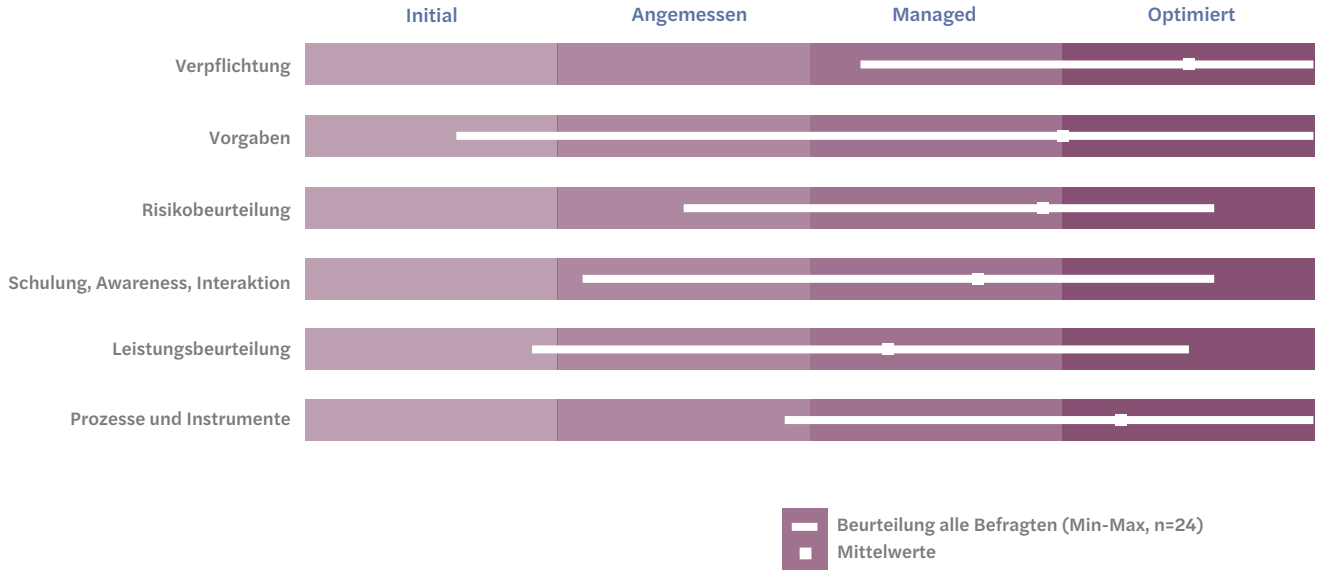
Der Mittelwert zu diesen zwei Aussagekategorien liegt nach Einschätzung der Compliance-Verantwortlichen beim Maturitätslevel optimiert, wobei zwischen den an der Umfrage teilnehmenden Krankenversicherern einerseits und den Lebens-/Sachversicherern andererseits keine grösseren Abweichungen in der Selbstbeurteilung zu beobachten sind.

Etwas weniger hoch schätzen die Compliance-Verantwortlichen die Maturität in den Aussagekategorien Risikobeurteilung und Schulung, Awareness, Interaktion sowie Leistungsbeurteilung ein. Für diese drei Aussagekategorien sind zwischen den Geschäftsfeldern der Krankenversicherer und der Lebens-/Sachversicherer jeweils auch etwas grössere Abweichungen hinsichtlich der Mittelwerte feststellbar. Die Umfrageergebnisse legen nahe, dass die Compliance Management Systeme bei den Lebens-/Sachversicherern für diese drei Aussagekategorien einen etwas höheren Maturitätslevel aufweisen als diejenigen bei den Krankenversicherern.

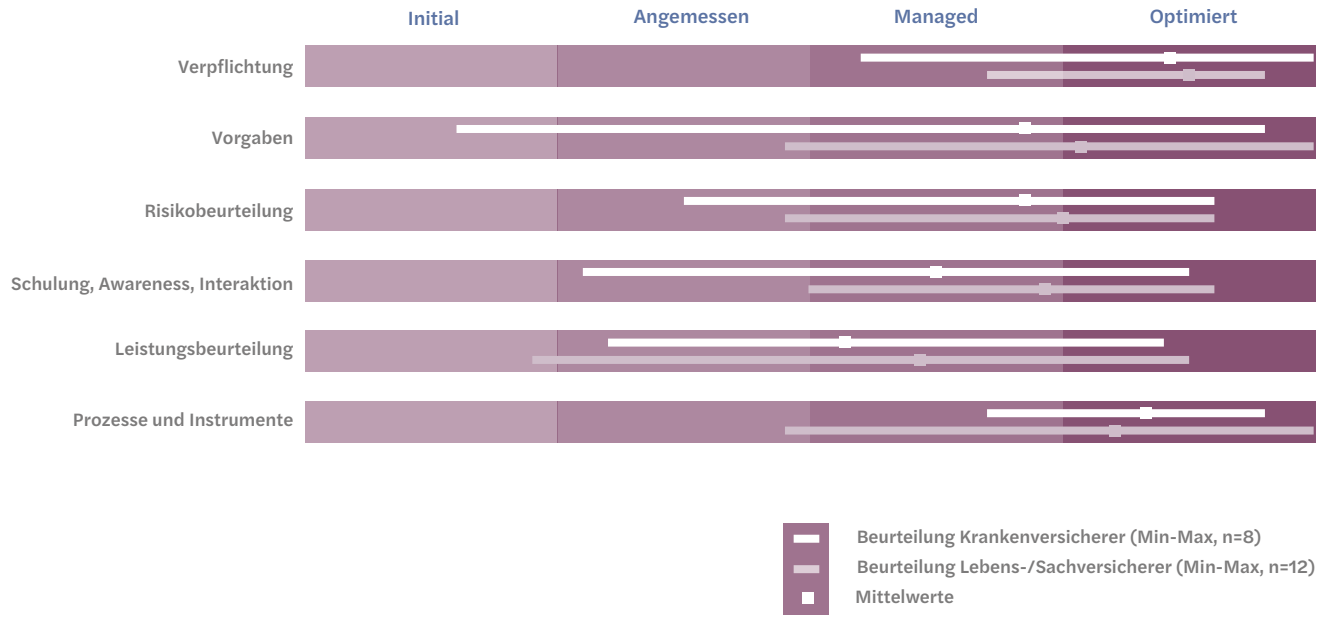
Die Resultate der Befragung zeigen zudem auf, dass bezüglich Prozesse, Instrumente und Praktiken der Leistungsbeurteilung das grösste Entwicklungspotential besteht.

Die grössten Unterschiede hinsichtlich der Maturität der Compliance Management Systeme der befragten Versicherungsgesellschaften ist bei den Aussagen zu den Vorgaben festzustellen. Hier reichen die Maturitätsstufen im Urteil der Compliance-Verantwortlichen von initial bis hin zu optimiert.

Auswertung alle Befragten



Auswertung alle Befragten nach Geschäftsfeld



Anhang

Verpflichtung

Ausmass der Verpflichtung wie das Thema Compliance von der Geschäftsleitung und den Kadern vorgelebt und unterstützt wird.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Verpflichtung zur Compliance	VR und GL reagierten wahrnehmbar auf Compliance-Vorfälle.	•			
	VR und GL haben umfassende Vorgaben und Richtlinien zum Compliance Management System erlassen.	•	•		
	VR und GL stellen ausreichend Ressourcen (Verfahren, Prozesse, Personal) zur Verfügung, damit die Compliance-Ziele erreicht werden können.	•	•	•	
Compliance-Kultur	VR und GL verhalten sich für die Mitarbeitenden sichtbar entsprechend den von ihnen geforderten gemeinsamen Verhaltensnormen.	•	•	•	
	VR und GL beweisen ihre Verpflichtung zu einem gelebten Compliance Management System, indem sie (auch bei verlockenden Gewinnaussichten oder guten Resultaten) unerwünschtes Verhalten nicht tolerieren und für alle Stufen konsequent sanktionieren.	•	•	•	•
Compliance-Führung	Organisatorische Massnahmen zur Sicherstellung der Unabhängigkeit der Compliance-Funktion sind definiert.	•	•		
	Der direkte Zugang der Compliance-Funktion zum VR ist jederzeit und dauerhaft sichergestellt.	•	•	•	
Compliance-Politik	Es besteht eine schriftlich dokumentierte, übergeordnete Compliance-Politik (inkl. der damit zusammenhängenden internen Weisungen und Richtlinien, dem sogenannten «House of Policies»).	•			
	Die Compliance-Politik ist mit den Werten, den Zielen und der Strategie der Organisation abgestimmt.	•	•		
	Die Compliance-Politik fordert explizit die Konformität mit den Compliance-Verpflichtungen. Zu solchen Compliance-Verpflichtungen gehören auch selbstauferlegte Compliance-Verpflichtungen (wie bspw. die Einhaltung von Umweltstandards wie CO_2-Ausstoss o.ä.).	•	•	•	
Compliance-Funktion	Die Aufgaben und Verantwortlichkeiten der Compliance-Funktion mit Bezug auf das Compliance Management System sind definiert und dokumentiert.	•	•		
	Es ist festgelegt, welche Überwachungsfunktionen durch die Compliance-Funktion wahrzunehmen sind und über welche organisatorischen Zugänge (Funktionen, Ebenen, Prozesse) die Compliance-Funktion verfügen muss, um ihre Aufgabe mit Bezug auf das Compliance Management System ausführen zu können.	•	•	•	
Verantwortlich-keiten direkte Vorgesetzte	Die Führungskräfte sind über Compliance informiert und geschult.	•	•		
	Die Führungskräfte sind bezüglich der spezifischen Compliance-Themen in ihren jeweiligen Wirkungsfeldern informiert, geschult und zur Förderung des Bewusstseins des Personals (Schulungen, Kompetenzen) für Compliance-Verpflichtungen und -Anweisungen angehalten.	•	•	•	
	Die Führungskräfte stellen sicher, dass die Compliance-Verpflichtungen in den Prozessen integriert und durch die Mitarbeitenden erfüllt werden (z.B. durch Prozess-Überprüfungen und File Reviews).	•	•	•	•

Risikopolitik

Bewertung, wie das Risikomanagement im Unternehmen verankert ist.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Umgang mit Compliance-Risiken	Massnahmen zur Adressierung der einzelnen Compliance-Risiken sind vereinzelt festgehalten.	•			
	Massnahmen zur Adressierung der einzelnen Compliance-Risiken sind einheitlich dokumentiert.	•	•		
	Die Massnahmen umfassen auch spezifische risikomindernde Massnahmen wie bspw. prozessbasierte Schlüsselkontrollen, spezifische Weisungen, adressatengerechte Schulungen, automatisiertes Monitoring, etc.	•	•	•	
	Die Effektivität der risikominimierenden Massnahmen werden im Rahmen des Compliance-Monitorings konsequent erhoben und laufend gemessen.	•	•	•	•
Verständlichkeit der Compliance-Politik	Unsere Compliance-Politik ist für die Mitarbeitenden leicht zu verstehen und nachvollziehbar.	•	•		
	Unsere Compliance-Politik ist auch für einen (externen) Dritten leicht zu verstehen und nachvollziehbar.	•	•	•	
Kommunikation der Compliance-Politik	Mitarbeitende wurden im Rahmen einer Kommunikationsmassnahme gezielt betreffend der Compliance-Politik informiert.	•			
	Mitarbeitende wissen, wo die dokumentierte Compliance-Politik zu finden ist und haben leichten Zugang dazu (bspw. Intranet).	•	•		
	Relevante Änderungen in der Compliance-Politik werden zeitnah im Unternehmen kommuniziert.	•	•	•	
	Im Rahmen von Schulungen werden Mitarbeitende zielgruppengerecht hinsichtlich der Compliance-Politik sensibilisiert.	•	•	•	•

Risikobeurteilung

Vorgehen zur Erhebung sowie Identifikation und Bewertung von Compliance-Risiken.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Verstehen der Organisation und Ihres Kontextes	Relevante interne und externe Themen, die sich auf das Compliance Management System insgesamt auswirken, sind bestimmt.	•	•		
	Der Einfluss von relevanten internen und externen Aspekten auf das Compliance Management System, wie bspw. Veränderung der Gesellschaft, Änderungen im Verhalten der Kunden, etc., wird mindestens einmal jährlich neu beurteilt.	•	•	•	
Prozess zur Compliance-Risikobeurteilung	Für die Compliance-Risikobeurteilung besteht ein definierter und implementierter Prozess.	•	•		
	Die Vollständigkeit und Angemessenheit des Prozesses zur Compliance-Risikobeurteilung wird regelmässig beurteilt.	•	•	•	
	Die Compliance-Risikobeurteilung wird mindestens einmal jährlich im gegenseitigen Gespräch sowohl «bottom-up» vom Fachbereich («1st Line of Defense») wie auch aus Sicht der Compliance-Abteilung «top down» vorgenommen.	•	•	•	•
Neubeurteilung von Compliance-Risiken	Eine Beurteilung von Compliance-Risiken erfolgt fallweise bei Bedarf.	•			
	Compliance-Risiken werden mindestens 1x jährlich resp. bei Änderungen des rechtlichen und regulatorischen Umfelds neu beurteilt.	•	•		
	Aus der regelmässigen, wiederkehrenden Beurteilung der Compliance-Risiken wird für jedes dieser Compliance-Risiken in einem individuellen Compliance-Programm dokumentiert, mit welchen Massnahmen das jeweilige Compliance-Risiko adressiert wird.	•	•	•	
	Anlässlich der periodisch wiederkehrenden Beurteilung der Compliance-Risiken wird gleichzeitig auch eine Optimierung der Risikoexponierung angestrebt.	•	•	•	•
Risk-Owner	Der Bereich Compliance ist Risiko-Eigner von Compliance-Risiken	•			
	Die operativ tätigen Fachbereiche («1st Line of Defense») sind Risiko-Eigner ausgewählter Compliance-Risiken.	•	•		
	Die Verantwortung betreffend den Compliance-Risiken ist – abhängig von der Wesentlichkeit und Kategorisierung der Risiken – sowohl beim Bereich Compliance als auch in den Fachbereichen («1st line of defense») angesiedelt. In den Fachbereichen sind die Verantwortlichkeiten im Zusammenhang mit den Compliance-Risiken auch in den Stellenbeschreibungen der Mitarbeitenden enthalten.	•	•	•	

Schulung und Awareness

Schulungen, bereichsübergreifende Zusammenarbeit sowie weitere Sensibilisierungsmassnahmen dem Thema Compliance gegenüber.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Schulungen für Mitarbeitende	Compliance-Schulungen finden bei Eintritt der Mitarbeitenden und ad-hoc anlässlich von Vorfällen statt.	•			
	Compliance-Schulungen finden mindestens einmal jährlich statt.	•	•		
	Compliance-Schulungen werden regelmässig zielgruppenspezifisch durchgeführt und auf ihre Wirksamkeit geprüft.	•	•	•	
	Der Inhalt und die Form von Compliance-Schulungen werden laufend verbessert und den Bedürfnissen der Mitarbeitenden angepasst.	•	•	•	•
Compliance-Awareness	Ein Bewusstsein für Compliance-Aspekte ist bei den Mitarbeitenden des Unternehmens ansatzweise vorhanden.	•			
	Compliance-Aspekte werden regelmässig bei der Entscheidungsfindung diskutiert.	•	•		
	Die Wichtigkeit von Compliance-Aspekten wird erkannt und gefördert, indem Mitarbeitende auf ihren persönlichen Beitrag zum Erfolg des Compliance Management Systems im Rahmen der jährlichen Zielvereinbarungen verpflichtet werden.	•	•	•	
	Compliance ist fester Bestandteil der regelmässigen Mitarbeiterbeurteilung bei relevanten Mitarbeitenden.	•	•	•	•
Information zum CMS – extern	Die Existenz des Verhaltenskodex wird intern – und bei Anfrage – auch an extern kommuniziert.	•			
	Mitarbeitende und fallweise auch Geschäftspartner werden zur Einhaltung des Verhaltenskodex verpflichtet (bspw. durch Unterzeichnung einer entsprechenden Erklärung).	•	•		
	Die tatsächliche Einhaltung des Verhaltenskodex ist Gegenstand von Prüfungen bei wesentlichen Geschäftspartnern.	•	•	•	

Austausch und Interaktion

Einbettung der Compliance-Funktion im Unternehmen.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Einbezug von Compliance	Der Compliance-Funktion wird fallweise die Möglichkeit gegeben, im Rahmen von Projekten und Vorhaben ihre Einschätzung bezüglich den damit verbundenen Compliance-Risiken abzugeben.	•			
	Die Compliance-Funktion wird systematisch hinzugezogen, um im Rahmen von Projekten und Vorhaben ihre Einschätzung bezüglich der damit verbundenen Compliance-Risiken abzugeben.	•	•		
	Die Einschätzung der Compliance-Funktion ist fester Bestandteil der Entscheidungsprozesse im Unternehmen, die eine Relevanz im Zusammenhang mit Compliance haben oder haben könnten.	•	•	•	
	Wirksame Eskalationswege sind definiert, sollten im Rahmen von Projekten oder Vorhaben wesentliche Compliance-Risiken erkannt werden.	•	•	•	•
Austausch mit «1st Linie of Defense»	Ein Austausch zwischen Compliance und den Fachbereichen (Funktionen der «1st Linie of Defense») findet in unregelmässigen Abständen oder informell statt.	•			
	Es findet ein regelmässiger Austausch zwischen Compliance und den Funktionen der «1st Linie of Defense» statt. Ziel und Zweck dieser Austausche ist ein laufender gegenseitiger Informationsaustausch sowie die Vermittlung von Fachwissen.	•	•		
	In den Fachbereichen stehen der (zentralen) Compliance-Funktion dezidierte und ausgebildete Ansprechpartner für die Belange der Compliance «vor Ort» zur Verfügung.	•	•	•	
Austausch mit anderen Kontroll-funktionen	Zwischen Compliance und anderen Kontrollfunktionen findet anlassbezogen ein Austausch statt.	•			
	Zwischen Compliance und anderen Kontrollfunktionen findet ein regelmässiger Austausch statt, wodurch sichergestellt ist, dass ein Verständnis darüber besteht, was andere Kontrollfunktionen machen.	•	•		
	Die Kontrollfunktionen stimmen sich gezielt bezüglich ihrer jeweiligen Methodologie ab und definieren resp. dokumentieren dabei auch bspw. die Schnittstellen und Zuständigkeiten, so dass es zu keinen Überlappungen oder ungenügend abgedeckten Risiko-Expositionen kommt.	•	•	•	
Outsourcing	Die Compliance-Funktion wird bei FINMA-wesentlichen Outsourcings fallsweise involviert.	•			
	Die Compliance-Funktion wird systematisch und während des gesamten Outsourcing-Lebenszyklus (Auswahl, Überwachung, Beendigung) involviert.	•	•		

Leistungsbewertung

Überwachung und Messung der Effektivität
von Compliance Management Systemen.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Überwachung CMS	Die Überprüfung des Compliance Management Systems findet fallweise durch externe Parteien statt.	•			
	Die Überprüfung des Compliance Management Systems findet fallweise durch die interne Revision statt.	•	•		
	Die Prozesse zur Überprüfung des Compliance Management Systems sind definiert. Es findet eine systematische Überprüfung der Angemessenheit statt.	•	•	•	
	In regelmässigen Abständen findet eine Überprüfung der Wirksamkeit des Compliance Management Systems statt.	•	•	•	•
Indikatoren / KPIs	Unser Unternehmen hat ein Konzept und hat eine Vorstellung davon, anhand welcher betriebs-spezifischer Indikatoren die Effektivität der Compliance-Massnahmen gemessen werden könnte. Die Indikatoren sind jedoch nicht implementiert.	•			
	Unser Unternehmen misst die Erreichung der Compliance-Leistung anhand uneinheitlicher, allgemeiner Kriterien.	•	•		
	Um die Compliance-Leistung insgesamt zu messen und zu beurteilen, hat unser Unternehmen einheitliche Kriterien implementiert (wie bspw. Anzahl Anfragen beim Compliance Office, Anzahl Meldungen über den vertraulichen Meldekanal, Anzahl ausgesteuerter Transaktionen automatisierter Kontrollen, etc.).	•	•	•	
	Unser Unternehmen verfügt über ergebnisorientierte Indikatoren zur Bewertung der Wirksamkeit des Compliance Managment Systems, z.B. ob durch Einführung eines Meldekanals Fälle von «non compliance» früher aufgedeckt und dadurch Kosten gespart werden oder ob die Compliance-Massnahmen dazu führen, dass die Anzahl Konsultationen der Fachbereiche beim Compliance Office laufend zunehmen.	•	•	•	•
Compliance-Berichterstattung	Eine Berichterstattung an den VR findet ad-hoc bei Compliance-Vorfällen statt.	•			
	Eine formalisierte Berichterstattung an den VR findet regelmässig statt. Dabei werden die relevanten Aspekte, wie bspw. Compliance-Risiken, risikoadressierende Massnahmen, Compliance-Vorfälle, Tätigkeitsbereich Compliance, etc. abgedeckt.	•	•		
Interne Audits	Die interne Revision prüft Aspekte im Zusammenhang mit dem Compliance Management dann, wenn sie vom Compliance Office gebeten wird, entsprechende Prüfungshandlungen durchzuführen.	•			
	Die interne Revision deckt fallweise auch Aspekte des Compliance Management Systems ab. Beispielsweise werden zusätzlich zu den ordentlichen Prüfungshandlungen der internen Revision am Rande zusätzlich auch noch vereinzelte Prüfungshandlungen hinsichtlich Compliance-Aspekten vorgenommen.	•	•		
	In regelmässigen Abständen werden interne Audits hinsichtlich Angemessenheit (design) des Compliance Management Systems durchgeführt.	•	•	•	
	In regelmässigen Abständen werden interne Audits hinsichtlich der Wirksamkeit (operating effectiveness) des Compliance Management Systems (bspw. der Schlüsselkontrollen) durchgeführt.	•	•	•	•
Bericht-erstattung zu Compliance-Risiken	Die Compliance-Risiken werden von der zentralen Risiko-Management Funktion unternehmensweit erhoben und bewertet.	•			
	Die Compliance-Risiken werden durch das Compliance-Office erhoben und gemäss der unternehmensweit gültigen Risiko-Bewertungsmethodik bewertet.	•	•		
	Die Compliance-Risiken werden unternehmensweit zentral durch das Compliance-Office «top down» erhoben und durch das Compliance-Office anhand einer eigenen Bewertungsmethodik bewertet.	•	•	•	
	Die Compliance-Risiken werden unter Koordination des Compliance-Office sowohl bottom-up, unter Einbezug der Compliance Verantwortlichen in den Geschäftsbereichen («1st Line of Defense»), als auch «top down» aus der Sicht des zentralen Compliance-Office («2nd Line of Defense») erhoben und gemäss einer eigenen Methodik des Compliance-Office bewertet.	•	•	•	•

Instrumente

Grad der Umsetzung der formellen Vorgaben mittels geeigneter Instrumente und Vorgehen, um Compliance in den Prozessen und somit der Kultur des Unternehmens zu verankern.

Sub-Bereich	Zu bewertende Aussage (stimme zu, stimme teilweise zu, stimme nicht zu)	Initial	Angemessen	Managed	Optimiert
Legal Inventory	Eine dokumentierte und systematische Bestandsaufnahme der wesentlichen rechtlichen, regulatorischen und selbstauferlegten Verpflichtungen findet statt und dient als Basis zum Unterhalt des Inventars an Compliance-Risiken.	•	•		
	Die Bestandesaufnahme wird bei Bedarf als auch in regelmässigen Abständen überprüft und aktualisiert.	•	•	•	
	Regulierungs- und Gesetzesvorhaben werden laufend überwacht und fliessen laufend in die Bestandesaufnahme ein.	•	•	•	•
Code of Conduct	Unser Unternehmen verfügt über einen Verhaltenskodex.	•			
	Der Verhaltenskodex trägt den spezifischen Gegebenheiten des Unternehmens Rechnung.	•	•		
	Der Verhaltenskodex wird regelmässig überprüft und aktualisiert.	•	•	•	
	Der Verhaltenskodex wird von der Geschäftsleitung oder direkten Vorgesetzten anlässlich von Mitarbeiteranlässen proaktiv thematisiert.	•	•	•	•
Whistleblowing	Die Mitarbeitenden unseres Unternehmens sind angehalten, bei Beobachtungen zu Fehlverhalten ihren direkten Vorgesetzten oder das Compliance-Office anzusprechen.	•			
	Unser Unternehmen verfügt über einen formellen und für jedermann erreich- und kontaktierbaren Kanal, um Fehlverhalten zu melden («Whistleblowing»).	•	•		
	Die Mitarbeitenden werden regelmässig auf die «Whistleblowing»-Meldestelle hingewiesen.	•	•	•	
	Die Mitarbeitenden wissen aufgrund vergangener Vorfälle, in welchen Mitarbeitende Meldung erstatteten, dass ein Hinweisgeber beim Absetzen einer gerechtfertigten Meldung keine negativen Konsequenzen (bspw. Entlassung, «shaming and blaming», etc.) zu befürchten hat.	•	•	•	•
Compliance-Risiken/ Kontrollen	Compliance-Risiken und entsprechende Kontrollen sind im IKS ansatzweise dokumentiert.	•			
	Compliance-Risiken und entsprechende Kontrollen sind im integralen IKS vollständig dokumentiert und werden systematisch auf ihre Relevanz geprüft (Scoping) und aktualisiert. Es besteht eine dokumentierte Verlinkung zu den relevanten operativen Prozessen.	•	•		
Kontroll-überwachung	Die Kontrollen werden fallweise und in unstrukturierter Form überprüft (z.B. Plausibilitätsprüfungen).	•			
	Die IKS-Kontrollen zur Handhabung von Compliance-Risiken werden auf ihre Angemessenheit geprüft. Es bestehen jedoch keine Vorgaben für ein systematisches Testing/Prüfung durch eine unabhängige interne oder externe Stelle.	•	•		
	Die Kontrollen werden regelmässig (jährlich oder mindestens einmal alle drei Jahre) durch eine unabhängige interne oder externe Stelle auf ihre Wirksamkeit geprüft. Diese Überprüfung basiert auf einem Jahres- oder Mehrjahrestestplan. Über die Ergebnisse dieser Überprüfung wird Bericht erstattet.	•	•	•	

Autoren

Matthias Kiener
Partner und Leiter Forensic
bei Mazars Schweiz

Denise Wipf
Parnerin und Leiterin Versicherungen
bei Mazars Schweiz

Angela Zeier Röschmann
Dr. oec. HSG
Professorin und stellvertretende Leiterin
des Instituts für Risk & Insurance
ZHAW School of Management and Law

Sebastian Barth
M.A. HSG
Wissenschaftlicher Mitarbeiter am
Institut für Risk & Insurance
ZHAW School of Management and Law

Mazars ist ein führendes internationales Unternehmen, das auf die Bereiche Wirtschaftsprüfung, Steuern und Recht* sowie Accounting, Financial Advisory und Consulting spezialisiert und in über 90 Ländern vertreten ist. Unsere 44.000 Experten – 28.000 in unserer integrierten Partnerschaft, 16.000 in der Mazars North America Alliance – arbeiten vertrauensvoll mit ihren Kunden zusammen und unterstützen sie dabei, ihr Geschäft nachhaltig zu sichern und auszubauen. In der Schweiz arbeiten mehr als 300 Experten an den Standorten in Zürich, Bern, Genf, Lausanne, Freiburg, Neuenburg, Sitten und Delsberg.

* wo dies nach den geltenden Landesgesetzen zulässig ist

Das Institut für Risk & Insurance (IRI) ist das Kompetenzzentrum der ZHAW School of Management and Law für ökonomische und sozialwissenschaftliche Fragen im Bereich der Versicherungswirtschaft. Mit seinen Tätigkeiten in Aus- und Weiterbildung trägt es zur professionellen Qualifizierung von Fachleuten der Versicherungsbranche bei. Als kompetenter Partner in Forschung und Beratung arbeitet es eng mit verschiedenen in- und ausländischen Institutionen zusammen.

Herausgeber

Mazars AG
Herostrasse 12
8048 Zürich

ZHAW School of Management and Law
Institut für Risk & Insurance
Technoparkstrasse 2
Postfach
8401 Winterthur
Schweiz

Kontakt

Matthias Kiener
matthias.kiener@mazars.ch

Denise Wipf
denise.wipf@mazars.ch

Angela Zeier Röschmann
angela.zeier@zhaw.ch

mazars

Zürcher Hochschule
für Angewandte Wissenschaften

zh
aw

School of
Management and Law