Compliance als unabhängige Kontrollfunktion
Rolle / Zusammenarbeit mit Risk / Herausforderungen

September 2020

Daniel Gysel / Chief Compliance Officer Zurich Schweiz

45. Fachveranstaltung – Netzwerk Risikomanagement

Inhalt

Alles compliance oder was? – Allgemeiner Kontext zu Compliance

Die drei Verteidigungslinien und ihre Herausforderungen

© Zurich

Inhalt

© Zurich

Einführung

Eine etwas provozierende Aussage zum Start…

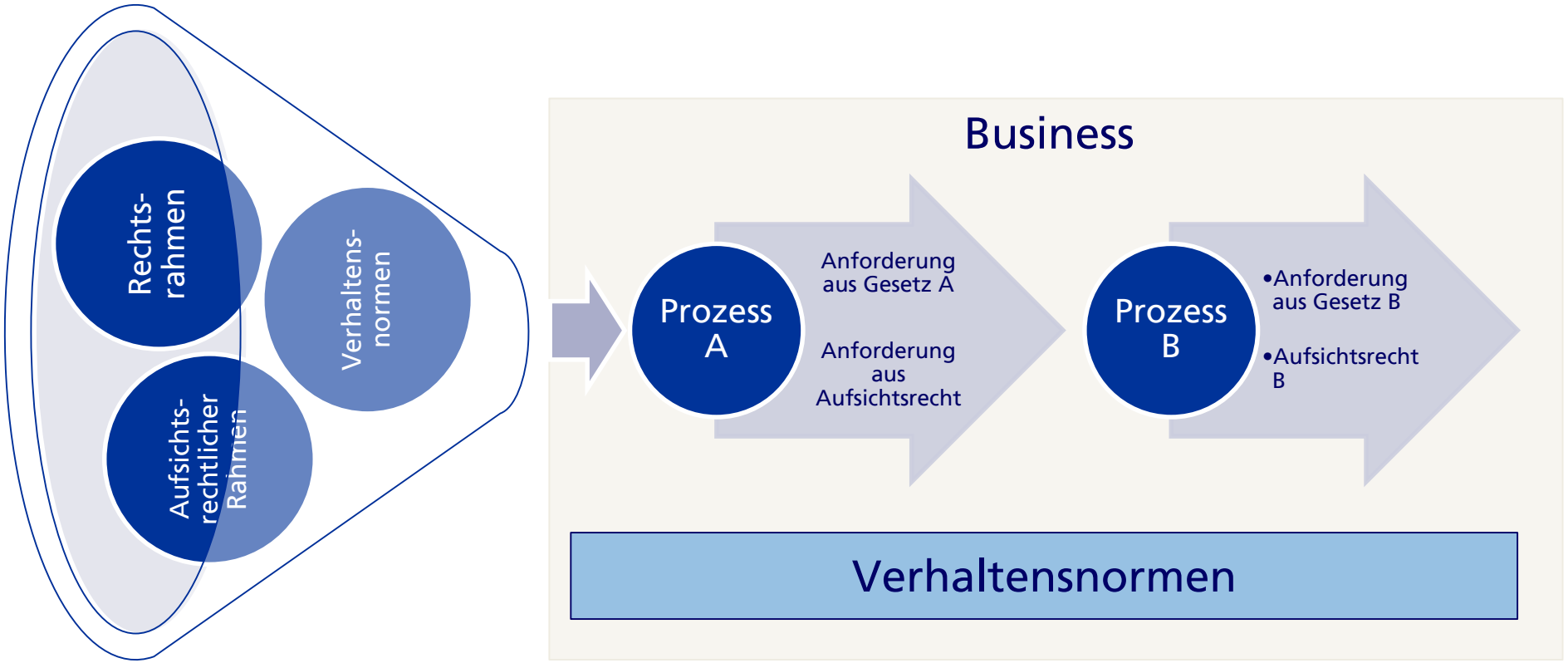
«Compliant sein» ist wie schwanger sein: Man ist es oder man ist es nicht. Dazwischen gibt es nichts.

…und, schlussendlich hat Compliance sehr viel mit einer erwarteten «Verhaltensnorm» zu tun…

© Zurich

Einführung

Aber was ist Compliance mit einfachen Worten erklärt wirklich…..?



“Operationalisierung von Gesetzen und Verhaltensnormen”

© Zurich

1. Aufsichtsrechtliche Vorgaben

Welche Vorgaben werden an die Compliance-Funktion gestellt (Auswahl)?

Quelle	Elemente
Kapitel – Risikomanagement Aufsichtsverordnung (AVO) Art. 96 Abs. 3	Wirksame Compliance-Funktion und wirksame Compliance-Prozesse. Sie stellen in ihrer Gesamtheit sicher, dass die Rechtsnormen und die internen Vorschriften eingehalten werden.
Kapitel – Risikomanagement: Aufsichtsverordnung (AVO) Art. 96 Abs. 4	Die Compliance-Funktion muss unabhängig sein. Ausstattung in Bezug auf die Grösse, der Geschäfts- und Organisations-komplexität und der Risiken des Versicherungsunternehmens.

© Zurich

1. Aufsichtsrechtliche «Praxis»

Welche aufsichtsrechtlich formulierte Praxis gilt?

Quelle	Elemente
FINMA-Rundschreiben 2017/2 Corporate Governance – Versicherer	Rz. 11: Einrichtung einer wirksamen Compliance-Funktion und periodische Überprüfung deren Angemessenheit durch eine unabhängige Partei.
	Rz. 12: Festlegung von Grundsätzen, Prozessen und Strukturen zur Einhaltung von gesetzlichen, regulatorischen und internen Vorschriften.
	Rz. 37: Identifiziert seine wesentlichen rechtlichen/regulatorischen Verpflichtungen. Einschätzung der wesentlichen Compliance-Risiken.
	Rz. 42: Beurteilung der Angemessenheit der vom Unternehmen eingerichteten Grundsätze, Prozesse und (Kontroll-)Strukturen zur Einhaltung der rechtlichen, regulatorischen und internen Vorschriften
	Rz. 43: Der Leiter Compliance nimmt periodisch eine Einschätzung der wesentlichen Compliance-Risiken vor und berichtet darüber dem VR.

© Zurich

3. Fokus auf das wesentliche

Was ist für die Compliance-Funktion von «Wesentlichkeit»?

Fragestellung

Was unternimmt die Gesellschaft, um Risiken (unternehmensweite und prozessbezogene) in Bezug auf die Befolgung von Rechtsnormen und internen Vorschriften zu managen?

Antwort

Die Befolgung von Rechtsnormen und internen Vorschriften unterliegt faktisch keiner «Wesentlichkeit» ➔ Wir können uns nicht erlauben «nicht compliant» zu sein.

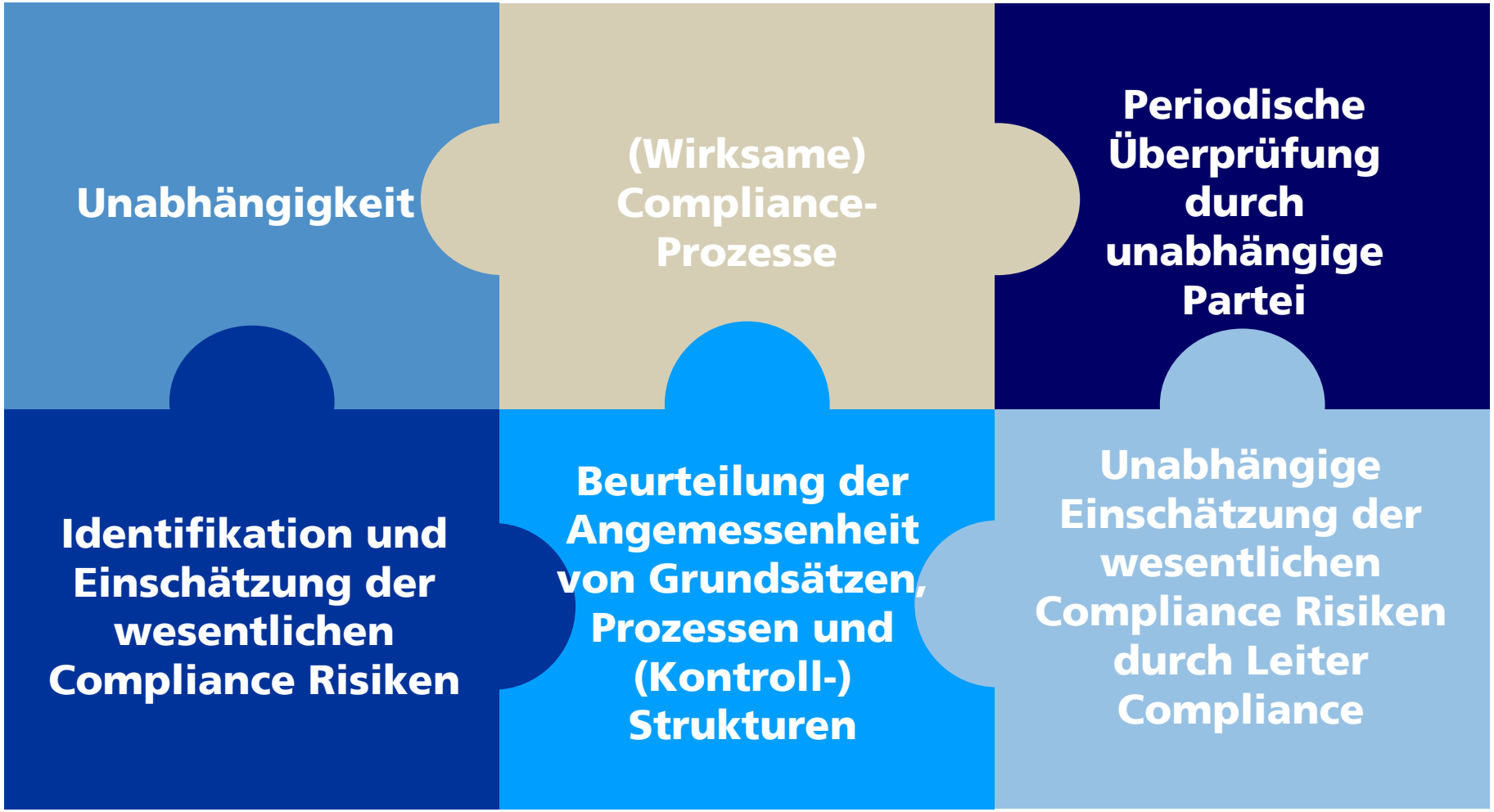
Konsequenz

Kenne deinen Rechtsrahmen in dem du dich bewegst, kenne deine Weisungen und etabliere Mechanismen zu deren Einhaltung!

© Zurich

1. Vorgaben und «Praxis»

Übersicht der wichtigsten Elemente einer Compliance-Funktion



© Zurich

2. «Moderne» Compliance-Funktion

Was macht eine moderne Compliance-Funktion aus?

ZURICH

Unab-hängigkeit	Organisatorische Eingliederung direkt beim CEO oder «dotted line» zum General Counsel. Oder als Minimalzustand keine operativen Aufgaben der Business-Bereiche sowie direkter Zugang zur GL und zum VR. Weitere wichtige Faktoren bilden die Kompetenzen, die Berichterstattung, der freie Zugang zu allen relevanten Informationen.
(Wirksame) Compliance-Prozesse	• Neben «klassischen» Themen wie Weisungswesen, Schulung von Mitarbeitern, Datenschutz, GwG etc. sind nach heutiger Auslegeordnung weitere Elemente abzudecken: ▪ Überwachung des Rechtsumfeldes und Transformierung in Weisungen ▪ Frühe, enge Begleitung von Projekten ▪ Führen eines Legal Inventory sowie eines Compliance-Risiko Inventar ▪ Überprüfung der Einhaltung von externen/internen Vorgaben durch die operativen Einheiten (Testen von IKS-relevanten Kontrollen) ▪ Regelmässige Berichterstattung an GL und VR.

© Zurich

2. «Moderne» Compliance-Funktion

Was macht eine moderne Compliance-Funktion aus?

Überprüfung der Funktion	• Periodische Überprüfung der Compliance-Funktion und der Prozesse durch die Interne Revision oder durch eine externe, unabhängige Partei.
Identifikation und Einschätzung Compliance Risiken	• Das Versicherungsunternehmen (und nicht die Compliance-Funktion) ist für die Identifikation, Einschätzung und Adressierung der Compliance-Risiken verantwortlich. **ABER** – die Compliance-Funktion muss trotzdem eine zentrale Koordinations-Rolle inne haben (Beurteilung der eingerichteten Prozesse und (Kontroll-)-Strukturen ist ansonsten nicht realistisch). • Die «Ownership» über das Compliance-Risikoregister liegt bei der Compliance-Funktion.
Beurteilung von Prozessen und (Kontroll) - Strukturen	• Compliance als 2nd Line of Defense ➔ Überprüfung der für die Identifizierung, Einschätzung und Adressierung von Compliance-Risiken vorhandenen Prozesse und Kontrollen in den operativen Einheiten (IKS Testing). Die Intensität der Überprüfung: «Prinzip der Verhältnismässigkeit».

© Zurich

2. «Moderne» Compliance-Funktion

Was macht eine moderne Compliance-Funktion aus?

ZURICH

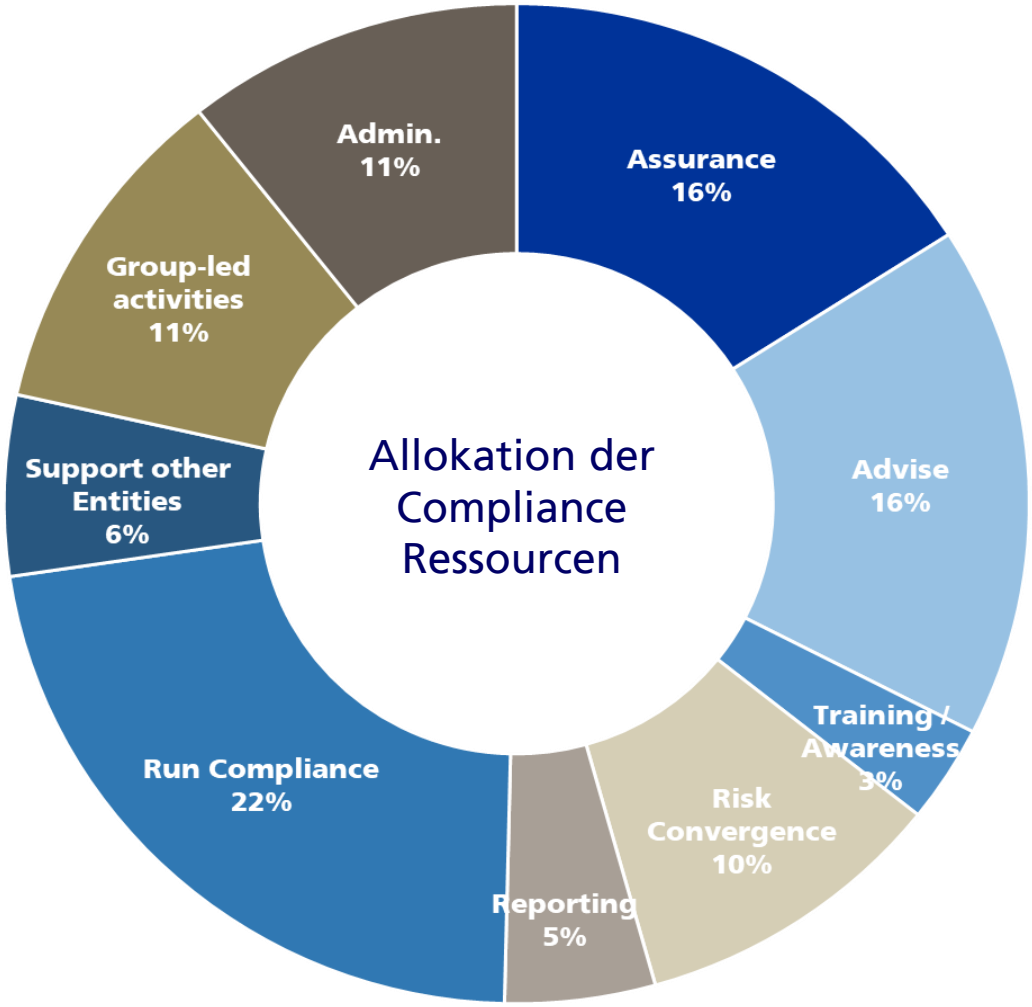
Einschätzung durch Leiter Compliance-Funktion

- Mindestens jährliche Einschätzung der «wesentlichen» Compliance-Risiken und Berichterstattung an den Verwaltungsrat.
- Im Idealfall führt das Unternehmen ein Top-Down sowie Bottom-Up Risk Assessment durch. Die Basis hierzu sollte das Operationelle Risikomanagement liefern können. Im jährlichen Compliance-Bericht an den Verwaltungsrat sind die relevantesten Risiken aufzuführen und durch den Leiter Compliance zu kommentieren.
- Basierend auf dem Risiko-Assessment wird der jährliche Compliance-Plan (Prospektiv) erstellt (inklusive Budget und Ressourcen Angaben), so dass der VR der Compliance-Funktion «formell» das Mandat erteilen kann.

© Zurich

Übersicht unserer Haupt-Tätigkeitsblöcke im 2020

Assurance (unabhängiges Testing im Business) gewinnt mehr und mehr an Relevanz



Group led activities (11% of available resources)
Initiatives initiated by the Group Compliance function.

Assurance activities (16%)
75% of all planned assurance activities will focus on a "Review" level of assurance. 20% on "Testing".

Advise (16%)
Provide advice based on internal requirements (obligation to seek guidance from Compliance) and other requests of the business.

Risk Convergence (10%)
In order to further strengthen our Internal Control System, we need to develop an approach to support the systematic identification of compliance risks. In a second step, the identified compliance risks need to be properly allocation to the business processes.

Run Compliance (22%)
The Compliance function will increasingly support the business in its major projects and also provide assurance in favor to the management.

Support other Entities (6%)
Support / Manage Compliance of other group-owned legal entities.

© Zurich

Compliance im Fokus der Aufsicht

Worauf achtet die Aufsicht bei der Compliance (Funktion)?

Reguläre Aufsicht

Governance Assessment

- Verantwortung des VR für den Aufbau, die Ausgestaltung und Überwachung einer Compliance-Funktion
- Einrichtung einer wirksamen Compliance-Funktion inkl. Berichterstattungswege
- Verantwortungsbereich des Leiters der Compliance-Funktion/Unabhängigkeit der Funktion
- Vorhandensein einer Bestandsaufnahme der wesentlichen rechtlichen, regulatorischen und sonstigen externen Vorschriften (inkl. Verantwortlichkeit betr. Einhaltung dieser Vorschriften)
- Systematische und dokumentierte Einschätzung der Compliance-Risiken

- **Bewilligung von Geschäftsplänen und Geschäftsplanänderungen (lit. b)**
- **Vor-Ort Kontrollen durch die FINMA**
- **IKS Questionnaire (Abdeckung der Compliance Risiken im Unternehmen)**

© Zurich

Inhalt

© Zurich

Three Lines of Defense (LoD)

Wie hat die Zurich dies definiert?

1st Line of Defense	management, including its compliance risks. The first line has **responsibility** and **accountability** for implementing and operating controls to ensure compliance with all applicable laws, regulations and internal requirements, professional and industry standards and Zurich's stated corporate values **to set the tone-at-the-top** by their own exemplary conduct.
2nd Line of Defense	**Group Risk Management** and **Group Compliance** provide different lenses and frameworks to manage risks, independent challenge, oversight, monitoring and assurance, advice and support the first line in promoting Zurich's customer centric and ethical culture.
3rd Line of Defense	**Audit (Internal and External)** provides independent and objective assurance, through challenge and testing, regarding the adequacy and effectiveness of the Group's risk management, internal controls and governance processes.

© Zurich

Auszug aus einer Unterhaltung zwischen Risk und Compliance

Der CRO hatte mal dem CCO geschrieben:
«Ich habe den Eindruck, dass nur Mitarbeiter X und Y als Schnittstelle zu haben nicht ausreicht um den Koordinationsbedarf abzudecken. Intuitiv fände ich es effektiver, wenn sich je der Risk Officer und der Compliance Officer, die die gleiche Funktion abdecken wie ein Team zusammentun, sich regelmässig treffen und sich gemeinsam um ganzheitliche und koordinierte Assurance für die Funktion kümmern würden. Beim Agenturvertrieb funktioniert das z.B. schon ganz gut.»

Der CCO hatte zurück geschrieben:
Meine Vorstellung einer idealen Interaktion zwischen Risk und Compliance auf einer "Arbeitsebene" sieht wie folgt aus:

- *Regelmässige Austauschmeetings zwischen den jeweiligen Risk sowie Compliance Managern*
- *Fachlicher Lead (und falls angezeigt unter Einbezug der jeweiligen 2nd LoD Funktion) bei rechtlich gelagerten Risiken bei Compliance*
- *Fachlicher Lead bei Risk für Op. Risks und FRR.*

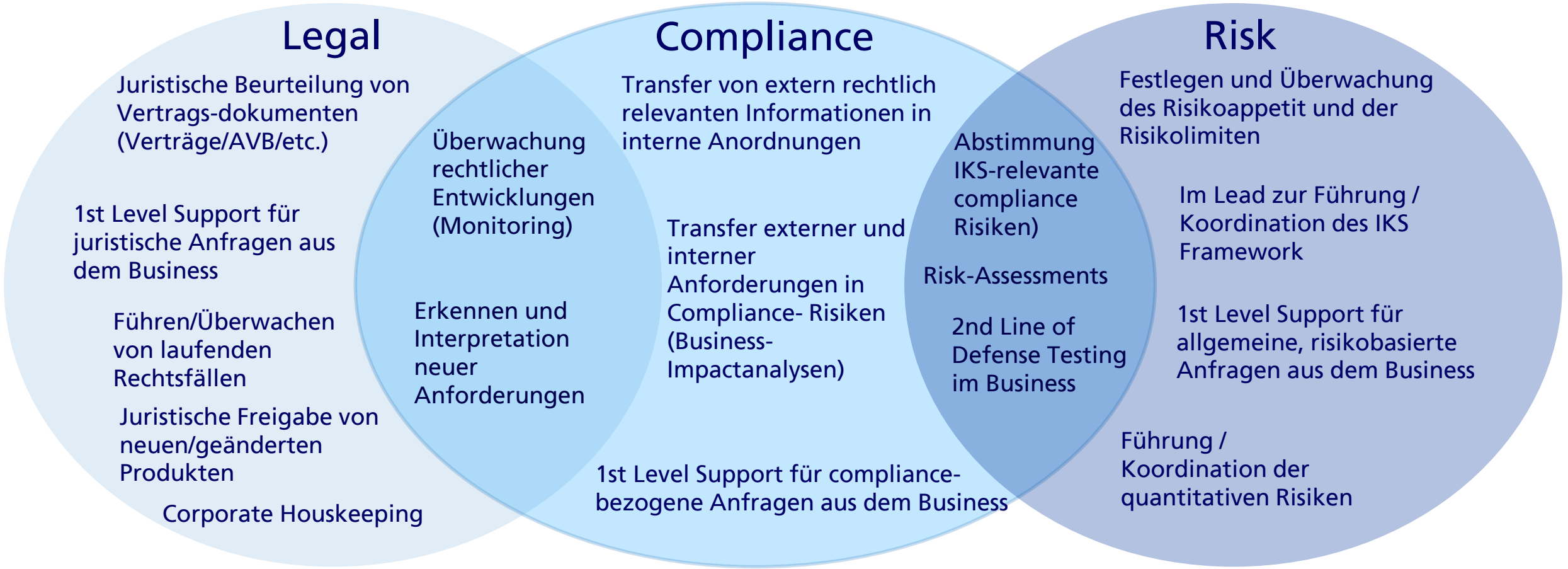
Wir müssen einen Modus Operandi finden der uns nicht unnötig lähmt infolge von ewigen Koordinationsmeetings, aber die jeweiligen Arbeiten/Erkenntnisse des Gegenüber nicht in den Wind schlägt. Darum würde ich den jeweiligen Topic Lead wie oben skizziert begrüssen.

Der CRO war begeistert:
«Ganz genau so!»

© Zurich

3. Arbeitsteilung: Legal, Compliance und Risk

Geht das auf eine effiziente Art und Weise in Bezug auf Rechtsrisiken?



© Zurich

Compliance Risk Convergence

Unsere lokalen Compliance-Risikocluster

#	Unsere Compliance Risiko-Cluster
1	Geschäftsplanänderungen / Auskunftspflicht
2	Corporate Governance
3	Vertrieb/Vermittlung & Kundenschutz
4	AIA/FATCA
5	Tax
6	AML
7	Datenschutz
8	Antikorruption / Betrug / Kartellrecht / IP
9	Anlageverwaltung und -fonds
10	Human Resources
11	Underwriting
12	Aktuariat Leben
13	Aktuariat Nicht-Leben
14	Gebundenes Vermögen
15	Risikopolitik, Kapitalmodelle und IKS
16	Finance & Accounting
17	Embargo
18	Technologie / IT Security / Operational Resilience
19	Schaden/Leistungen
20	Tarifierung
21	Produktentwicklung

© Zurich

Besten Dank für den Austausch

Daniel Gysel
Chief Compliance Officer
Compliance Zurich Schweiz

Zürich Versicherungs-Gesellschaft AG
Postfach, 8085 Zürich
Hagenholzstrasse 60
8050 Zürich

+41 76 352 10 82
daniel.gysel@zurich.ch
www.zurich.com

© Zurich