



DICO-Positionspapier ESG

Stand: Juni 2023

DICO

Deutsches Institut für Compliance

Inhaltsverzeichnis

ZUSAMMENFASSUNG	3
A. EINLEITUNG	4
B. DARSTELLUNG DER OPTIONEN	9
1. SÄULENMODELL, SOG. KLEINE LÖSUNG	9
A) AUSGANGSLAGE	9
B) DAS SÄULENMODELL	9
C) GRUNDLAGEN	9
D) ORGANISATION VON ESG IM UNTERNEHMEN	10
E) ZUORDNUNG SPEZIFISCHER ESG-ZUSTÄNDIGKEITEN	11
F) ÖFFNUNG MULTIFUNKTIONALER CMS-ELEMENTE FÜR ESG-THEMEN	11
G) ZUSAMMENARBEIT UND SCHNITTSTELLEN BEI ESG	12
H) BUDGET/RESSOURCEN	13
I) ESG-BERICHTERSTATTUNG/RATINGS	13
J) UMSETZUNG, WEITERENTWICKLUNG UND AUSBLICK	13
2. CROSS-FUNKTIONALES MODELL, SOG. „MITTLERE LÖSUNG“	14
A) AUSGANGSLAGE	14
B) DAS CROSS-FUNKTIONALE MODELL	14
C) GRUNDLAGEN	14
D) ORGANISATION VON ESG IM UNTERNEHMEN	15
E) SPEZIFISCHE ESG-ZUSTÄNDIGKEITEN UND AUFGABEN DER COMPLIANCE FUNKTION	16
F) ZUSAMMENARBEIT UND SCHNITTSTELLEN BEI ESG	17
G) BUDGET/RESSOURCEN	18
H) ESG-BERICHTERSTATTUNG/RATINGS	18
I) UMSETZUNG UND WEITERENTWICKLUNG	18
3. GESAMTSTEUERUNGSMODELL, SOG. „GROSSE LÖSUNG“	19
A) AUSGANGSLAGE	19
B) DAS GESAMTSTEUERUNGSMODELL	20
C) GRUNDLAGEN	21
D) ORGANISATION VON ESG IM UNTERNEHMEN	21
E) SPEZIFISCHE ESG-ZUSTÄNDIGKEITEN UND AUFGABEN DER COMPLIANCE-FUNKTION	23
F) ESG-KONTROLLE, MONITORING UND BERICHTERSTATTUNG/RATINGS	26
G) BUDGET/RESSOURCEN	27
C. AUSBLICK	27

Zusammenfassung

- Steigende ESG (Environmental - Social - Governance)-Anforderungen führen für Unternehmen zu einer Vielzahl strategischer, wirtschaftlicher und rechtlicher Fragestellungen.
- Die Frage, wie diese Themen organisatorisch und prozessual im Unternehmen behandelt werden und wie Aufgaben und Verantwortlichkeiten im Einzelnen verteilt werden, betrifft auch die Compliance-Funktion.
- DICO legt mit diesem Positionspapier drei mögliche Gestaltungsoptionen vor, auf deren Basis die Compliance-Funktion ihren eigenen Beitrag für einen angemessenen und wirksamen ESG-Ordnungsrahmen bzw. eine entsprechende ESG-Governance bestimmen kann.
 - Im **Säulenmodell**, der sog. „**kleinen**“ **Lösung**, agiert Compliance als Säule im ESG-System für die klassischen Compliance-Themen (Korruptionsbekämpfung, Kartellrecht, Menschenrechte). ESG-Querschnittsprozesse werden unterstützt (z.B. Hinweisgebersystem, Geschäftspartnerprüfungen). Zum Reporting liefert Compliance der ESG-Berichterstattung als verantwortlicher Fachbereich für die Compliance-Themen zu und hat darüber hinaus keine Rolle. Compliance überwacht ferner die Umsetzung relevanter Kontrollen im operativen Geschäft für seine Themen und passt diese ggf. an.
 - Im **cross-funktionalen Modell** – der sog. „**mittleren**“ **Lösung** – übernimmt Compliance kompetenzbasiert neben den klassischen Compliance Themen auch Aufgaben aus anderen ESG-Feldern (z.B. gesamthafte ESG-Risikoanalyse, Prüfung von Greenwashing-Hinweisen). Zum Reporting liefert Compliance der ESG-Berichterstattung als verantwortlicher Fachbereich für die Compliance-Themen sowie für die zusätzlichen Aufgaben zu. Compliance überwacht die Umsetzung relevanter Kontrollen im operativen Geschäft für seine Themen und passt diese ggf. an.
 - Beim **Gesamtsteuerungsmodell**, der sog. „**großen Lösung**“, übernimmt Compliance auf Ebene der 2nd Line die Gesamtsteuerung zu Definition, Ausgestaltung und Betrieb der ESG-Governance. Zusätzlich deckt Compliance neben den zugeordneten Compliance-Themen weitere inhaltliche Aufgaben (s. mittlere Lösung) ab. Zum Reporting liefert Compliance der externen ESG-Berichterstattung zu und verantwortet gesamthaft die Berichterstattung zur Beurteilung der ESG-Governance. Ferner überwacht Compliance (in Abstimmung mit dem nicht-finanziellen IKS) die Umsetzung relevanter Kontrollen zur Beurteilung der Angemessenheit und Wirksamkeit der ESG-Governance und passt diese ggf. an.
- Die Optionen sind als Beitrag zu verstehen, das Thema ESG aus Sicht der Compliance-Funktion zu durchdringen und die Compliance-Funktion im Lichte dieser Entwicklungen zu positionieren.

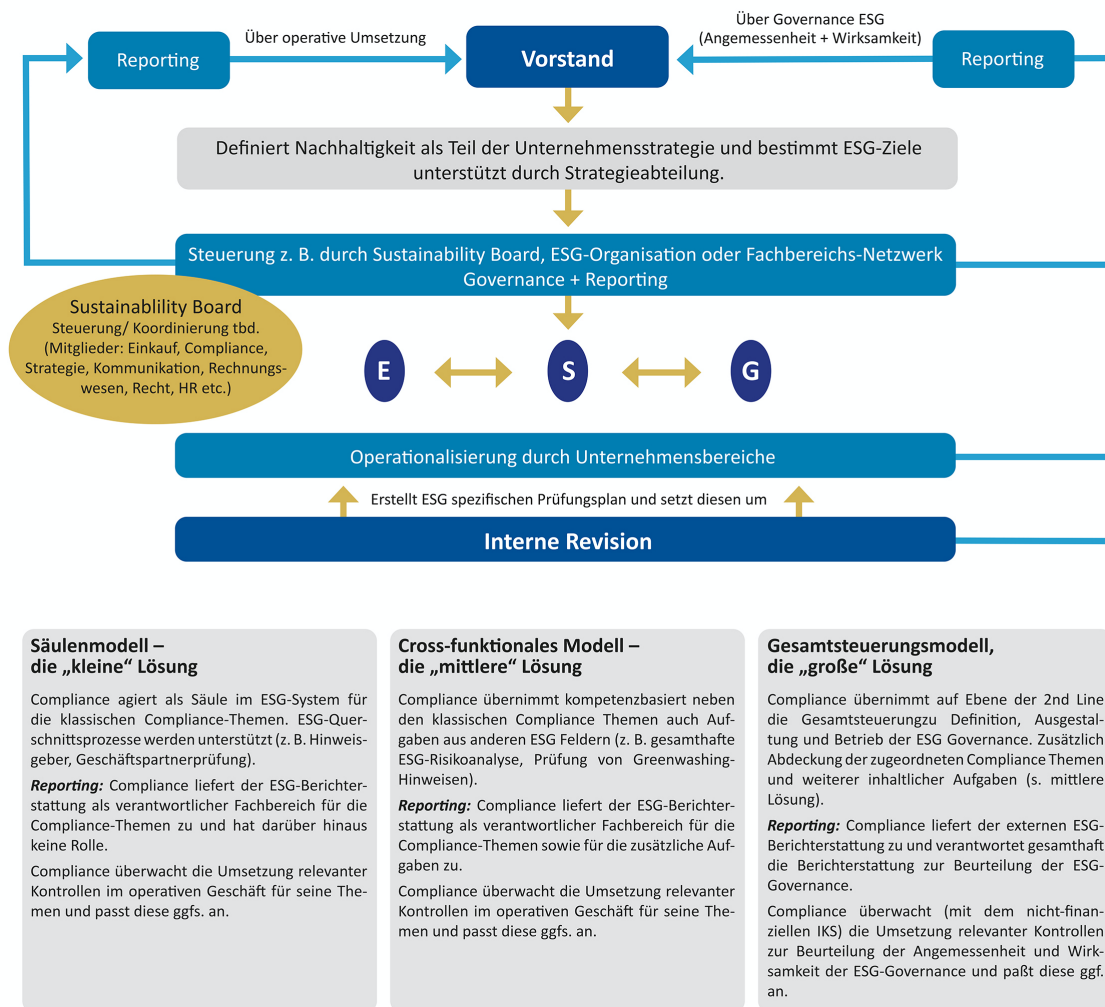


Abbildung 1: Übersicht der verschiedenen Modelle

A. Einleitung

1. „Nachhaltigkeit“ wurde in den Unternehmen lange Zeit im Schwerpunkt den Funktionen Kommunikation und Marketing, Human Resources und/oder Investor Relations überlassen. Compliance kümmerte sich allenfalls um die Interpretation und Umsetzung von Rechtsvorgaben im Bereich Nachhaltigkeit, die mit schwerwiegenden Sanktionen oder Haftungsrisiken für das Unternehmen, die Unternehmensführung oder die Mitarbeitenden belegt sind. ESG (für: Environmental - Social - Governance) stellt diese Ordnung in Frage. Bereits mit dem UK-Modern Slavery Act aus dem Jahr 2015 wurden Unternehmen verpflichtet, dafür Sorge zu tragen, dass in der Lieferkette die Menschenrechte eingehalten werden. Mehr und mehr Umwelt- und Sozialstandards, wie auch Grundsätze guter Unternehmensführung werden gesamtgesellschaftlich getragen und auf Betreiben der Zivilgesellschaft und Politik in verbindliche Normen überführt. Das hat Auswirkungen auf die Organisation von Unternehmen, die diese Rahmenbedingungen bei ihrer Geschäftstätigkeit zu beachten haben.

Aber sind die Unternehmen bereit, sich auf diese Veränderungen einzustellen? „Das haben wir schon immer so gemacht“ sagen diejenigen, die am Status-Quo festhalten und jedem Bereich seine angestammte Zuständigkeit für bestimmte Themen belassen wollen. Eine Unternehmensleitung jedoch, die sich mit den neuen und dynamischen ESG-Anforderungen befasst, wird schnell erkennen, dass die bisherige Unternehmensorganisation an ihre Grenzen stößt. Die ESG-Regulatorik führt zu neuen rechtlichen Risiken im unternehmerischen Handeln. Derartigen Risiken wirksam zu begegnen war in der Vergangenheit schon immer die Aufgabe von Compliance und wird es auch in Zukunft sein. Insofern müssen sich die Compliance-Organisationen in Unternehmen auf beachtliche Veränderungen einstellen.

2. Compliance wäre jedenfalls nicht gut beraten, sich zurückzulehnen und zu warten, ob der ESG-Hype vorüberzieht. Denn das wird er nicht. Es sei an dieser Stelle daran erinnert, dass vor knapp 20 Jahren viele dasselbe vom „Compliance-Hype“ dachten. Die Unternehmensleitung darf und sollte von ihrem Compliance-Bereich erwarten, dass dieser Vorschläge macht, wie sich neue Rechtsrisiken, die sich aus dem ESG-Hype ergeben, am besten eingrenzen lassen. Compliance verfügt über die Erfahrung, die Methodenkompetenz und die Instrumente, um diesen Risiken zu begegnen. Compliance ist zudem in vielen Unternehmen schon heute Treiber einer ethischen Unternehmenskultur und damit in besonderer Weise geeignet, sich Themen wie der Einhaltung der Klimaziele und der Menschenrechte, wie auch der Verhinderung von Greenwashing sowie gute Unternehmens-Governance mit auf die Fahnen zu schreiben.

Für bestehende Compliance-Organisationen ist jedenfalls jetzt der Moment, den zukünftigen Verantwortungs- und Tätigkeitsbereich (mit) zu gestalten. Was bedeutet ESG für das jeweilige Unternehmen? Was bedeutet ESG für Compliance?

3. Die Corporate Sustainability Reporting Directive „CSRD“ (EU 2022/2464) ist am 5. Januar 2023 in Kraft getreten und muss innerhalb von 18 Monaten von den Mitgliedsstaaten umgesetzt werden. Vorausgegangen waren die Non-Financial Reporting Directive (2014/95/EU), die Offenlegungsverordnung (2019/2088/EU) und die Taxonomieverordnung (2020/852/EU).

Die CSRD erweitert die bisher bestehenden Pflichten zur Nachhaltigkeitsberichterstattung in allen Belangen: (1) In der EU steigt die Zahl der berichtspflichtigen Unternehmen von 12.000 auf 50.000, (2) die Berichtsinhalte in den Bereichen „E“, „S“ und „G“ werden inhaltlich deutlich ausgedehnt und über verbindliche Berichtstandards vereinheitlicht, und sie werden (3) durch externe Prüfer mit steigender Anforderung (von „Limited Assurance“ zu „Reasonable Assurance“) geprüft. Die Berichterstattung wird ferner in den Lagebericht des Unternehmens/Konzerns aufgenommen und muss in einem einheitlichen Format (ESEF) auch maschinell auswertbar sein.

Die in der CSRD enthaltenen Regelungen zu den Inhalten der Berichte werden durch sog. ESRS-Guidelines ergänzt. Diese ESRS-Guidelines werden von der European Financial Reporting Advisory Group (EFRAG [www.efrag.org]) erlassen. Sie sollen ein einheitliches Format für die Berichterstattung in allen drei Bereichen (E, S und G) und für Industriesektor-spezifische Berichtspflichten gewährleisten. Dafür wird eine sogenannte „Berichtsmetrik“ aufgebaut, die in zwei übergreifenden Standards, fünf „E“-Standards, vier „S“-Standards sowie einem „G“-Standard über 100 konkrete Berichtsgegenstände beschreibt. Die Standards werden ihrerseits in „basis for conclusion papers“ (nach Art einer Gesetzesbegründung) erläutert werden. Einschließlich der Conclusion Papers und der Anhänge umfassen die ESRS-Guidelines mehr als 700 Seiten.

Börsennotierte Gesellschaften haben zudem den Deutschen Corporate Governance Kodex (DCGK) zu berücksichtigen, der in der Präambel klarstellt, dass einerseits Sozial- und Umweltfaktoren für den Unternehmenserfolg relevant sind und andererseits die Tätigkeiten des Unternehmens Auswirkungen auf Mensch und Umwelt haben (doppelte Wesentlichkeit). Beides ist im Rahmen des Unternehmensinteresses zu berücksichtigen. Konkrete ESG-Inhalte ergeben sich im DCGK insbesondere aus Grundsatz 3, den Empfehlungen A.1 und A.2 sowie aus Abschnitt G zur Vergütung.

4. Was hat dies nun mit Compliance zu tun? Bestehende Compliance-Organisationen werden – je nach Ausgestaltung – ein natürliches Interesse an einer ganzen Reihe von Berichtspflichten haben (müssen), da sie schon jetzt in ihre Zuständigkeit fallen. Dazu gehören – je nach Zuschnitt des Aufgabenbereichs der Funktion – im Bereich der „S“-Standards bspw. Berichtspflichten rund um Arbeitssicherheit, Arbeitnehmer- und Kundendatenschutz, Entgeltgleichheit, Anti-Diskriminierung oder Hinweisgeberkanäle. Der „G“-Standard betrifft Korruption und Lobbyismus. Hier werden auch Berichte über wesentliche Aspekte des Compliance Management Systems verlangt, einschließlich konkreter Darlegungen zu Unternehmenskultur, Unternehmensinternen Ermittlungen, Hinweiserschutzes oder Sanktionierungsmechanismen.

In den „E“-Standards werden umweltbezogene Berichtspflichten definiert. Vieles darin gehört heute nicht zum originären Aufgabenbereich einer Compliance-Organisation; das Umweltstrafrecht und die Produktsicherheit sind aber durchaus schon heute Themen, die für etliche Compliance-Organisationen bedeutsam sind.

Die Unternehmen sind außerdem gehalten, zu jedem Berichtsthema Ausführungen zur jeweiligen Risikosituation zu machen und darzulegen, welche Maßnahmen zur Risikosteuerung und Chancengenerierung getroffen wurden. Die Durchführung von Risikoanalysen und die Definition von risikominimierenden Maßnahmen gehören zum Standardrepertoire der Compliance-Organisationen, jedenfalls für bestimmte Themenfelder.

Es zeigt sich also, dass eine ganze Reihe der Berichtspflichten Bereiche berühren, die thematisch im Tätigkeitsbereich einer Compliance-Funktion liegen (können). Umgekehrt werden aber Risikofelder, die heutzutage durch Compliance-Organisationen bearbeitet werden (z.B. Kartellrecht, Außenwirtschaftsrecht oder Geldwäsche), von der Berichtspflicht – wenn überhaupt – nur am Rande erfasst.

Die Compliance-Funktionen haben in der Vergangenheit bewiesen, dass sie regulatorische Anforderungen im Unternehmen umsetzen können – unabhängig davon wie neu oder komplex diese Anforderungen sind. Die neuen ESG-Anforderungen unterscheiden sich insofern nicht von Herausforderungen in der Vergangenheit.

Drei bedeutende Unterschiede gibt es allerdings:

- a) Die ESG-Anforderungen haben einen direkten Einfluss auf die Unternehmensstrategie. Anders als die klassischen Compliance-Themen, wie Kartell- und Korruptionsvermeidung, geht es also nicht nur um Haftungsvermeidung und eine auf Integrität beruhenden Unternehmenskultur, sondern um die langfristige Existenzsicherung des Unternehmens und die Ausrichtung auf nachhaltige Produkte und Unternehmensführung.

- b) Daraus folgt unmittelbar, dass die Unternehmen noch nie so unter Zugzwang gesetzt wurden, wie jetzt. Die Unternehmensleitungen erkennen, dass die ESG-Anforderungen erhebliche Auswirkungen auf Investorenratings und auf andere Finanzierungsanforderungen haben. Es fehlt aber oft das Verständnis bei den Unternehmensleitungen, dass die ESG-Anforderungen auch erhebliche Haftungsrisiken beinhalten, die zum Teil über die Haftungsrisiken der klassischen Compliance-Felder hinausgehen.
 - c) Schließlich steigt die Transparenz ganz erheblich. Denn die nicht-finanzielle Berichterstattung muss in den Lagebericht aufgenommen werden, um sie der Finanzberichterstattung gleichzustellen. Nicht nur die Zahl der Berichtsthemen und die Berichtstiefe nehmen also zu. Die Unternehmen müssen letztlich auch ihre geschäftlichen (und gesellschaftlichen) Aktivitäten vor dem Hintergrund der zahlreichen ESG-Anforderungen rechtfertigen.
- 5. Schon heute ist es eine Mammutaufgabe für Unternehmen, Informationen zu Nachhaltigkeit zusammenzuführen. Aber das betrifft bislang nur eine überschaubare Anzahl von Informationen. Diese wird sich durch die Umsetzung der CSRD um den Faktor 30 erhöhen. Bisher ist in der Regel die Finanzfunktion mit der Aufgabe betraut, im Zusammenspiel mit vielen anderen Unternehmenseinheiten, die Finanzberichterstattung zu erstellen und im Zusammenhang damit auch die nicht-finanzielle Erklärung nach § 289 b ff., 315 ff. HGB zu veröffentlichen.
- 6. Die Herausforderungen einer zutreffenden und vollständigen Berichterstattung werden durch eine Vielzahl materiell-rechtlicher Fragen im ESG Kontext noch erweitert, etwa zu den rechtlichen Anforderungen an nachhaltigkeitsbezogene öffentliche Aussagen (Stichwort: Greenwashing), zur Auslegung und Umsetzung der Taxonomie-VO oder zum Verhältnis zwischen menschenrechtlichen Sorgfaltspflichten aus dem LkSG und Anforderungen aus (ebenfalls vom LkSG erfassten) Gesetzen zur Arbeitssicherheit und zu Arbeitsbedingungen. Schließlich wird die geplante Green Claims Directive die internen Prozesse zur belastbaren und damit rechtskonformen Kommunikation etwa umwelt- und klimabezogener Aussagen massiv verändern.
- 7. Für die Zukunft ergeben sich daraus rechtliche, praktische und organisatorische Fragen: In welchem Verhältnis steht die Berichterstattung nach CSRD zur bisherigen Berichterstattung von Compliance, IKS und Risikomanagement zu etwaigen Aussagen gegenüber dem Kapitalmarkt? Wie und durch wen sollen die Informationen, die für die Berichterstattung erforderlich sind, im Unternehmen eingesammelt, bewertet und zusammengeführt werden? Wie stellt ein Unternehmen bestmöglich sicher, dass die eingeholten Informationen richtig und belastbar sind? Wie geht man mit Haftungs-, Klage- und Reputationsrisiken um, falls die Berichterstattung nicht zutreffend ist (Klimaklagen, Greenwashing, Organhaftung usw.)? Werden die Klimaziele des Unternehmens sowie die sonstigen ESG-Anforderungen über den Code of Conduct oder sonstige unternehmensinterne Richtlinien abgesichert und was heißt das konkret für die Anwendung und Umsetzung der Taxonomie-VO? Ist jeder potenzielle Verstoß gegen das Verbot der Sonntagsarbeit ein Fall für den Menschenrechtsbeauftragten? Welche Aufgaben übernehmen in diesem breiteren Kontext die bereits bestehenden Governance-Funktionen, einschließlich der internen Revision?

Eine Antwort auf diese zahlreichen Fragen liegt in der Art und Weise, wie künftig die Governance im Unternehmen oder Konzern ausgestaltet wird. Es geht um den ESG-bezogenen Ordnungsrahmen oder mit anderen Worten um die **ESG-Governance**. Denkbar sind verschiedene Modelle: von mehreren nebeneinander bestehenden Governance-Systemen für einzelne Themenbereiche, über eine Lösung, in der ein Gremium ein ganzheitliches Governance-System für

die Organisation der zahlreichen Themen entwickelt und begleitet, bis hin zu einer übergreifenden Governance-Funktion für sämtliche dieser Themenbereiche. Will man nebeneinanderstehende, „unabhängig“ voneinander agierende Governance-Systeme, für die durch CSRD neu hinzukommenden Themen etablieren, muss man zusätzliche Verantwortungsbereiche schaffen.

Die Compliance-Funktion wird sich also erklären müssen, und sollte gemeinsam mit der Unternehmensleitung die Frage beantworten, welche Position sie in dieser künftigen Governance-Landkarte besetzen möchte:

- a) Möchte sie als „unabhängige“ Funktion ihre bisherigen Themen fortführen und neben den anderen Governance-Organisationen auf diese Themen beschränkt verantwortlich sein, ggf. auch in einer übergreifenden Rolle funktionelle Beiträge zu ESG-Themen liefern (**Kleine Lösung oder „Säulenmodell“**),
- b) oder möchte sie mehr Verantwortung auch für andere ESG-Themen und ggf. eine maßgebliche Funktion bei der Gesamtsteuerung der ESG-Organisation übernehmen (**Mittlere Lösung oder „Cross-Funktionales Modell“**),
- c) oder möchte sie sich an die Spitze der Bewegung setzen und das Thema ESG und die Organisationsverantwortung – mit oder ohne Gremium – insgesamt übernehmen (**Große Lösung oder „Gesamtsteuerungsmodell“**)?

Dabei geht es jeweils „nur“ um die Aufgaben des Risikomanagements und der Ordnungsfunktion auf Ebene der sog. 2nd Line. Dagegen abzugrenzen ist die unmittelbare Verantwortung zur Festlegung und Operationalisierung der Unternehmensstrategie, zur Einhaltung von CO²-Vorgaben oder für sonstige nachhaltigkeitsbezogene Aufgaben in operativen Einheiten. Diese Verantwortung muss selbstverständlich bei der Unternehmensführung bzw. bei den operativen Einheiten verbleiben.

8. Die nachfolgenden Abschnitte beschreiben diese drei Optionen mit ihrem jeweiligen Für und Wider. Diese Ausführungen sollen dabei helfen, für das eigene Unternehmen die richtige Lösung zu finden. Letztlich geht es darum, einen im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenen und wirksamen Ordnungsrahmen für das Thema ESG zu gestalten. Selbstverständlich sind Varianten dieser drei Optionen denkbar; sie erheben also keinen Anspruch auf vollständige Beantwortung der Fragestellung. Das Ziel ist Orientierung zu geben, wenn es um die Frage geht: Wer soll für Compliance im Unternehmen verantwortlich sein, wenn sich die Welt durch ESG verändert?

Hinweis zum Begriff „Governance“ in diesem Dokument bzw. im ESG-Kontext:

Der Begriff Governance wird in diesem Dokument bzw. im ESG-Kontext in doppelter Hinsicht wie folgt verwendet:

Das „G“ aus ESG steht im Folgenden für bestimmte inhaltliche Governance-bezogene Nachhaltigkeitsaufgaben bzw. -themen, wie etwa Grundsätze der Unternehmensführung, Vergütung, Diversität, Lobbying, Risikomanagement, Korruptionsbekämpfung. Die Themenliste orientiert sich am einschlägigen EFRAG Standard „G1“.

ESG-Governance meint hingegen den Governance- oder Ordnungsrahmen, also das gesamthafte Steuerungs- und Monitoring-System, um die Nachhaltigkeitsziele gesamthaft zu etablieren, ihre Umsetzung abzusichern und darüber zu berichten.

B. Darstellung der Optionen

1. Säulenmodell, sog. kleine Lösung

a) Ausgangslage

Im umfassenden Sinne bedeutet Compliance die Einhaltung aller Gesetze sowie unternehmensinterner Richtlinien. Typischerweise fokussieren sich Compliance-Abteilungen beim Betrieb eines Compliance Management Systems (CMS) in der fachlichen Zuständigkeit auf bestimmte Kernrisikofelder (z.B. Korruptionsprävention, Kartellrecht, Geldwäsche etc.). Andere Compliance-Themenfelder werden hingegen typischer Weise (z.B. Steuern) oder je nach Ausgestaltung (z.B. Datenschutz, Sanktionen, Produkt- oder Arbeitssicherheit) von anderen Organisationseinheiten verantwortet. Ferner können bestimmte Elemente des CMS dabei auch für andere Themenfelder geöffnet werden. So können etwa regelmäßig über das Hinweisgebersystem auch Verdachtsmeldungen zu Verletzungen von Rechtsvorschriften abgegeben werden, die nicht im fachlichen Zuständigkeitsbereich der Compliance-Abteilung liegen. Diese werden dann an die zuständige Abteilung zur Bearbeitung weitergeleitet. Vor diesem Hintergrund differenziert das Säulenmodell bei ESG-Themen zwischen Aufgaben, die die Compliance-Abteilung als Bestandteil der eigenen Kernzuständigkeit begreift (typisch: „Korruptionsbekämpfung“), als „fremde“ Zuständigkeit in Dienstleistung mit übernimmt (Öffnung des Hinweisgebersystems auch für andere Themen) oder außerhalb ihres Aufgabenbereichs sieht (etwa „Einhaltung von Klima- und Umweltzielen“).

b) Das Säulenmodell

Beim Säulenmodell bleibt die bisherige Zuständigkeit der Compliance-Funktion im Wesentlichen unverändert. Die ESG-Governance wird neben dem bestehenden CMS (neu) in einer weiteren Säule der Unternehmensorganisation aufgebaut. Nur soweit zur Einrichtung der ESG-Governance-Themen oder Aufgaben betroffen sind, die in der Zuständigkeit des Compliance-Bereichs liegen, werden diese über das klassische CMS abgebildet. Die Compliance-Funktion und das CMS werden als Teil eines übergeordneten ESG-Management Systems verstanden. Zwischen der ESG und Compliance-Organisation werden vor allem formal-technische Schnittstellen geschaffen.

Dementgegen werden Compliance-Organisationen, die sich mit einem breiteren Verständnis als umfassender Governance-Gestalter verstehen oder Opportunitäten zum Wachstum suchen, eher eine bestimmende Rolle in einer integrierten Governance-Landschaft bevorzugen. Dafür mögen die „mittlere“ oder „große“ Lösung besser geeignet sein. Bestimmungsfaktor für die geeignete Lösung ist die Erwartungshaltung der Unternehmensleitung und das Selbstverständnis der eigenen Funktion, wie auch jenes anderer Governance-Funktionen (Risikomanagement, Interne Kontrollen). Relevant sind aber auch Faktoren wie Ressourcenverfügbarkeit, allgemein bestehende Organisationsmerkmale im Unternehmen, Funktionalitätsfragen oder auch die strategische Ausrichtung und Maturität des CMS.

c) Grundlagen

Die Korruptionsbekämpfung ist und bleibt das klassische Compliance Thema, das zugleich auch ein ESG-Thema ist. Sie wird wie gehabt vom Compliance-Bereich verantwortet. Alle Maßnahmen zur Prävention, Aufdeckung und Reaktion liegen in der Zuständigkeit des Compliance-

Bereichs. Soweit Kennzahlen zum Thema Korruptionsbekämpfung für die ESG-Berichterstattung relevant sind (vgl. Disclosure Requirements G1-3 und 4 des ESRS G1 „Business Conduct“), werden diese vom Compliance-Bereich an den ESG- bzw. Berichtsverantwortlichen gemeldet.

Daneben gibt es CMS-Elemente, die von ihrer Natur her bereits typischerweise breiter angelegt sind und auch Themen erfassen, die außerhalb der fachlichen Kernzuständigkeit der Compliance-Abteilung liegen (z.B. Öffnung des Hinweisgeberverfahrens für alle Rechtsverletzungen).

Das führt beim Säulenmodell dazu, dass grundsätzlich sämtliche Governance- und Risikomanagement-Elemente, die inhaltlich (etwa Klimaschutz) oder strukturell (etwa ESG-Kontrollen und Berichterstattung) über das bereits bestehende klassische CMS hinausgehen, außerhalb des Compliance-Bereichs verantwortet werden.

Etwas anderes gilt nur dann, wenn es nicht sinnvoll ist, für strukturell ähnlich gelagerte Fallkonstellationen mehrere Parallelsysteme vorzuhalten. Es ist z.B. nicht sinnvoll, für verschiedene Rechtsgebiete mehrere unternehmenseigene Hinweisgebersysteme parallel zu betreiben (soweit es um die Verletzung materieller Rechtsnormen geht) oder eine Third-Party-Due Diligence mehrfach bzw. getrennt voneinander durchzuführen.

Im Säulenmodell nimmt Compliance grundsätzlich keine übergreifenden Ordnungs-, Governance- bzw. Assurance-Funktion zu ESG-Themen wahr. Alle ESG-Aufgaben mit einer fachlich-inhaltlichen Schwerpunktsetzung außerhalb der klassischen Compliance-Zuständigkeit werden auch außerhalb von Compliance verantwortet (z.B. klimaschutzbezogene Kommunikation, allgemeine ESG-Awareness und Trainings, interne Untersuchungen, die nicht-finanzielle Berichterstattung und entsprechende Kontrollen sowie eine ESG-bezogene Risikoanalyse). Die Zusammenführung der Informationen für die erforderliche Berichterstattung sowie die Überwachung der Einhaltung der ESG-Anforderungen erfolgt durch andere Stellen im Unternehmen.

In einem ggf. übergeordneten ESG-Risiko-Board sollte Compliance jedoch mit einem Sitz vertreten sein, um den Austausch und die Schnittstellen effizient zu behandeln und weitere Entwicklungen gesamthaft im Blick zu behalten.

d) Organisation von ESG im Unternehmen

Die Gesamtverantwortung für die ESG-Strategie und die Implementierung des Themas im Unternehmen trägt die Unternehmensleitung. Aufgabe der Unternehmensleitung ist es u.a., mit Blick auf den Umfang der Geschäftstätigkeit und die spezifische Risikosituation des Unternehmens eine sachgerechte und effiziente Aufgabendelegation vorzunehmen.

Soweit der ESG-Ordnungsrahmen auf bestehenden Abteilungsstrukturen aufsetzt, sind Schnittstellen vor allem zu den folgenden Unternehmensfunktionen zu definieren: Compliance, Einkauf, Personalbereich, Risikomanagement, Rechnungslegung, interne Kontrollen, interne Revision und – soweit vorhanden – zum Bereich für Nachhaltigkeit. Alle diese Bereiche verantworten einzelne ESG-Teilaufgaben. Im Säulenmodell ist daher vom Unternehmen (d.h. unmittelbar von der Unternehmensleitung oder von einer dazu bestimmten „ESG-Abteilung“) durch geeignete Prozesse festzulegen, wie aus diesen Abteilungen die für die ESG-Berichterstattung und Steuerung relevanten Informationen zusammengetragen und verwertet werden. Details dazu sollen hier nicht weiter vertieft werden.

Betrachtet man diese Aufgabenzuordnung mit Blick auf das sog. 3-Lines-bzw. 3-Lines-of-Defense-Modell, so sind die Compliance-Aufgaben wie bisher auch weitgehend auf der zweiten Linie zu verorten. Für das Thema ESG, also den im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenen und wirksamen ESG-Ordnungsrahmen, trägt allerdings nicht Compliance, sondern die dafür von der Unternehmensleitung bestimmte Abteilung (oder auch ein Gremium, wie etwa „Sustainability Board“) die gesamthafte Verantwortung.

e) Zuordnung spezifischer ESG-Zuständigkeiten

Nachfolgend wird anhand typischer ESG-bezogener Aufgaben illustriert, wie im Säulenmodell die Themen- und Aufgabenzuordnung in der zweiten Verteidigungslinie erfolgen könnte. Dabei wird zwischen den übergeordneten Aufgaben „Risikoanalyse, Prävention sowie Aufklärung und Reaktion unterschieden.

	Risikoanalyse	Prevent	Detect/Respond
Menschenrechte / LkSG	ESG-Owner / Compliance	ESG-Owner / Compliance	ESG-Owner, bei (bestimmten) Rechtsverletzungen ggf. zusammen mit Compliance
Korruptionsbekämpfung	Compliance	Compliance	Compliance
Anti-Diskriminierung	HR	HR	HR, bei (bestimmten) Rechtsverletzungen ggf. zusammen mit Compliance
Arbeitsschutz	HR	HR	HR, bei (bestimmten) Rechtsverletzungen ggf. zusammen mit Compliance
Klimaziele	ESG-Owner	ESG-Owner	ESG-Owner

f) Öffnung multifunktionaler CMS-Elemente für ESG-Themen

Neben die Frage, wie und an wen im Unternehmen die ESG-Themen zugeordnet werden, tritt auch im Säulenmodell die Überlegung, inwieweit die Compliance-Funktion ihr CMS für einzelne ESG-Themen öffnen sollte, um Synergieeffekte zu heben und die Prozessexpertise der Compliance-Abteilung zu nutzen. Die folgenden Bestandteile und Elemente des CMS kommen dafür in Betracht:

- Maßnahmen zur Prägung der Unternehmenskultur (Awareness für ethisches Verhalten, Integrität und Werte)
- Verankerung einzelner ESG-Anforderungen im Code of Conduct

- Risikoanalyse: Ggf. Öffnung für die Erfassung weiterer Risiken (etwa zum Thema Menschenrechte), soweit dies im Rahmen des bestehenden Systems effizient ist (z.B. Risikoanalyse im eigenen Geschäftsbereich unter Einbindung der lokalen Compliance-Officer). Hinweis: hier besteht eine Schnittstelle zur mittleren Lösung, s.u.
- Richtlinien: Ergänzung eines Bekenntnisses zu Menschenrechten und Nachhaltigkeit in nachgelagerten Richtlinien (ggf. unter Verweis auf eine menschenrechtliche und umweltbezogene Grundsatzerklärung)
- Trainings: Technische Plattform kann zur Verfügung gestellt werden. Inhaltlich kann eine Grundsensibilisierung zu ESG in einem zentralen Training zum Code of Conduct erfolgen
- Beratung: Verständnis zu Governance-Prozessen (3-Lines-Modell; Funktionstrennung; ESG-Grundlagen)
- Hinweisgebersystem: Öffnung für sämtliche Rechtsgebiete zur Vermeidung mehrerer parallellaufender Systeme durch Öffnung des Portals
- Interne Untersuchungen/Case-Management: Fokus bleibt bei den vom CMS umfassten Rechtsgebieten. Ansonsten erfolgt grundsätzlich eine Weiterleitung der Hinweise an andere Abteilung (Fachabteilung oder Revision). Im Einzelfall kann selbstverständlich je nach Ausrichtung/Expertise der Compliance-Abteilung auch eine Untersuchung von Hinweisen zu anderen Themengebieten erfolgen. Omnizuständigkeiten sollten allerdings vermieden bzw. nur bei entsprechenden Prozessen und Ressourcen übernommen werden. Hinweis: Für die Zukunft stellt sich auf dieser Basis dann für Hinweise etwa auf Greenwashing beim Säulenmodell die Frage, wer diese kompetent untersuchen soll und wie sich der Aufbau mehrerer im Unternehmen für interne Untersuchung zuständiger Stellen vermeiden lässt. Bei technischen Fragen (etwa zur Erreichung von CO² oder Klimazielen) stellt sich zudem die Herausforderung, dass ESG-relevante fachliche Bewertungen regelmäßig nur unter Hinzuziehung fachlich zuständiger ESG-Experten möglich sein werden.
- Berichterstattung: Compliance liefert im Rahmen der eigenen Befassung an den übergeordnet für ESG zuständigen Bereich zu.

g) Zusammenarbeit und Schnittstellen bei ESG

Im Säulenmodell sind die oben aufgezeigten Schnittstellen zwischen Compliance und ESG in Bezug auf die relevanten Aufgaben, (IT-)Prozesse sowie Abteilungen zu definieren. Entsprechende Regelungen sind zu verabschieden bzw. Service- und Schnittstellenvereinbarungen sind abzuschließen.

Die Einrichtung eines übergeordneten ESG-Boards erscheint zum Erfahrungs- und Wissensaustausch sowie Schnittstellenmanagement sinnvoll. Zudem sind die unterschiedlichen ESG-bezogenen Berichte abzustimmen und zu konsolidieren. Die Compliance Funktion sollte in einem solchen Gremium vertreten sein, wäre bei der „kleinen Lösung“ aber nicht im Lead.

h) Budget/Ressourcen

In der kleinen Lösung gibt es grundsätzlich keinen Bedarf für ein zusätzliches ESG-Budget im Compliance-Bereich, da sich die bestehenden Aufgaben materiell kaum erweitern. Denkbar ist, dass durch die ESG-Berichterstattung (vgl. ESRS G1 „Business Conduct“) ausgelöste Mehrarbeit nicht durch die bestehende Ressourcensituation abgedeckt werden kann. In solchen Fällen kann also Aufstockungsbedarf bestehen.

Bei einer Gesamtbetrachtung aus Unternehmenssicht ist der Budget- und Ressourcenbedarf gegenüber der mittleren oder großen Lösung wahrscheinlich erhöht, da neben dem CMS neue und möglicherweise auch parallellaufende Strukturen aufgebaut werden müssen und mögliche Synergien schwerer zu heben sind.

i) ESG-Berichterstattung/Ratings

Die ESG-Berichterstattung findet bei der kleinen Lösung nicht in der Verantwortung der Compliance-Organisation statt. Compliance liefert lediglich fachlichen Input in diese Berichterstattung zu.

j) Umsetzung, Weiterentwicklung und Ausblick

Die Unternehmensleitung wird sich die Frage stellen und definieren, ob sie die Compliance-Funktion als Bestandteil eines übergreifenden ESG-Management-Systems sieht oder ESG und CMS (mit der beim Säulenmodell unterstellten klassischen Themenzuordnung) unter Berücksichtigung der aufgezeigten Schnittstellen nebeneinander bestehen. Tendenziell werden dabei die ESG-Themen und Abteilungen aufgrund der zunehmenden inhaltlichen Tiefe und zur Erfüllung steigender Berichterstattungspflichten gestärkt werden. Compliance fokussiert sich dagegen auf die bestehenden Themenfelder.

In einer „modernen“ und auf Synergien angelegten integrierten Governance-Landschaft, die optimaler Weise auf einer integrierten IT-Infrastruktur arbeitet, erscheint die „stand alone“ Lösung im Säulenmodell nachteilig. Sie wird bei weiter aufkommenden regulatorischen Anforderungen zu erheblichen Mehraufwendungen und zusätzlichen Komplexitäten führen. Dies gilt allerdings nicht unumschränkt für sämtliche Unternehmen. Je nach Umfang der Geschäftstätigkeit und Risikolage des Unternehmens wird sich auch eine ESG-Organisation sehr schlank darstellen können. Hier sind weniger Synergien zu erwarten, weil die vielgestaltigen ESG-Themen ohnehin deutlich stärker gebündelt werden können. In solchen Fällen kann das Nebeneinander zweier kleiner (ESG- und Compliance-)Organisationen mit gut definierten Schnittstellen der Zusammenarbeit auch eine tragfähige Herangehensweise sein.

2. Cross-funktionales Modell, sog. „Mittlere Lösung“

a) Ausgangslage

Die Ausgangslage hat sich zur „Kleinen Lösung“ im Säulenmodell nicht verändert. Im umfassenden Sinne bedeutet Compliance die Einhaltung aller Gesetze und unternehmensinterner Richtlinien. Typischerweise fokussieren sich die Compliance-Abteilungen auf den Betrieb des CMS mit fachlicher Zuständigkeit auf bestimmte Kernrisikofelder (z.B. Korruptionsprävention, Kartellrecht, Geldwäsche etc.). Andere Compliance-Themenfelder werden hingegen typischerweise (z.B. Steuern) oder je nach Ausgestaltung (z.B. Datenschutz, Sanktionen, Produkt- oder Arbeitssicherheit) von anderen Organisationseinheiten verantwortet.

Allerdings öffnet sich das CMS auch für andere Themenfelder und übernimmt abgestuft entweder partiell oder als Owner die Verantwortung. Dies ist teilweise bereits beim Säulenmodell (also bei der „kleinen Lösung“) der Fall, etwa in Bezug auf „multifunktionale“ Elementen des CMS. Beim cross-funktionalen Modell der mittleren Lösung vertieft sich dieser Ansatz: ESG-Themen werden nicht nur als eigene Aufgaben der Compliance-Abteilung im Bereich ihrer klassischen Kernzuständigkeiten begriffen (typisch: „Korruptionsbekämpfung“), sondern verstärkt auch cross-funktional für oder gemeinsam mit anderen Abteilungen abgedeckt.

b) Das cross-funktionale Modell

Im cross-funktionalen Modell integriert sich die Compliance-Abteilung nach Wertschöpfungsgesichtspunkten möglichst nahtlos in die ESG-Governance unter Nutzung des bestehenden CMS. Überall dort wo eine Wertschöpfung/Synergie möglich ist (insbesondere aufgrund der Governance- oder Prozess-Kenntnisse) wird Compliance die ESG-Governance Themen abbilden. Eine fließende Grenze liegt dort, wo inhaltliche Fachkenntnis neu erworben werden muss. Zwischen ESG und Compliance werden inhaltliche, aber auch formal-technische Schnittstellen geschaffen, abhängig von den jeweiligen „Roles & Responsibilities“.

Bestimmungsfaktor für die Aufgaben der Compliance Funktion ist maßgeblich der **integrative** Gedanke: Die Unternehmensleitung organisiert den Ordnungsrahmen in der Weise, dass unter Beachtung des Umfangs der Geschäftstätigkeit, der allgemeinen Organisationsmerkmale und der Risikolage Expertise, Erfahrungen sowie Ressourcenverfügbarkeit der involvierten Abteilungen und Bereiche cross-funktional mit größtmöglicher Effektivität und Effizienz genutzt wird. Dabei sind auch die strategische Ausrichtung und Maturität des CMS zu berücksichtigen.

c) Grundlagen

Die Compliance-Funktion nimmt vollumfängliche alle Aufgaben zu Aufbau und Betrieb des CMS im Bereich der klassischen Compliance-Felder wahr. Das gilt also auch für solche Aufgaben mit ESG-Bezug wie insbesondere Korruptionsbekämpfung und – je nach Ausgestaltung Menschenrechte (insoweit dem Säulenmodell entsprechend).

Darüber hinaus übernimmt die Compliance-Funktion einzelne zusätzliche Aufgaben auch für andere ESG-bezogene Themen und Prozesse, auch wenn die Gesamtverantwortung für diese Themengebiete (etwa Einhaltung Klimaziele, Sozialstandards, Arbeitssicherheit) nicht bei der Compliance Funktion liegt. Das heißt die Compliance-Funktion trägt zur funktionalen Integration/Verschränkung und damit auch zur Verankerung der Organisation im Netzwerk bzw. Gesamtkontext des Unternehmens bei.

Um zu identifizieren, welche Aufgaben das im Einzelnen sind, bietet sich eine Kompetenzanalyse der Compliance-Funktion an: Wo bestehen Stärken und Methodenkompetenz, auch im Vergleich zu anderen Abteilungen im jeweiligen Unternehmen?

Typische Beispiele für Stärken und Methodenkompetenz sind:

- Durchführung eines holistischen Risk Assessments nach einheitlicher Methodik (gleiche Metrik, Darstellung, einheitliche Berichterstattung) und Umsetzung unter Leitung der Compliance-Funktion (ein Fragebogen; ein Interview) und zwar auch für Compliance-fremde Themen. Die inhaltlichen Aspekte sind von der jeweiligen Expertenfunktion (etwa zur Einhaltung Klimaziele) beizusteuern.
- Durchführen von internen Untersuchungen zur Prüfung von ESG- Themen, z.B. Greenwashing Vorwürfen.

Die ESG-Governance und das CMS definieren beim cross-funktionalen Modell ihre Schnittstelle in der Weise, dass Compliance zwar „fachfremde“ Leistungen qua Methodenkompetenz zuliefert, aber weder für das Erreichen dieser Ziele noch für die Angemessenheit und Wirksamkeit des ESG-Ordnungsrahmens, inkl. der dafür aufgesetzten Kontrollstrukturen eine gesamthafte Verantwortung trägt. In Abgrenzung zur „großen Lösung“ überlässt Compliance mithin die Leitung und Organisationsverantwortung für die Einrichtung eines angemessenen und wirksamen Ordnungsrahmens für ESG auf der Second Line einer anderen Abteilung bzw. einem Gremium oder Netzwerk.

In einem ggf. übergeordneten ESG-Risiko-Board sollte Compliance gleichwohl in jedem Fall mit einem Sitz vertreten sein.

d) Organisation von ESG im Unternehmen

Die Organisation i.S.d. Organisationsverantwortung bleibt im cross-funktionalen Modell genauso unverändert wie im Säulenmodell:

Die Gesamtverantwortung für die ESG-Implementierung im Unternehmen trägt die Unternehmensleitung. Zu den Aufgaben der Unternehmensleitung gehört eine ordnungsgemäße Organisation des ESG-Ordnungsrahmens, inkl. wirksamer Delegation der jeweiligen Zuständigkeiten. Dabei ist der Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens zu berücksichtigen.

Soweit der ESG-Ordnungsrahmen auf bestehenden Abteilungsstrukturen aufsetzt, sind Schnittstellen vor allem zu den folgenden Unternehmensfunktionen zu definieren: Compliance, Einkauf, Personalbereich, Risikomanagement, Rechnungslegung, interne Kontrollen, interne Revision und – soweit vorhanden – zum Bereich für Nachhaltigkeit. Alle diese Bereiche verantworten einzelne ESG-Teilaufgaben. Auch im cross-funktionalen Modell ist daher vom Unternehmen (d.h. unmittelbar von der Unternehmensleitung oder von einer dazu bestimmten „ESG-Abteilung“) durch geeignete Prozesse festzulegen, wie aus diesen Abteilungen die für die ESG-Berichterstattung und Steuerung relevanten Informationen zusammengetragen und verwertet werden. Details dazu sollen hier nicht weiter vertieft werden.

Betrachtet man diese Aufgabenzuordnung mit Blick auf das sog. 3-Lines-bzw. 3-Lines-of-Defense-Modell, so sind die Compliance-Aufgaben wie bisher sowie analog zum Säulenmodell weiterhin auf der zweiten Linie zu verorten. Für das Thema ESG, also den im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenen und wirk-

samen ESG-Ordnungsrahmen trägt allerdings nicht Compliance, sondern die dafür von der Unternehmensleitung bestimmte Abteilung (oder auch ein Gremium, wie etwa „Sustainability Board“) die gesamthafte Verantwortung.

e) Spezifische ESG-Zuständigkeiten und Aufgaben der Compliance Funktion

Beim cross-funktionalen Modell macht eine ESG-themenbezogene Analyse und Zuordnung (vgl. für das Säulenmodell oben unter 2. e) wenig Sinn. Denn es liegt im Wesen des Modells und des integrativen Ansatzes, dass Compliance auf die eine oder andere Art bei jedem ESG-Thema involviert ist.

Daher bleibt es dabei, dass die Compliance-Funktion für die vom Unternehmen zugeordneten CMS-Themen die Verantwortung trägt. In Bezug auf weitergehende bzw. andere ESG-Aufgaben ist der Beitrag der Compliance-Funktion dagegen prozess- und aufgabenorientiert zu bestimmen:

- Maßnahmen zur Prägung der Unternehmenskultur (Awareness für ethisches Verhalten, Integrität und Werte)
- Der Code of Conduct sollte ein Dokument der Compliance-Funktion sein. Inhaltliche Beiträge anderer Funktionen sind zu integrieren. Umsetzungsmaßnahmen zum Roll-Out, zur inhaltlichen Verankerung und zur Verzahnung mit den Unternehmenswerten können von Compliance – ggf. gemeinsam mit anderen Abteilungen – durchgeführt werden.
- Risikoanalyse: Die Compliance-Funktion steuert ihre Prozess- und Methodenkompetenz zur Durchführung von Risk Assessments zu. Diese kann mit den bestehenden ESG-Ressourcen in diesem Bereich kombiniert bzw. integriert werden. Je nach Reifegrad der im Unternehmen bereits durchgeführten ESG-bezogenen Wesentlichkeits- oder Materialitätsanalyse liegt die Federführung in anderen Bereichen.

Die Zunahme gesetzlich vorgeschriebener Compliance-Risikoanalysen (neben der Pflicht zur Durchführung einer allg. Compliance-Risikoanalyse zur Bestimmung und Ausgestaltung des CMS sind für die Lieferkette §§ 3 Abs. 1 Nr. 1, 4 LkSG sowie für die Geldwäscheprävention des Güterhändlers §§ 4, 5 GwG zu nennen) sowie die Pflicht zur Durchführung einer doppelten Wesentlichkeitsanalyse (vgl. nur ESRS 1 General requirements, Ziffer 3) sollte als Chance genutzt werden, die unterschiedlichen Anforderungen zu analysieren und Gemeinsamkeiten zu identifizieren. Zur Sicherstellung von Effektivität und Effizienz der erforderlichen Prozesse sollten – soweit wie möglich – Vereinheitlichungen in puncto Methodik, Metrik, Kompetenzaufbau- und -entwicklung, Implementierungsprozessen und Berichterstattung vorgenommen werden.

- Richtlinien: Compliance kann die gesamthafte Verantwortung für das Regelungsmanagement übernehmen. Anders als beim Code of Conduct (gesamthafter Roll Out und Verankerung durch Compliance) verbleibt die Verantwortung zur Implementierung aber bei der für die jeweilige Regelung zuständigen Fachabteilung.
- Trainings: Die technische Plattform (etwa für E-Learnings sowie zur Teilnehmerbenennung sowie Teilnahmemessung und -kontrolle) kann von Compliance bereitgestellt und gepflegt werden. Auch die Trainingssteuerung kann auf ESG-bezogene Trainings, die über die CMS-Trainingsinhalte hinausgehen, durch die Compliance Funktion wahrgenommen werden, soweit nicht eine andere zentrale Stelle im Unternehmen diese Aufgabe innehat. Dadurch kann eine inhaltliche und organisatorische Bündelung, inkl. Aufwandsteuerung

erreicht und Synergien (etwa bei didaktischen Fähigkeiten) gehoben werden. Auch Abnutzungs- und Abstoßeffekte durch zu viele Trainings lassen sich so eher vermeiden. Die konkreten Trainingsinhalte sind selbstverständlich von anderen Abteilungen zuzuliefern.

- Hinweisgebersystem und Beschwerdeverfahren: Mit dem Ziel, möglichst nur ein System und einen Meldekanal betreiben zu müssen, können diese Prozesse für sämtliche Rechtsverletzungen geöffnet werden.
- Interne Untersuchungen/Case-Management: Auch bei internen Untersuchungen können Fachwissen und Ressourcen gebündelt werden, um Hinweisen auf Rechtsverstößen durch die Compliance-Abteilung prüfen und verfolgen zu lassen. Dabei geht es nicht nur um Synergien, sondern auch um einen risikoadäquaten Umgang mit Hinweisen, die ein erhebliches Schadenspotential beinhalten können. Insbesondere an Vorwürfe auf Greenwashing, Diskriminierung oder ähnliche ESG-bezogene Hinweise ist hier zu denken.
- Kontrollen/Audits: Compliance kann je nach Ausgestaltung und Durchdringungsgrad der Compliance-Funktion im Unternehmen durchaus Kontroll- und Monitoringaufgaben übernehmen, die über die vom CMS erfassten Themen hinausgehen. Denkbar sind insbesondere ESG-spezifische Audits, etwa zur anlassunabhängigen Identifizierung von Greenwashing Risiken, soweit hier nicht die interne Revision in der Federführung ist. Beim Monitoring und bei automatisierten Kontrollen liegt die Federführung regelmäßig beim nicht-finanziellen Internen Kontrollsystem. Compliance dürfte insoweit also eher eine ergänzende Aufgabe übernehmen.
- Berichterstattung:
 - Die Compliance-Funktion bleibt für den Compliance-Bericht bzw. die Compliance-Berichterstattung inhaltlich und organisatorisch zuständig.
 - Soweit Compliance-Inhalte in die interne oder externe ESG-Berichterstattung eingehen, verbleibt es bei einer Zuliefererrolle von Compliance: Die entsprechenden Informationen und Berichtsteile werden der übergeordnet für ESG bzw. für die nicht-finanzielle Berichterstattung zuständigen Abteilung zur Verfügung gestellt.
 - Gleiches gilt für Informationen und Daten, die die Compliance-Funktion erhält bzw. verantwortet, soweit sie für Systeme- und Prozesse zuständig ist, also etwa Trainingszahlen oder Ergebnisse aus Risk Assessments.
 - Darüber hinaus ist es zwar grundsätzlich denkbar, dass die Compliance-Funktion auch die gesamthafte Prozessverantwortung für die ESG-bezogene Berichterstattung übernimmt. Allerdings ist insoweit die Nähe zum Geschäftsbericht und zur Abschlussprüfung zu beachten. In aller Regel wird Compliance hier also lediglich Zulieferer des Rechnungswesens sein.

f) Zusammenarbeit und Schnittstellen bei ESG

Es liegt im Wesen des integrativen Ansatzes des cross-funktionalen Modells, dass es eine Vielzahl von Schnittstellen zu anderen Abteilungen gibt. Darin liegt im Sinne einer funktionierenden Netzwerkorganisation Stärke wie Schwäche der mittleren Lösung. Denn einerseits kann Wissen und Expertise ressourcenschonend gebündelt werden. Andererseits besteht das Risiko, dass Themen durch den Rost fallen oder aufwendige Prozesse und Abstimmungen zur Klärung der Zuständigkeiten zu Ineffizienzen führen.

Neben operativen Schnittstellen ist insbesondere auf eine gute Zusammenarbeit in folgenden Bereichen zu achten: Interne Revision bei Prüfungen und Kontrollen, Rechtsabteilung bei der Beurteilung und im Umgang mit Greenwashing, IKS-Abteilung im Bereich nicht-finanzieller Kontrollen, Risikomanagement bei der Durchführung von Risk Assessments, HR im Bereich der Trainingssteuerung oder bei Diversity und Anti-Diskriminierungsthemen.

Letztlich sind das keine neuen Herausforderungen, sondern Aufgaben, die aus dem Betrieb des CMS weitestgehend bekannt und eingefahren sein dürften. Allerdings führt die Komplexität und Weite der ESG-Themen zu steigenden Anforderungen an die Grundsätze guter Zusammenarbeit.

Um damit vernünftig umzugehen und die Themen- und Aufgabenvielfalt zu meistern, empfiehlt sich die Einrichtung eines übergeordneten ESG-Boards. Compliance sollte darin in jedem Fall vertreten, aber nicht im Lead sein.

g) Budget/Ressourcen

Im cross-funktionalen Modell gibt es grundsätzlich Bedarf für ein zusätzliches ESG-Budget im Compliance-Bereich, um übernommene Aufgaben auch erfüllen zu können. Zu berücksichtigen sind FTE und Sachkosten, insbesondere zur Ausweitung der Digitalisierung und Wahrnehmung der Prozesszuständigkeiten.

h) ESG-Berichterstattung/Ratings

Die Verantwortung für die ESG-Berichterstattung findet beim cross-funktionalen Modell nicht in der Verantwortung der Compliance-Organisation statt. Compliance liefert lediglich fachlichen Input in diese Berichterstattung zu (Einzelheiten s.o.). Das gilt für die interne wie externe Berichterstattung, wie auch für allfällige ESG-Ratingprozesse.

i) Umsetzung und Weiterentwicklung

Beim cross-funktionalen Modell hat sich die Unternehmensleitung dafür entschieden, ESG-bezogene Prozesse und Abläufe im Netzwerk zu lösen. Das führt nicht nur zu einer gewissen Komplexität in der Steuerung, sondern auch zu stärker verzahnten Governance-Systemen. Das CMS als Stand-Alone System bleibt zwar einerseits erhalten, andererseits führt die Übernahme weitergehender ESG-Aufgaben durch die Compliance-Funktion aber zwangsläufig zu einer Erweiterung des Kompetenzbereichs über die klassischen Compliance-Themen hinaus. Auch werden die IT-Infrastruktur und die Prozesse stärker integriert werden. Dementsprechend erfolgen Weiterentwicklung der Systeme, Investitionen und Ressourcensteuerung ebenfalls gesamthaft.

Das cross-funktionale Modell erscheint ideal um Compliance als wertschöpfenden Faktor, der allerdings nicht omnipräsent ist, zu etablieren und auch um das immer noch z.T. vorhandene „Polizeiimage“ der Compliance-Funktion zu ändern. In arbeitsteiligen Organisationen, sind bei einer mittleren Lösung Mehraufwendungen und zusätzliche Komplexitäten sicherlich nicht vermeidbar, aber besser durchsetzbar und nicht mit einem rein kompetitiven Ansatz anderen Abteilungen gegenüber belastet. Triebfeder des cross-funktionalen Modells sind jedenfalls Wertschöpfung, Systemintegration und Synergien, weil die vielgestaltigen ESG-Themen ohnehin deutlich stärker gebündelt werden müssen.

3. Gesamtsteuerungsmodell, sog. „große Lösung“

a) Ausgangslage

Die Ausgangslage des Gesamtsteuerungsmodells kann anders beschrieben werden als bei den anderen beiden Optionen: Hier geht es darum, dass das Unternehmen sich bereits dahingehend positioniert hat, dass Umfang, Vielschichtigkeit und Komplexität des Themas ESG eine umfassende Transformation der Governance des Unternehmens bedürfen. Dafür soll ein gesamthaft ausgerichteter ESG-Ordnungsrahmen geschaffen werden, der von einer dafür geeigneten Funktion einheitlich unter Einbezug anderer Governance-Systeme und Funktionen definiert, gesteuert und umgesetzt wird.

Die Gründe dafür im Einzelnen (vgl. dazu auch bereits die Erläuterungen oben in der Einleitung):

ESG und die damit verbundenen strategischen Zielsetzungen des Unternehmens verlangen eine chancen- und risikoorientierte Steuerung und eine am 3-Lines-Modell orientierte Aufbau- und Ablauforganisation.

Denn die Ausgangslage bei ESG unterscheidet sich nicht mehr von der Ausgangslage zur Sicherstellung finanzieller Ziele. Mehr noch: beide Themen und Ziele sind weitestgehend miteinander verwoben. Langfristiger Unternehmenserfolg ist weder ohne finanzielle Stabilität und Ertragskraft noch unter Missachtung der ESG-Ziele denkbar. Innovation ist stets zugleich Investment zur Erreichung finanzieller- wie ESG-bezogener Ziele.

Diese Ausgangslage hat durch die geänderte öffentliche Erwartungshaltung und den massiv veränderten Rechtsrahmen zu erweiterten Anforderungen an die Berichterstattung und zu einer erheblichen Ausweitung der materiellen Risikolage geführt. Infolgedessen wurden in vielen Unternehmen bereits entsprechende Anpassungen der Governance vorgenommen:

- Die nicht-finanzielle Berichterstattung ist der herkömmlichen finanziellen Rechnungslegung und Berichterstattung in Methode, Inhalt und Abschlussprüfung weitestgehend angenähert.
- Die Einrichtung eines angemessenen und wirksamen Internen Kontroll- sowie Risikomanagementsystem erfolgt, um gleichermaßen die finanziellen, wie die nicht-finanziellen Ziele langfristig abzusichern. Das Interne Kontrollsystem (im engeren Sinne) deckt dementsprechend sowohl die finanziellen wie auch die nicht-finanziellen Kontrollen ab.
- Bußgeld- und Haftungsrisiken sowie Gefahren für die Reputation des Unternehmens bestehen mit potenziell bestandsgefährdender Wirkung auch für Verstöße gegen ESG-Anforderungen. Das gilt für Verstöße gegen materielle Rechtsvorgaben (Menschenrechtsverletzungen, Greenwashing-Vorwürfe, klima- und umweltschädliches Verhalten), wie auch gegen entsprechende Berichterstattungspflichten. Dabei besteht häufig eine Wechselwirkung zwischen finanziellen und nicht-finanziellen Fehlincentivierungen, bzw. ein solcher Zusammenhang wird von Klägerseite vorgebracht (etwa bei den meisten Klimaklagen).
- Und schließlich: es geht stets um Unternehmenskultur und wertebasierte Unternehmensführung. Die damit verbundenen Fragen lassen sich nicht zwischen finanziellen und nicht-finanziellen Zielen differenzieren. Gute – im Sinne von legale, legitime und

an den Unternehmenswerten ausgerichtete – unternehmerische Entscheidungen basieren auf gleichen Handlungsmaximen und auf einer entsprechenden Haltung.

Vor diesem Hintergrund erscheint der Betrieb der Governance-Systeme mit einer Trennung zwischen finanziellen und nicht-finanziellen Risiken auf Dauer nicht nur ineffizient, sondern auch zu risikobehaftet. Denn genauso wie auf der operativen Seite ein untrennbarer Konnex zwischen finanziellen und nicht-finanziellen Zielen und Incentivierungen besteht, bedarf es auf der Ebene der 2nd Line einer unmittelbaren Verzahnung und einer weitgehenden Integration auf Ebene der Aufbau- und Ablauforganisation. Die Komplexität der Gesamthematik legt es zudem nahe, die Steuerung dieses Systems nicht einem Netzwerk unterschiedlicher Funktionen zu überlassen, sondern eine Funktion mit der Gesamtsteuerung und dem Monitoring der mannigfaltigen Aufgaben und beteiligten Abteilungen und Funktionen zu betrauen.

Damit ist auch eine Entscheidung gegen eine eigenständige – Stand-Alone agierende – Compliance-Funktion gefallen und es stellt sich die Frage, an welcher Stelle und mit welchen Aufgaben sich die (bisherige) Compliance-Funktion bei dieser Neuausrichtung wiederfindet. Anders als im Säulenmodell und beim crossfunktionalen Modell ist damit im Ausgangspunkt naheliegend, dass die Compliance-Funktion klassische Kompetenzen und Aufgaben (etwa Betrieb des CMS, inkl. Maßnahmen zur Korruptionsbekämpfung und zum Kartellrecht) nicht mehr in gleicher Weise fortsetzen wird. Stattdessen werden klassische Compliance-Themen und Aufgaben in weiterentwickelte Strukturen und Prozesse überführt und die Compliance-Funktion verändert grundlegende ihr Gesicht und ihren Charakter.

Unternehmen, die ihr CMS bereits in diese Richtung weiterentwickelt haben, nehmen daher auch eine Änderung der Funktionsbezeichnung vor, indem es keinen Chief Compliance Officer, sondern nur noch einen Chief Integrity, Chief Responsibility oder Chief Responsible Officer gibt.

b) Das Gesamtsteuerungsmodell

Das Gesamtsteuerungsmodell basiert auf der Annahme, dass Compliance als federführende Funktion einen gesamthaften ESG-Ordnungsrahmen definiert, aufbaut und betreibt, in den das bisherige CMS so weit wie möglich organisatorisch, prozessual und inhaltlich integriert wird. Diese ESG-Governance bzw. dieser ESG-Ordnungsrahmen wird nachfolgend als „Compliance & Sustainability Governance-Systems – CS GS“ (Arbeitstitel) bezeichnet. Das CS GS ermöglicht der Unternehmensleitung, die als Teil der Unternehmensstrategie definierten ESG-Ziele ganzheitlich, konsequent und kontinuierlich zu steuern und zu überwachen. Ferner werden die mit den unterschiedlichen ESG-Themen befassten Mitarbeiter bei der ordnungsgemäßen und effizienten Wahrnehmung ihrer Aufgaben unterstützt, wobei die Maßnahmen Teil einer wertebasierten ethischen Unternehmensführung sind. Das CS GS ist darauf ausgerichtet, ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames ESG-Governance-System einzurichten und zu betreiben. Gleichzeitig basiert das CS GS vor dem Hintergrund der beschriebenen Ausgangslage auf einem holistischen Ansatz, der die Governance zwischen finanziellem und nicht-finanziellem Risikomanagement effektiv verzahnt.¹

¹ Vgl. zu diesem Ansatz auch die folgenden Veröffentlichungen: The Rise and Role of the Chief Integrity Officer, White Paper des World Economic Forum, Dezember 2021; MIT Sloan Management Review/Malan, *Taylor/Tunkel/Kurtz*, 07/2022; Pikó/Uhl *Schweizer Handbuch Compliance/Rita Pikó/Laurenz Uhl* § 1 Rn. 56 ff.; Pikó/Uhl *Schweizer Handbuch Compliance/Viviane Gehri-Burkhardt* § 14 Rn. 27 ff.

Bestimmungsfaktor für die Aufgaben der Compliance-Funktion ist maßgeblich ein gestaltender und steuernder Gedanke: Die Unternehmensleitung richtet ein CSGS unter Leitung der Compliance-Funktion ein, um die Steuerung und das Monitoring der unterschiedlichen ESG-Aufgaben und Themen gebündelt an einer Stelle durch eine gesamthaft und auch in Bezug auf finanzielle Risiken holistisch agierende Funktion sicherzustellen. Compliance agiert als „THE Assurance Function“ des Unternehmens und bringt für diese Aufgabe die zur Leitung komplexer Governance-Systeme und zur effektiven unternehmensweiten Zusammenarbeit mit anderen Funktionen und Abteilungen erforderliche Expertise, Erfahrungen sowie Ressourcen ein. Eine derart weitreichende Transformation der Compliance-Funktion wird regelmäßig nur dann gelingen, wenn bereits ein reifes und im Unternehmen sowie bei weiteren Stakeholdern akzeptiertes CMS vorhanden ist.

c) Grundlagen

Zielsetzung des Gesamtsteuerungsmodells ist der Aufbau und Betrieb eines gesamthaften „Compliance & Sustainability Governance-Systems – CSGS“. Das CSGS ermöglicht der Unternehmensleitung, die als Teil der Unternehmensstrategie definierten ESG-Ziele konsequent und kontinuierlich zu überwachen und zu steuern.

Im Unterschied zum Säulenmodell und zum cross-funktionalen Modell geht die „große Lösung“ von der Annahme aus, dass durch die Umsetzung eines gesamthaften CSGS im Unternehmen ein Prozess in Gang gesetzt wird, in dessen Verlauf es keine eigenständige Compliance-Funktion im bisherigen Sinne mehr gibt. Compliance muss sich daher diesem Entwicklungsprozess stellen und ein aktiver und zentraler Bestandteil davon werden.

Die gute Nachricht ist: die Compliance-Funktion hat alles, was sie dafür braucht! Sie ist schon heute in der Regel die Funktion im Unternehmen, die in die gesamte Wertschöpfungskette, in alle zugehörigen Kern- und die Unterstützungsprozesse, hineinagiert.

Compliance hat die erforderlichen Fähigkeiten und Methodenkompetenz für das Design, die Umsetzung und das Monitoring eines CSGS. Damit ist die Compliance-Funktion auch gesamthaft in der Lage, die Angemessenheit und Wirksamkeit des Systems zur Umsetzung der ESG-Ziele zu überwachen und der Unternehmensleitung darüber zu berichten.

Die Compliance-Funktion schlüpft in der „großen Lösung“ gewissermaßen in die Rolle des Katalysators des CSGS. Die bisherigen Inhalte und Aufgaben der Compliance-Funktion gehen dabei im CSGS auf. Die Zusammenarbeit zwischen unterschiedlichen Abteilungen, die einen Beitrag zur ESG-Governance leisten, gewinnt an Bedeutung. Schnittstellen müssen für den Gesamtablauf des CSGS neu definiert werden.

d) Organisation von ESG im Unternehmen

Die Unternehmensleitung definiert Nachhaltigkeit als Teil der Unternehmensstrategie und bestimmt die ESG-Ziele für das Unternehmen. Dabei unterstützt Compliance, wie auch andere Fachbereiche, bei der Unternehmensleitung bei der Definition. Compliance achtet insbesondere darauf, dass die Unternehmensstrategie und die ESG-Ziele im Einklang mit gesetzlichen Vorgaben steht und realistisch umsetzbar ist.

Die Steuerung und Koordinierung der Umsetzung der ESG-Governance im Rahmen des CSGS erfolgt z.B. durch das „Sustainability Board“ (SB). Dieses Gremium berichtet direkt an die Unternehmensleitung und setzt sich als Kernmitglieder z.B. aus den folgenden Funktionen zusammen: Compliance, Strategie, Kommunikation, Rechnungswesen/Berichterstattung, Recht, Personal sowie ggf. technische Abteilungen mit entsprechender Nähe zu Klima- und Umweltzielen. Ein Fokus des SB liegt auf der Sicherstellung ordnungsgemäßer und damit angemessener und wirksamer ESG-Governance. Daher bietet es sich mit Blick auf die Rollenverteilung beim Gesamtsteuerungsmodell an, dass die Compliance-Funktion die Leitung des SB übernimmt.

Die Operationalisierung der ESG-Ziele in der „1st Line“ erfolgt durch die operativen Unternehmensbereiche und Abteilungen und wird etwa durch die Strategieabteilung gesamthaft gesteuert. Diese übernimmt auch die entsprechende Berichterstattung an den Vorstand. Compliance verantwortet hier als zuständige Abteilung die typischen, operativen Aufgaben, wie Korruptionsbekämpfung, etc.

Auf Ebene der 2nd Line des CSGS übernimmt die Compliance-Funktion (zusammen mit anderen Governance-Funktionen, wie bspw. IKS) nicht nur die Befähigung der Mitarbeitenden zur Erfüllung der ESG-Anforderungen, sondern insgesamt die Governance und das Monitoring. Basis ist ein zu definierender angemessener Kontrollrahmen für alle ESG-Aufgabenbereiche. Bei der Berichterstattung an den Vorstand legt Compliance den Schwerpunkt auf die Angemessenheit und Wirksamkeit des CSGS. Dazu kann auch die Validierung der für (externe) ESG-Ratings bereitgestellten Informationen gehören, soweit dies nicht im Rahmen der nicht-finanziellen Berichterstattung und der Abschlussprüfung erfolgt.

Wesentliche Schnittstellen bestehen auf der 2nd Line zum IKS und der entsprechenden IKS-Abteilung, zum Rechnungswesen und den Prozessen der finanziellen und nicht-finanziellen Berichterstattung als Brückenkopf zum Abschlussprüfer, zum Risikomanagement nach § 91 Abs. 2 bzw. nach § 91 Abs. 3 AktG (für börsennotierte Gesellschaften). Weitere wesentliche Schnittstellen sind zu definieren zur Strategieabteilung (Ausgestaltung und Operationalisierung der strategischen [ESG]-Ziele), Kommunikation (Vermittlung der Unternehmensstrategie und der Nachhaltigkeitsziele) und zur Rechtsabteilung (Rechtsberatung, etwa zur Vermeidung von Greenwashingrisiken bei öffentlichen Aussagen, Prüfung/Abwehr entsprechender Ansprüche). Mit Blick auf die geplante Green Claims Directive der EU Kommission sind weitere erhebliche Änderungen nicht nur des Rechtsrahmens, sondern auch der darauf zugeschnittenen Aufbau- und Ablauforganisation absehbar, etwa: interne Vorvalidierung zur Einhaltung der Vorgaben der Green Claims Directive, Schnittstelle zum (externen) Verifier gem. Art. 10, 11 der Directive (Entwurfssfassung vom 22.03.2023).

Auf Ebene der 3rd Line trägt die Interne Revision durch unabhängige ESG-spezifische Prüfungen zur Entwicklung und Umsetzung des CSGS bei. Ausgangspunkt für die Prüfungsplanung ist eine enge Zusammenarbeit mit dem SB.

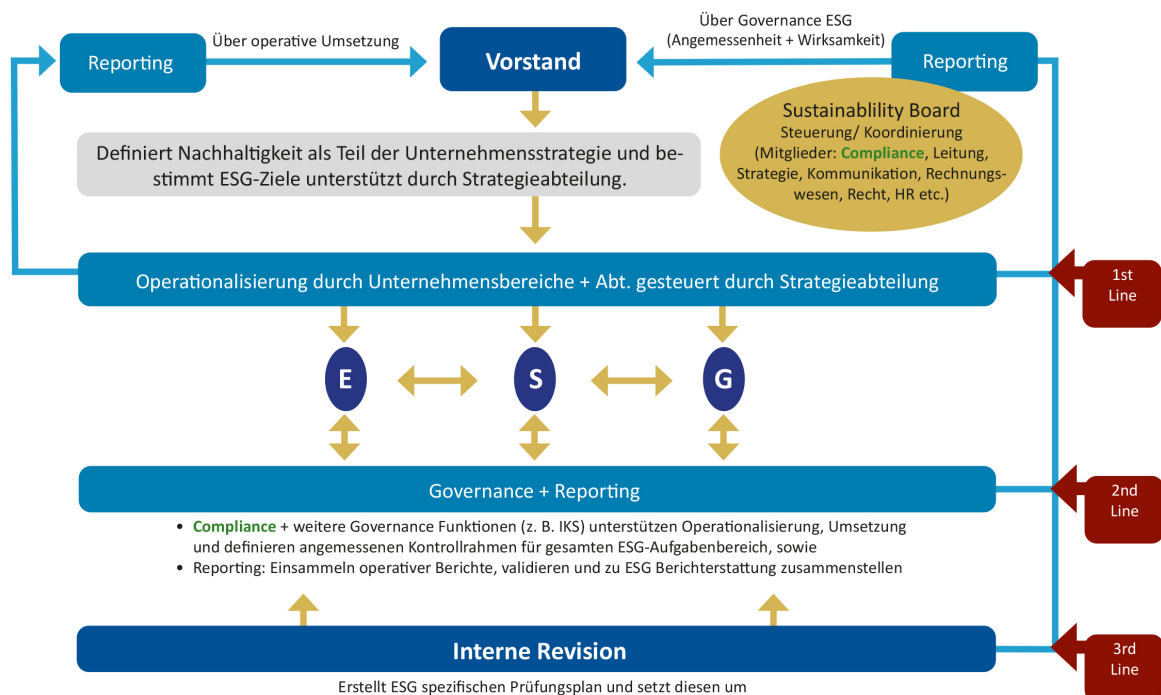


Abbildung 2: Umsetzung ESG im Unternehmen und CSGS

e) Spezifische ESG-Zuständigkeiten und Aufgaben der Compliance-Funktion

Die spezifischen ESG-Zuständigkeiten und Aufgaben der Compliance-Funktion verteilen sich beim Gesamtsteuerungsmodell vor allem auf die Begleitung der operativen Umsetzung spezifischer ESG-Themen (etwa Korruptionsbekämpfung) und die übergeordnete Governance, einschließlich Monitoring.

Zunächst überführt die Strategieabteilung die ESG-Ziele in Zusammenarbeit mit dem SB in konkrete Aufgaben und KPIs für die zuständigen Abteilungen im Unternehmen (1st Line). Die Auswahl der Themen orientiert sich dabei zum einen an externen Vorgaben aus aktuellen (Branchen-)Standards und relevanter Regulierung (insb. EFRAG-Standards). Zum anderen müssen die internen Rahmenbedingungen und organisatorischen Möglichkeiten berücksichtigt werden.

Der überwiegende Teil der fraglichen Themen und Aufgaben sind bereits in der Organisation operativ zugeordnet. Daher kann es sinnvoll sein, diese Zuordnung im Sinne einer gesamthafte ESG-Umsetzung zu überprüfen und soweit nötig neu zu gestalten. Denn die Zusammenarbeit zwischen den Abteilungen ist zu intensivieren und klassische Abgrenzungen in den Zuständigkeiten sind weiterzuentwickeln.

Für die Compliance-Funktion kann es bspw. bedeuten, dass sie gemeinsam mit dem Einkauf, mit HR sowie mit den für Arbeitssicherheit und Gesundheitsschutz zuständigen Abteilungen die Aufgabenverteilung für das Thema „Sozialstandards in der Lieferkette“ überprüft und anpasst. Zu beachten sind die Grundprinzipien des 3-Lines Modells mit einer von der 1st zur 2nd Line abgestuften Verantwortung für das Risikomanagement. Hinzu kommen praktische Unterschiede zwischen zentralen Stabsabteilungen, Werken und Produktionsanlagen, kleineren lokalen Organisationen sowie Schnittstellen zu externen Kooperationspartnern und Lieferanten.

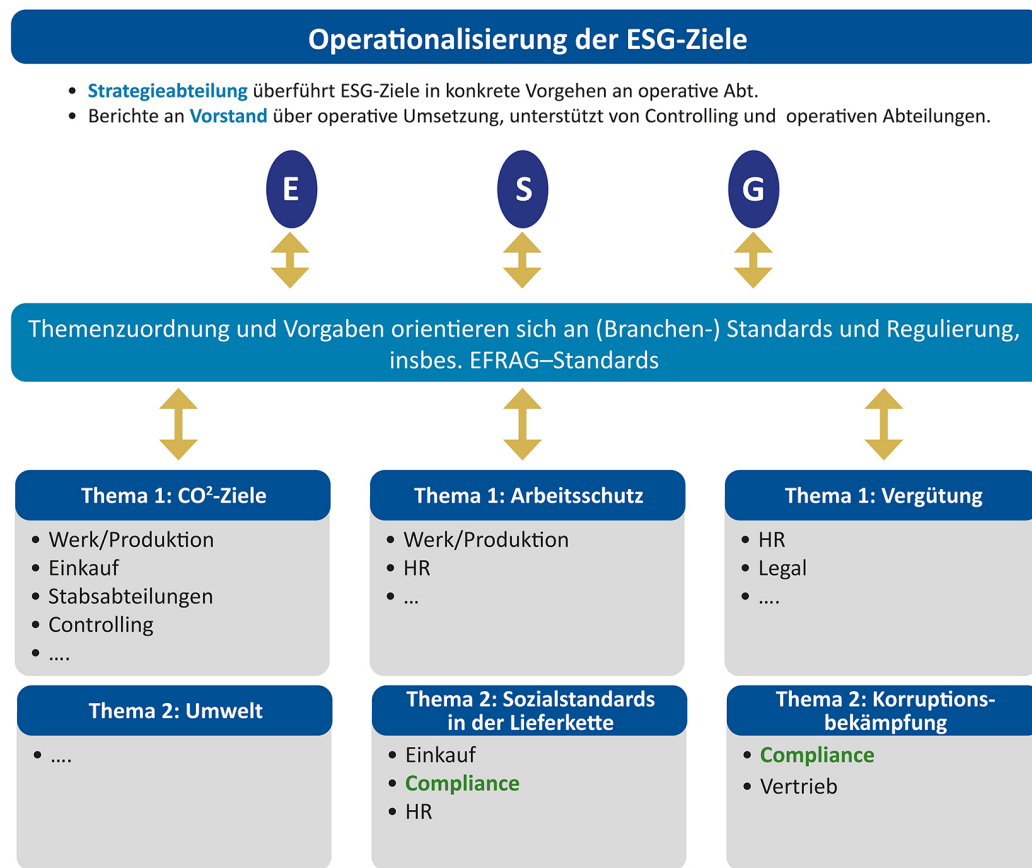


Abbildung 3: Zuordnung der Themen im Rahmen der ESG-Umsetzung

Die wesentliche Bedeutung der Compliance-Funktion für ESG zeigt sich in der „großen Lösung“ im Aufbau und Betrieb des erforderlichen Governance-Rahmens bspw. dem CSGS (2nd Line). Die im cross-funktionalen Modell dargestellten Vorschläge (vgl. oben 2) e)), an welchen Stellen die Compliance-Funktion spezifische ESG-Zuständigkeiten übernimmt und entsprechenden Mehrwert leisten kann, gelten vollumfänglich auch im Gesamtsteuerungsmodell.

Orientiert an dem bekannten Plan-Do-Check-Act- oder auch Prevent-Detect-Respond-Modell lassen sich für die „große Lösung“ vier Phasen oder Abläufe darstellen:

1. ESG-Design
2. Enable & Support
3. Monitoring & Control
4. Report & Act

Die Phasen sind als Kreislauf zu verstehen, der es dem Unternehmen ermöglicht, das CSGS kontinuierlich weiterzuentwickeln. Dieser Kreislauf wird von der Compliance-Funktion koordiniert und gesteuert.

1. ESG-Design

Die seitens der Unternehmensleitung festgelegten ESG-Ziele werden durch die Compliance-Abteilung in Zusammenarbeit mit den zuständigen Bereichen in einen angemessenen Regelungsrahmen überführt und in der Organisation verankert. In diesem Zusammenhang kann

eine entsprechende Pflichtendelegation erfolgen, die im Design und in der Umsetzung durch die Compliance Funktion betreut wird.

Auf Grundlage des ESG-Regelungsrahmen erfolgt unter Federführung der Compliance-Abteilung die regelmäßige Durchführung eines ESG-Risk-Assessments (vgl. dazu im Einzelnen bereits oben 2) e) zum cross-funktionalen Modell).

2. Enable + Support

Die Ergebnisse des ESG-Risk-Assessments werden von der Compliance Funktion zur Entwicklung bzw. Weiterentwicklung ESG-spezifischer Maßnahmen im Rahmen des CS GS genutzt. Die Schwerpunkte können dabei durchaus analog zum CMS und ganz ähnlich wie beim cross-funktionalen Model (oben 2) e)) bestimmt werden:

- ESG-Kultur und der erforderliche Tone from the Top
- Awareness- und Kommunikation (insb. Schulungen) sowie Beratung und Unterstützung der Fachabteilungen
- Prozesslandschaft und IT-Tools, inkl. Einrichtung und Betrieb des ESG-Hinweisgebersystems

3. Monitoring & Control

Rückgrat für das Monitoring und die Kontrolle des CS GS ist das (bestehende) nicht-finanzielle Interne Kontrollsystem (IKS), das entweder bereits im Unternehmen von einer entsprechenden Abteilung verantwortet und betrieben wird oder auf Grundlage des ESG-Regelungsrahmens (von der Compliance-Funktion in Zusammenarbeit mit der IKS-Funktion) zu definieren bzw. weiterzuentwickeln ist.

Mit Hilfe des Non-Financial IKS und ggf. weiterer Maßnahmen erfolgt das laufende Monitoring und die Plausibilisierung zum einen der internen ESG-Vorgaben und zum anderen ggü. dem Abschlussprüfer und externen Berichterstattungs-Anforderungen und Ratings.

4. Berichterstattung & Maßnahmen

In der Berichterstattung fasst die Compliance-Funktion die Erkenntnisse aus Monitoring und Plausibilisierung zusammen, und liefert so der Unternehmensleitung ein umfassendes Bild zur Angemessenheit und Wirksamkeit des CS GS. Dazu kann auch eine Validierung der (externen) ESG-Berichterstattung bzw. der für externe ESG-Ratings zur Verfügung gestellten Informationen gehören, soweit dies nicht bereits Bestandteil der Rechnungslegung und Abschlussprüfung ist. Außerdem werden im Rahmen der Berichterstattung in Zusammenarbeit mit dem SB erforderliche Maßnahmen zur Weiterentwicklung und kontinuierlichen Verbesserung festgelegt.

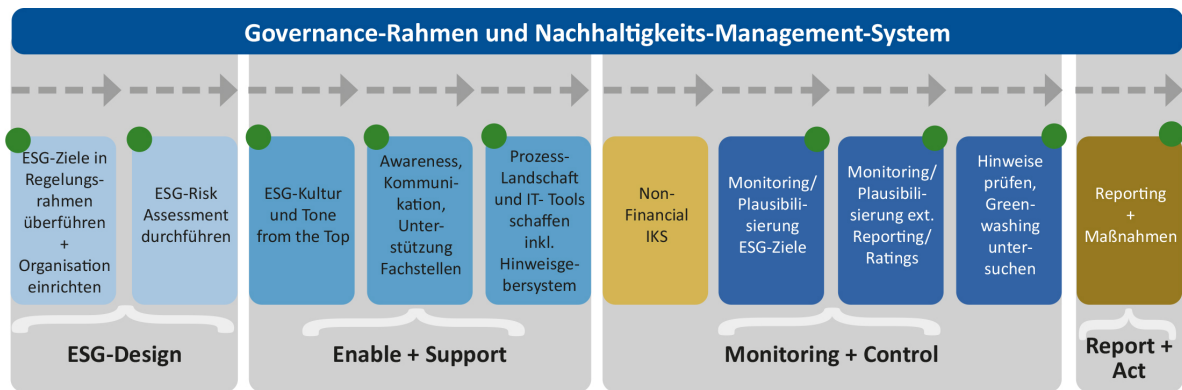


Abbildung 4: Vier Phasen-Modell CSGS

f) ESG-Kontrolle, Monitoring und Berichterstattung/Ratings

Im Gesamtsteuerungsmodell kommt der ESG-spezifischen Kontrolle, dem Monitoring und der Berichterstattung eine besondere Bedeutung zu. Und damit auch der Rolle der Compliance-Funktion.

Dabei gibt es zum einen das interne Monitoring der ESG-Zielerreichung, das über das Non-Financial IKS erfolgt und von der IKS-Abteilung gesteuert wird. Die Kontrollen selbst werden dabei von den Prozess-Ownern in den operativen Bereichen durchgeführt. Die Ergebnisse dienen der Strategieabteilung zum übergeordneten Review der ESG-Ziele bzw. deren Erreichung sowie der Berichterstattung darüber an die Unternehmensleitung. Auf dieser Grundlage trifft die Unternehmensleitung die erforderlichen Entscheidungen im Rahmen der Unternehmenssteuerung. Analog zum Financial-IKS prüft der Abschlussprüfer das Non-Financial-IKS im Rahmen der Jahresabschlussprüfung.

Auf der anderen Seite erfolgt das Monitoring der ESG-Ziele als Teil der externen ESG-Berichterstattung und für externe Ratings. Hier sind Validierung und Plausibilisierung von entscheidender Bedeutung, um Greenwashing und andere Verstöße zu vermeiden. Die Compliance-Funktion übernimmt daher die zentrale Aufgabe der Beurteilung der Angemessenheit und Wirksamkeit der ESG-Governance bzw. des CSGS und berichtet hierzu über das SB regelmäßig an die Unternehmensleitung. Hierzu kann sie selbst die Umsetzung einzelner Aspekte des CSGS überprüfen und durch externe, unabhängige Stellen überprüfen lassen.

In letzter Instanz erfolgt eine regelmäßige Berichterstattung zum Non-Financial IKS sowie der Angemessenheit und Wirksamkeit der ESG-Governance an den Aufsichtsrat bzw. den Prüfungsausschuss des Aufsichtsrates. Entweder durch die Unternehmensleitung oder das SB.

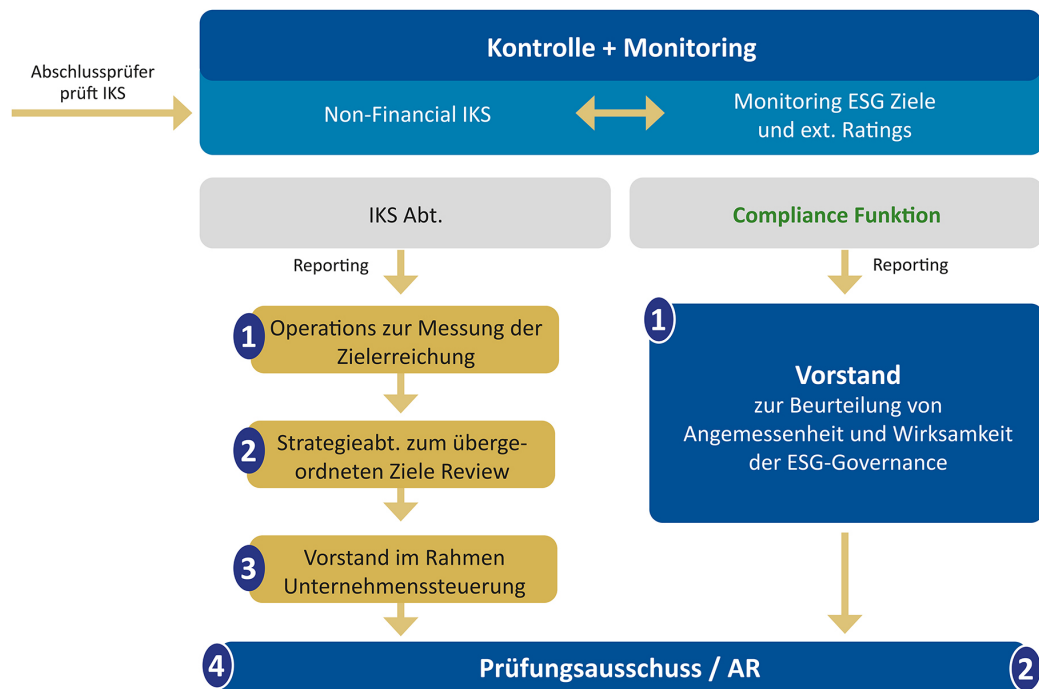


Abbildung 5: Kontrolle und Monitoring

g) Budget/Ressourcen

Zielsetzung der „großen Lösung“ ist der Aufbau und Betrieb eines gesamthaften „Compliance and Sustainability Management-Systems“ (CSGS). Die Compliance-Funktion schlüpft dabei in eine für sie neue, zentrale Rolle mit umfassender Verantwortung und vielfältigen Managementaufgaben. Voraussetzung dafür ist nicht nur ein eigenes Budget in ausreichendem Umfang. Auch personell muss die Compliance-Funktion über die bisherigen Umfänge hinaus ausgestattet werden und fachlich deutlich breiter besetzt sein. Auch wenn das Budget der Compliance-Funktion im Vergleich zum Säulenmodell oder dem cross-funktionalen Modell bei dem Gesamtsteuerungsmodell höher ausfallen wird, sollten sich aus Gesamtsicht erhebliche Synergien bilden, so dass die Gesamtkosten zur Umsetzung der ESG-Anforderungen nicht höher ausfallen sollten als in den oben genannten Optionen, und möglicherweise sogar niedriger sind.

C. Ausblick

DICO möchte mit diesem Positionspapier einen wichtigen Beitrag für die Praxis leisten. Unternehmen und ihre Compliance-Funktionen können – unabhängig von Größe, Reifegrad und Risikoprofil – auf Basis dieser Unterlage diskutieren und evaluieren, wie die Themen Compliance und ESG organisatorisch und inhaltlich aufgestellt und miteinander verzahnt werden sollen. Die Optionen sollen die Compliance-Funktionen dabei unterstützen, ihre Rolle beim Thema zu finden und einen größtmöglichen Mehrwert zu schaffen. Gleichzeitig ist das Positionspapier Startschuss für DICO, sich noch intensiver und strukturierter mit Compliance-Fragestellungen rund um das Thema ESG zu befassen. Der parallel zur Veröffentlichung des Positionspapiers gegründete DICO Arbeitskreis ESG wird dabei eine treibende und gestaltende Rolle einnehmen, um dieses dynamische Thema für DICO auch in Zukunft angemessen zu behandeln.

Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX- Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften, sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.



DICO – Deutsches Institut für Compliance

Bergstraße 68

D-10115 Berlin

info@dico-ev.de

www.dico-ev.de

