horn & company

GOVERNANCE UND RISIKOKULTUR IM FOKUS DER AUFSICHT

Ein Weckruf für die Branche: Der Fall Credit Suisse

Im März 2023 verschärfte sich die jahrelange Vertrauenskrise der Credit Suisse: binnen Tagen zogen Kunden in Panik massiv Gelder ab, der Aktienkurs brach ein, die Bank musste in einer Zwangsübernahme durch die UBS gerettet werden. Die Schweizer Finanzmarktaufsicht FINMA identifizierte in ihrem Bericht vom Dezember 2023 unter anderem tief verankerte Mängel in der Risikokultur der Bank als eine der Kernursachen des Kollapses. Etwa machten die Mosambik-Kredite, die Geschäftsbeziehungen mit den Greensill-Gesellschaften sowie mit dem Family Office Archegos Mängel im gruppenweiten Risikomanagement[1], im Risikomanagement und in der Betriebsorganisation[2] bzw. in der Organisation und dem Risikomanagement[3] sichtbar. Laut FINMA übernahmen die Führungskräfte keine klare Verantwortung und Eskalationsmechanismen funktionierten nur auf dem Papier. Warnsignale aus dem Risikomanagement wurden abgeblockt und Entscheidungswege blieben intransparent. Der Kollaps der Credit Suisse war damit nicht allein Folge externer Marktbedingungen, sondern Ausdruck struktureller Mängel in Governance, Kontrolle und Kultur. Die staatlich orchestrierte Notübernahme der Credit Suisse durch die UBS im März 2023 gilt als der bedeutendste Eingriff in eine systemrelevante Bank in Europa seit der Finanzkrise 2008 und brachte erhebliche Reputations- und Stabilitätsrisiken für das europäische Bankensystem mit sich.[4]

Governance und Risikokultur als zunehmender Prüfungsfokus

Mitunter durch die Krise der Credit Suisse rückte die Risikokultur in den vergangenen Jahren zunehmend in den Fokus der Aufsichtsbehörden.

Schon seit einiger Zeit betont die BaFin die Bedeutung einer risikobewussten Unternehmenskultur als wesentliches Steuerungselement. In den Mindestanforderungen an das Risikomanagement (MaRisk) wird die Geschäftsleitung verpflichtet, eine angemessene Risikokultur zu fördern und dauerhaft zu verankern. Sie müsse in der Lage sein, sämtliche Risiken zu erkennen, zu bewerten und geeignete Maßnahmen zu ihrer Begrenzung zu ergreifen. Zusätzlich ist jeder Geschäftsleiter innerhalb seines Zuständigkeitsbereichs verpflichtet, angemessene Kontroll- und Überwachungsprozesse sicherzustellen.

In seiner Sitzung im November 2024 gab das Fachgremium MaRisk zudem bekannt, dass es im 2. oder 3. Quartal 2025 eine Konsultation zu den „EBA-Leitlinien zu Internal Governance" geben soll. Inwieweit sich daraus Änderungsbedarf für die MaRisk ergibt, soll zu einem späteren Zeitpunkt geprüft werden.[5]

[1] Siehe etwa https://www.finma.ch/de/news/2021/10/20211019-mm-cs-mosambik/.
[2] Siehe etwa https://www.finma.ch/de/news/2023/02/20230228-mm-greensill/.
[3] Siehe etwa https://www.finma.ch/de/news/2023/07/20230724-mm-archegos/.
[4] https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/cs-bericht/20231219-finma-bericht-cs.pdf
[5] https://www.bafin.de/SharedDocs/Downloads/DE/Protokoll/dl_protokoll_FG_MaRisk_20241127_BA.pdf

Darüber hinaus erläuterte der BaFin-Präsident Mark Branson im Mai 2025, dass die Ursache der Schieflage einiger kleiner Banken in der letzten Zeit vermehrt Geschäfte waren, deren Risiken sie nicht verstanden. „Und diese Geschäfte konnten sie machen, weil ihre Führung und ihre Aufsichtsorgane ihren Anforderungen nicht gewachsen waren. Lange Rede kurzer Sinn: Sie hatten eine schlechte Governance." Aus seiner Sicht muss sich die BaFin in ihrer Aufsichtstätigkeit deshalb künftig mehr mit dem Faktor Mensch auseinandersetzen.[1]

Auch die EZB setzt in ihren Aufsichtsprioritäten für die Jahre 2025 bis 2027 einen klaren Schwerpunkt auf die Stärkung von Governance-Strukturen und Risikokultur. In Kürze wird die finale Version des Leitfadens zu Governance und Risikokultur erwartet, der im Sommer 2024 erstmalig zur Konsultation gestellt wurde. Dieser Leitfaden konkretisiert die Erwartungen an Banken und deren Führung in Bezug auf Risikokultur, insbesondere hinsichtlich Tone from the Top, Kommunikation, Risikotoleranz (Risk Appetite Framework) und der Ausgestaltung von Anreizsystemen. Der Leitfaden stellt Verknüpfungen zu aktuellen EBA-Leitlinien, CRD-Vorgaben und FSB-Standards her, wodurch er faktisch als Interpretation bestehender EU-rechtlicher Verpflichtungen fungiert. Nach Aussage des Fachgremiums MaRisk habe dieser jedoch keinen normativen Charakter und würde nationale Anforderungen nicht ersetzen oder ergänzen. Dennoch ist es vorstellbar, dass dieser Leitfaden als Grundlage für die o.g. EBA-Konsultation dienen wird und somit über Umwege seinen Weg ins nationale Recht findet.[2]

EZB-Leitfaden 2024 zu Governance und Risikokultur

Der EZB-Leitfaden zu Governance und Risikokultur ersetzt die Aufsichtserklärung von 2016 und dient als Bewertungsgrundlage für zukünftige Prüfungen. Die Europäische Zentralbank legt darin klare Erwartungen an Institute fest – mit Fokus auf vier zentrale Elemente:

1. Tone from the Top / Leitungskultur

Das Verhalten der Geschäftsleitung soll Maßstäbe setzen. Integrität, Verantwortungsbewusstsein und Vorbildfunktion sind entscheidend für die Risikokultur.

2. Offene Kommunikation und kritischer Dialog (Effective Communication and Challenge)

Es soll eine Kultur geschaffen werden, in der sich jeder traut, Bedenken oder Meinungen offen zu äußern. Unterschiedliche Sichtweisen werden ernst genommen. Entscheidungen sollten von konstruktiver Kritik getragen und durch offene Diskussionen verbessert werden.

3. Verantwortlichkeiten der Mitarbeiter (Accountability for risks)

Es sollen klare Verantwortlichkeiten geschaffen werden für die Übernahme, die Überwachung, Steuerung und Vermeidung von finanziellen und nicht-finanziellen Risiken zusammen mit einer klaren Definition der Rollen der Kontrollfunktionen.

[1] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/RedenInterviews/re_250507_jahrespressekonferenz2025.html

[2] https://www.bafin.de/SharedDocs/Downloads/DE/Protokoll/dl_protokoll_FG_MaRisk_20241127_BA.pdf

4. Angemessene Anreizstrukturen (Incentives)
Vergütungssysteme sollen risikoorientiertes Verhalten fördern. Kurzfristige Boni ohne Rücksicht auf Risiken werden kritisch gesehen. ESG-Ziele sollen stärker berücksichtigt werden.

Ziel des Leitfadens ist eine stärkere Verankerung der Risikokultur in allen Organisationsebenen. Als wesentliche Stellhebel sieht die Europäische Zentralbank dabei die Geschäftsführung und ihre Kontrollgremien, die internen Kontrollfunktionen, das Risk Appetite Framework (RAF), sowie das Anreiz- und Vergütungssystem.

Zur Herausarbeitung der vier Dimensionen arbeitet der Leitfaden mit Praxisbeispielen, Best Practices und Red Flags aus der Aufsichtserfahrung, die Instituten konkrete Orientierung bieten.[1]

Der neue Leitfaden bringt im Vergleich zur Erklärung aus 2016 eine deutliche inhaltliche und strukturelle Weiterentwicklung mit sich. Die Aufsicht formuliert nun nicht mehr nur grundsätzliche Erwartungen, sondern legt einen umfassenden, operativ ausgerichteten Maßstab an, der sowohl das Verhalten von Leitungsorganen als auch die institutionelle Ausgestaltung der Governance vertieft adressiert. Besonders hervorzuheben sind folgende zentrale Änderungen:

/// Klare Definition und Operationalisierung der Risikokultur mit den oben genannten vier Kern-Dimensionen sowie Vorgaben zur regelmäßigen Überprüfung und Messung der gelebten Kultur.

/// Verbindliche Anforderungen an Leitungsorgane, darunter Diversität, Unabhängigkeit, Ausschussstruktur, Selbstbewertungen und aktive Aufsichtsfunktion – alles mit klarer Verankerung in regulatorischen Vorgaben.

/// Systematische Verankerung von Governance-Anforderungen in den internen Kontrollfunktionen, inklusive Rollenklärung, Durchsetzungsfähigkeit und direkter Berichterstattung an das Leitungsorgan.

/// Stärkere Kopplung von Anreizsystemen und Risikokultur, einschließlich konkreter Anforderungen an Governance-Strukturen zur Vergütung (z. B. Vergütungsausschuss, Malus / Clawbacks, Gender-Pay-Governance).

/// Ausweitung der Anwendbarkeit auch auf kleinere Institute über das Proportionalitätsprinzip – verbunden mit der Erwartung, dass nationale Aufseher den Leitfaden ebenfalls heranziehen (lesen Sie oben unsere Einschätzung zur Adaption der MaRisk).

[1] Möchten Sie wissen, ob auch Red Flags in Ihrem Institut zu finden sind? Sprechen Sie uns zu unserem Governance und Risikokultur-Quick Check an.

Diese Änderungen zeigen den verstärkten und tiefergreifenden Prüfungsfokus, den die EZB auf dieses Thema legt. Sie kündigt in ihrem Schreiben unter anderem an, ihren Aufsichtsansatz im Bereich Governance und Risikokultur kontinuierlich weiterzuentwickeln. Dabei werden regulatorische Entwicklungen, Veränderungen in der Bankenpraxis sowie neue Erkenntnisse aus der internationalen Aufsichtsgemeinschaft einbezogen. Ziel ist es, Risiken frühzeitig zu erkennen und die Steuerungsfähigkeit der Institute langfristig zu stärken.

Die EZB und BaFin signalisieren damit klar, dass Risikokultur und Governance nicht mehr als „weiche Faktoren" behandelt werden, sondern als prüfbare, bewertbare und sanktionierbare Elemente einer integralen Bankensteuerung.

Red Flags und Best Practices

Die EZB formuliert klare Red Flags sowie Best Practices, die Banken dabei helfen können, ihre Prozesse und Systeme zu optimieren.

Aus Sicht der EZB setzen ein belastbares Governance-System und eine wirksame Risikokultur voraus, dass strukturelle Rahmenbedingungen, Führungsverhalten und Anreizsysteme konsistent aufeinander abgestimmt sind.

Demgegenüber stehen zahlreiche Red Flags, die auf strukturelle Schwächen und kulturelle Risiken hinweisen. Zentral ist ein unzureichender „Tone from the Top" – also ein Führungshandeln, das weder klare Erwartungen formuliert noch gewünschtes Verhalten vorlebt. Fehlende Unabhängigkeit der Kontrollfunktionen, mangelnde Sanktionierung unethischen Verhaltens und unklare Eskalationsmechanismen schwächen die Risikokultur ebenso wie eine Kultur des Schweigens, in der Fehlermeldungen unterdrückt oder ignoriert werden. Auch eine unzureichende Vielfalt im Gremium, dominierende Einzelpersonen und eine fehlende Debattenkultur („Groupthink") sind klare Warnzeichen.

Im Bereich der Anreizsysteme stellen undifferenzierte oder gar fehlgeleitete Vergütungsstrukturen ein erhebliches Risiko dar. Auch eine unzureichende Verankerung individueller Verantwortlichkeit sowie schwache Transparenz bei der Berichterstattung über Risiken und Verstöße deuten auf eine defizitäre Governance hin.

Eine konsequente Auseinandersetzung mit diesen Schwachstellen und der Abgleich mit etablierten Best Practices ermöglichen es, gezielt an den neuralgischen Punkten der Risikokultur anzusetzen – bevor diese zum Prüfungsgegenstand oder Reputationsrisiko werden.

So formuliert die EZB für jedes der oben genannten Themen wie auch jeden Stellhebel eine klare gewünschte Umsetzung. All diese haben wir strukturiert aufgearbeitet und in ein Reifegradmodell überführt (siehe auch Kapitel „Governance und Risikokultur als zunehmender Prüfungsfokus").

Als Beispiel sollen die Best Practices zum Thema Anreizsystem in diesem Artikel im Detail beleuchtet werden.

Ein wirksames Anreizsystem im Bankensektor soll laut EZB finanzielle und nicht-finanzielle Elemente miteinander verbinden, um verantwortungsbewusstes Risikoverhalten gezielt zu fördern. Nicht-finanzielle Anreize umfassen temporäre Versetzungen in andere Abteilungen (Secondments), die Finanzierung von Zusatzqualifikationen oder die Teilnahme an spezialisierten Trainingsprogrammen. Nicht-finanzielle wie finanzielle Anreize (Boni, Gehaltssteigerungen oder Beförderungen) sollen beide an klar definierte und risikoadjustierte Leistungskennzahlen (KPIs) geknüpft werden. Diese Kennzahlen wiederum sollten mit dem Risikoappetit (RAF) verzahnt sein. Wenn das Verhalten eines Mitarbeiters beispielsweise zum Überschreiten eines Risikolimits führt, soll sich dies in seiner variablen Vergütung widerspiegeln.

Wichtig ist darüber hinaus, dass einzelne Anreize nicht isoliert betrachtet werden, sondern in ein umfassendes Governance- und Risikomanagementsystem eingebettet sind: So werden risikorelevante KPIs für Führungskräfte angemessen in ihrer Gesamt-Performance-Scorecard gewichtet, um kurzfristige, risikobehaftete Gewinnmaximierung zu verhindern und nachhaltige Wertschöpfung zu fördern. Die genannten KPIs wiederum sollen alle Stakeholder einbeziehen (d.h. Mitarbeiter, Kunden, den Regulator sowie Aktionäre).

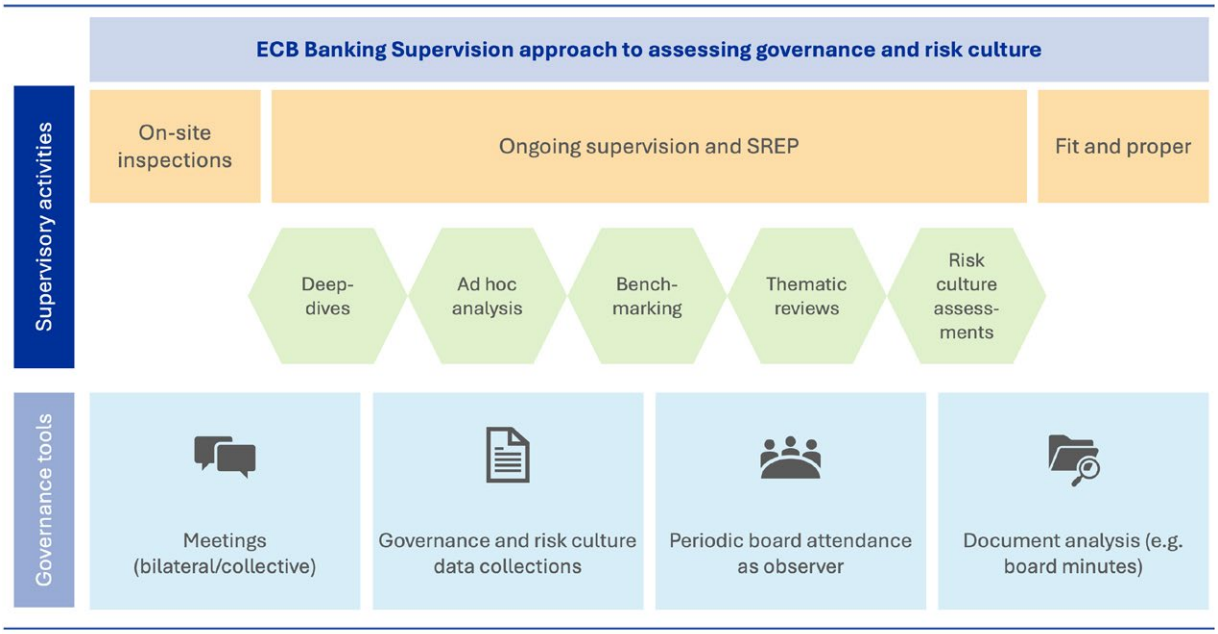
Prüfungsvorgehen

Während die EZB die Risikokultur sowie Governance fest als Bestandteil des SREP in ihren regelmäßigen Prüfungsprozess eingebettet hat, prüft die BaFin diese laufend weniger konkret im Rahmen ihrer regelmäßigen Bankengespräche, Ergebnisse aus internen Audits oder Informationen zu Whistleblowing-Fällen. Ein Deep-Dive in diese Themenbereiche kann jedoch immer Teil einer §44er KWG-Sonderprüfung sein.

Im Rahmen ihrer Prüfungen setzen sowohl EZB wie BaFin auf eine Kombination qualitativer und quantitativer Verfahren zur Bewertung der Risikokultur. Zum Einsatz kommen unter anderem strukturierte Interviews mit Führungskräften, interne Self-Assessments, Auswertungen von Sitzungsprotokollen sowie Indikatoren wie Mitarbeiterfluktuation, Whistleblowing-Meldungen oder Eskalationsverhalten.

Werden Mängel festgestellt, schlagen sich diese im SREP unmittelbar nieder – etwa in Form erhöhter Kapitalanforderungen, Einschränkungen der Geschäftstätigkeit oder konkreter Governance-Auflagen. Analog behält sich die BaFin vor, Strafen für im Rahmen der Sonderprüfung identifizierten Mängel zu verhängen – dies wurde bereits bei einigen Banken im Bereich Governance schlagend.

Darstellung EZB: Governance und Risikokultur im SREP



Eine Analyse von Geschäfts- und Risikoberichten verschiedener deutscher Banken

Im Folgenden zeigen wir zusammengefasst die Ergebnisse einer Analyse öffentlich verfügbarer Geschäfts- und Risikoberichte großer Privatbanken, Förderinstitute und Sparkassen.

Während sich alle untersuchten Institute zur Bedeutung einer starken Risikokultur bekennen, bleibt der Grad der Konkretheit sehr unterschiedlich. Manche Banken beschränken sich auf formelhafte Aussagen wie „Risikokultur ist Teil der Unternehmenswerte" oder „Verantwortlichkeiten sind definiert". Nur wenige gehen darüber hinaus und nennen konkrete Maßnahmen wie regelmäßige Schulungen, Feedbackformate oder die Bewertung von Instrumenten zur Kulturverankerung. Aussagen zur Messbarkeit – etwa in Form von KPIs, systematischem Monitoring oder klaren Eskalationsmechanismen – fehlen in der Mehrheit der Fälle vollständig. Auffällig ist zudem, dass die adressierte Zielgruppe selten konkret benannt wird: Mitarbeitende werden meist nur allgemein erwähnt, ihre Rolle bleibt oft unklar. Dies lässt Rückschlüsse auf eine eher normativ geprägte, weniger gelebte Risikokultur zu.

Wortwolke aus Analyse

H&C Reifegradmodell als Quick Check

Mit den Draft Guidelines und dem verstärkten Prüfungsfokus der EZB rücken Risikokultur und Governance ins Zentrum der europäischen Aufsicht – mit spürbaren Auswirkungen auf Deutschland. Jetzt ist der richtige Zeitpunkt, die gelebte Risikokultur kritisch zu prüfen: Wird sie nur kommuniziert oder im Alltag konsequent umgesetzt? Passt das Führungsverhalten zu Werten, Anreizsystemen und Eskalationswegen?

Risikokultur ist kein isoliertes Compliance-Thema, sondern ein strategisches Steuerungsinstrument, das messbar, in Governance-Strukturen verankert und durch glaubwürdige Führung sowie klare Kommunikation gestützt sein muss. Regulatorischer Druck und steigende Erwartungen bieten die Chance für ein Benchmarking mit Best Practices, um blinde Flecken zu identifizieren und Resilienz zu stärken.

Horn & Company hat dafür ein praxisnahes Reifegradmodell entwickelt, das Führung, Kommunikation, Anreizsysteme, Eskalationsmechanismen und Monitoring bewertet, Red Flags und Best Practices integriert und so gezielt Schwachstellen aufzeigt. Es liefert eine fundierte Standortbestimmung und konkrete Handlungsfelder – flexibel einsetzbar für verschiedene Institutstypen.

Wenn Sie wissen möchten, wo Ihr Institut derzeit steht, wie sich kulturelle Risiken frühzeitig erkennen lassen oder welche konkreten Schritte zur Weiterentwicklung Ihrer Risikokultur sinnvoll sind, kommen Sie gerne auf uns zu.

Wir unterstützen Sie mit fundierter Analyse, einem klar strukturierten Vorgehen und praxiserprobten Werkzeugen – passgenau für Ihr Geschäftsmodell und Ihre spezifischen Herausforderungen. Sprechen Sie uns an – wir begleiten Sie dabei, Risikokultur wirksam und zukunftssicher zu gestalten.

Beispielhaftes Ergebnis Reifegrad-Modell

Zusammenfassung & Empfehlungen

Tone from the Top: 47%

⚠ **Handlungsbedarf**

Empfehlung: Führungsebene muss dringend sichtbare Signale setzen. Klare Kommunikation, Integration von Risiken in Strategie, Role-Model-Trainings.

Anreizsysteme: 67%

◆ **Ausbaupotenzial**

Empfehlung: KPIs risikoorientierter gewichten, Beförderungsprozesse stärker mit Risikokultur verknüpfen.

Governance & Verantwortlichkeiten: 60%

◆ **Ausbaupotenzial**

Empfehlung: Governance-Struktur ausbaufähig. Ausschussarbeit und Unabhängigkeit verbessern.

Effektivität Leitungsorgan: 27%

⚠ **Handlungsbedarf**

Empfehlung: Leitungsorgan berücksichtigt Risiken unzureichend. Einrichtung eines Krisenkomitees und externe Trainings dringend.

Risk Appetite & Integration: 93%

✅ **Gut etabliert**

Empfehlung: RAF klar verankert, Best Practice beibehalten.

Operationale Umsetzung & Kontrollfunktionen: 60%

◆ **Ausbaupotenzial**

Empfehlung: Funktionen aktiv, aber inkonsistent. Regelmäßige Reporting- und Eskalationsprozesse stärken.

Risikobewusstsein & Alltagsverhalten: 60%

◆ **Ausbaupotenzial**

Empfehlung: Ausbaupotenzial. Kultur-Surveys, Lessons Learned-Prozesse, Integration von Risikothemen in Mitarbeitergespräche.

Feedback-, Eskalations- & Lernprozesse: 67%

◆ **Ausbaupotenzial**

Empfehlung: Prozesse vorhanden, aber schwach. Surveys und Indikatoren stärken.

Diversität & Nachfolgeplanung: 47%

⚠ **Handlungsbedarf**

Empfehlung: Diversität und Nachfolgeplanung unzureichend. Einführung verbindlicher Quoten und Nachfolgeprozesse nötig.

Compliance & Interne Revision: 87%

✅ **Gut etabliert**

Empfehlung: Wirksame Kontrollen, kontinuierliche Weiterentwicklung sicherstellen.

Gesamter Reifegrad: 61%

ÜBER HORN & COMPANY

HORN & COMPANY ist eine stark wachsende Topmanagement-Beratung, geführt von Partnern mit langjähriger Erfahrung und tiefer Branchenexpertise. Das Unternehmen ist auf die Beratung von Banken, Versicherungen, Industriegüter, Handel, Prozessindustrie und Automotive spezialisiert. Die rund 250 wissenschaftlich und fachlich überdurchschnittlich ausgebildeten Beraterinnen und Berater gestalten wertstiftende Optimierungsprogramme und sind dabei mehr als andere geleitet von einem quantitativen und daten-getriebenen Beratungsverständnis, einem messbaren Anspruch an die GuV-Wirksamkeit der Resultate und der Idee, dass die Kundenorganisation selbst Ownership auf den Veränderungsprozess erhält. Das Unternehmen mit Hauptsitz in Düsseldorf hat Büros in Berlin, Frankfurt am Main, Hamburg, Köln, München, Stuttgart, Charlotte, Singapur, Wien und Zürich. www.horn-company.com

//Autoren

Nadja Gawlik
Principal

Constantin Muranaka
Principal

Johannes Schmidt
Manager

HORN & COMPANY
Kaistraße 20 | 40221 Düsseldorf
Telefon +49 (0)211 30 27 26-0 | marketing@horn-company.de
www.horn-company.com