Thomas Kaiser

Praxis des Non-Financial Risk Managements im Finanzsektor

In 25 Jahren von „Other Risks“ zu Compliance, Conduct, Cyber & Co.

Springer Gabler

Praxis des Non-Financial Risk Managements im Finanzsektor

Thomas Kaiser

Praxis des Non-Financial Risk Managements im Finanzsektor

In 25 Jahren von „Other Risks“ zu Compliance, Conduct, Cyber & Co.

Springer Gabler

Thomas Kaiser
Professor Kaiser Risk Management Consulting
Steinbach (Taunus), Deutschland

ISBN 978-3-658-41867-0 ISBN 978-3-658-41868-7 (eBook)
https://doi.org/10.1007/978-3-658-41868-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Planung/Lektorat: Guido Notthoff
Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Das Papier dieses Produkts ist recyclebar.

Geleitwort

Das 25 Jahres-Jubiläum für Non-Financial Risk (NFR) ist ein sehr guter Zeitpunkt, den erreichten Entwicklungsstand und damit natürlich auch die offenen Baustellen des NFR zu betrachten. Denn auf der einen Seite wird NFR in den nächsten Jahren wieder einen starken Aufmerksamkeitszuwachs erleben – von Seiten der C-Suite, der Aktionäre, den Märkten und der Aufsicht. Das liegt an der Zyklizität des Verlustmusters.

Vermutlich die herausragendste Entwicklungsleistung des NFR in den letzten 25 Jahren war der gewaltige internationale Transparenzgewinn über die Verlustdimensionen und Verlustmuster. Operational Risk eXchange (ORX), deren Entwicklung und Wachstum ich im Board begleiten und unterstützen durfte, zeigt in ihren regelmäßigen öffentlichen Berichten nicht nur, wie gewaltig die NFR-getriebenen Verluste der Finanzindustrie in den verschiedenen Regionen der Welt sind, sondern auch, dass es eine kriseninduzierte Verlustzyklizität gibt.

Bisher sind zwei dieser Krisen in den Datenbeständen sichtbar: das Flatzen der dot-combubble und die weltweite Finanzkrise. Das gerade erlebte pandemiebedingte Anhalten und Neu-Starten der Weltwirtschaft ist wegen der zeitlichen Verzögerung, mit der NFR-Verluste bilanzwirksam werden, noch nicht deutlich sichtbar. Es fließen gerade die letzten Verluste aus der Finanzkrise in die Datenbank ein – gemeinsam mit den ersten aufgrund der pandemiebedingten Volatilität sichtbar gewordenen Kryptoindustrieverlusten.

Und auf der anderen Seite wird mit der Umsetzung von Basel III gerade das „let a thousand flowers bloom"-Projekt der risikosensitiven Eigenkapitalmodelle für die regulatorische Kapitalunterlegung von Operational Risk abgebrochen. Das zwingt die Finanzindustrie zum Verstehen der Gründe und zur Ableitung der nächsten Entwicklungsschritte. Woran ist dieses weltweit von hunderten großen Banken gleichzeitig unternommene und – wie mir als Head der Operational Risk Working Group des Institute of International Finance sehr deutlich sichtbar gemacht wurde – von den weltweiten Aufsehern sehr wohlwollend unterstützte Großprojekt der Advanced Measurement Ansätze (AMA) gescheitert?

In den vielen Jahren, in denen ich an der Frankfurt School for Finance & Management lehren durfte, erzeugte Non-Financial Risk durch die wunderbaren Verlust- und Risikoanekdoten (gehört ein Meteoriteneinschlag in den betrachteten Zeithorizont oder ein Krieg, eine Revolution, der Anstieg des Meeresspiegels, Tsunamis und die so spektakulä-

ren Betrugsfälle in den Handelsbereichen?) sehr schnell Faszination. Und etwas später Enttäuschung, dass es immer noch keinen Übersetzungsmechanismus gibt, durch die Reduzierung von zur Verfügung gestelltem Kapital das Risikoprofil zu verändern. Die (natürlich nur auf den ersten Blick bestehende) Einfachheit und Eleganz der Steuerungsmöglichkeit des Risikoprofils von Markt-, Kredit- und Liquiditätsrisiken ist bei NFR noch nicht erreicht. Die gerade im Vergleich damit vermeintliche Machtlosigkeit ist ein Grund dafür, dass NFR in den Zeiten nachlassender Verlustereignisse zumeist als zu optimierender unvermeidbarer Kostenblock ein Mauerblümchendasein fristet. Und in den (wiederkommenden) Zeiten der ansteigenden Verlustereignisse um so mehr (auch aktionistische) Aufmerksamkeit seitens Aufsicht und der C-Suite erreicht.

Gleichzeitig spornt es zu großartigen Forschungsleistungen an: Die unveröffentlichte Doktorarbeit von Patricia Rosa an der Frankfurt School hat sehr beeindruckend nachgewiesen, dass jeder einzelne Kunden-, Mitarbeiter- oder Infrastrukturvertrag, den ein Unternehmen abschließt oder ändert, ein einzelnes Rating verdient. Eine Kapitalunterlegung jedes einzelnen IPO-Vertrages anhand der Unternehmenskreditwürdigkeit hätte die dot.com-Verluste nicht nur in der Eintrittswahrscheinlichkeit, sondern auch in der Höhe vorhersagbar und damit steuerbar machen können.

Das Stoppen des globalen AMA-Projektes gibt der Finanzindustrie vielleicht die Gelegenheit, vom „toten Pferd" der eventtypfokussierten Modellierung abzusteigen und dem Schritt hin zur Einzelvertragsbetrachtung (und deren vielen Veränderungen etwa bei der Ausübung des Direktionsrechtes bei Aufbau- oder Ablaufänderungen) die Tür zu öffnen.

Vor NFR liegen gewaltige Entwicklungsaufgaben und es wird die nötigen Ressourcen und die nötige Aufmerksamkeit bekommen – gerade weil es im Vergleich zu den anderen Risikoarten so unterentwickelt ist.

Sehr gerne habe ich die Einladung angenommen, das Geleitwort zu diesem Buch zu schreiben. Vor ca. 25 Jahren, als in den Entwürfen zu Basel II die kargen Worte „other Risk" auftauchten, waren wir beide schon in Operational Risk-Einheiten tätig. Bei der Aufgabe, diesen zwei Worten mehr ökonomische Nützlichkeit einzuhauchen, begegneten und befreundeten wir uns. Mit ihm erlebe ich seit fast einem Vierteljahrhundert immer ein anregendes und produktives Reiben und Ringen um den nächsten Schritt der Weiterentwicklung von Non-Financial Risk (NFR) in den verschiedensten beruflichen Zusammenhängen. Jetzt ist deshalb eine gute Gelegenheit, ihm ausdrücklich dafür und für die persönliche Freundschaft zu danken.

Vielen Dank an Thomas, dass er hier seine einzigartigen Einblicke – ich kenne niemanden, der so viele verschiedene NFR-Implementierungen aus seiner Tätigkeit als Risikomanager, Berater, Prüfer und nicht zuletzt langjähriger Hochschullehrer im Detail gesehen hat – über den ganzen ersten Entwicklungszyklus, also die ganzen 25 Jahre, leicht lesbar und praktisch nutzbar mit uns teilt.

Thomas gelingt es, den aktuellen Stand zuzuspitzen. Er erläutert die großartigen Erkenntnisgewinne und auch die Spannungsfelder, die innerhalb der Banken und zwischen den Banken dadurch entstanden sind, zusammen mit den enttäuschten Hoffnungen und den vielen großen Aufgaben und Forschungsgelegenheiten, die noch einer Lösung harren.

Ich wünsche Ihnen allen das Vergnügen, das ich beim Lesen erlebt habe, und darüber hinaus ganz viele Anregungen NFR weiterzuentwickeln. Damit die NFR-Verträge bald so intuitiv identifiziert, bepreist (vielleicht mit Exposure Based Operation Risk Modellierung), genehmigt und gesteuert werden, wie es heute schon bei dem große Vorbild Kreditrisikomanagement gelingt.

Ich empfehle dieses Buch allen, die sich mit NFR ob im Risikomanagement der „Three Lines of Defense", ob in Studium oder Forschung oder in Prüfung, Beratung oder Aufsicht befassen.

ehem. Global Head of Operational Risk & Business Continuity Management
Deutsche Bank,
Frankfurt a. M., Deutschland
April 2023

Robert Hübner

Vorwort

In der Planungsphase dieses Buchs hatte ich den Arbeitstitel „Lehren aus einem Vierteljahrhundert Non-Financial Risk Management in Banken und Versicherungen – von „other risks“ zu Compliance, Conduct, Cyber & Co. Einblicke und Ausblicke in Vergangenheit, Gegenwart und Zukunft des Non-Financial Risk Managements“ verwendet. Aus verständlichen Gründen hat es dieser nicht auf das Cover des vorliegenden Buchs geschafft. Er ist aber fast schon eine Management Summary des Buchs und somit gut geeignet für dieses Vorwort.

Im Jahr 1995 hat der Untergang von Barings Bank durch „rogue trading“ (Nick Leeson) für nachhaltige Aufmerksamkeit gesorgt, 1997 sind erste Studien zu Operational Risk in Banken erschienen (BBA/C&L 1997), 1999 das erste Konsultationspapier zu „Basel II“ (BCBS 1999), in dem „other risks“ (aus denen später „operational risk“ wurde) thematisiert wurden. Vorreiter seitens der Banken waren u. a. Banker’s Trust und Credit Suisse (siehe IIEB 2000). Und ausgerechnet einer dieser Vorreiter scheint just zum Zeitpunkt des Schreibens dieses Buches an Problemen mit Non-Financial Risk (inklusive Risikokultur) zugrunde gegangen zu sein.

Somit ist ca. ein Vierteljahrhundert verstrichen, seit erste Banken begannen, sich systematisch mit dieser Disziplin (die seit ca. 10 Jahren im breiteren Sinne, unter Einschluss von Reputationsrisiken und teilweise auch strategischen Risiken bzw. Geschäftsrisiken zunehmend unter „Non-Financial Risk“ firmiert) zu beschäftigen. Versicherungen und andere Finanzdienstleister haben zu einem etwas späteren Zeitpunkt begonnen, sich mit diesen Themen intensiv auseinanderzusetzen. Ein Rückblick auf diese Zeitspanne und ein Ausblick auf die Zukunft scheint daher lehrreich zu sein.

Ich selbst habe irgendwann im Jahr 1998 den entscheidenden Anruf eines Headhunters bekommen – ob ich interessiert sei, die Quantifizierung operationeller Risiken voranzutreiben. Ich hatte zu dem Zeitpunkt offen gestanden keine Ahnung, was operationelle Risiken überhaupt sind – geschweige denn, wie man sie quantifizieren kann. Aber ich war der Herausforderung nicht abgeneigt – und bin das Thema seitdem nicht mehr losgeworden. Somit bin ich seit Januar 1999 in dem Thema unterwegs, zunächst bei der (gerade fusionierten: großes operationelles Risiko!) HypoVereinsbank, später dann bei der Commerzbank (wo ich – damals noch akzeptierte Praxis – durch die Welt reisen durfte,

um bei der Entstehung des OpRisk-Teils von Basel II mitzuhelfen – u. a. Mitglied von IIF- und BdB-Arbeitsgruppen). Danach lange Zeit globale Beratungsprojekte bei KPMG (sukzessive erweitert um Reputationsrisiken, strategische Risiken, Non-Financial Risk in der Breite, ESG-Risiken, Risikokultur …), unterbrochen von einem eher kurzen Aufenthalt bei der Deutschen Bank. Aktuell als selbstständiger Unternehmensberater („Professor Kaiser Risk Management Consulting") unterwegs. Und ergänzend halte ich zahlreiche Vorlesungen, Seminare, Konferenzen und Vorträge zu Operational Risk im Speziellen und Non-Financial Risk Management in der Breite (zunehmend unter Einschluss von ESG-Risiken, Risikokultur und verwandter Themen).

Die Entwicklung des Themas Operational Risk hat darunter gelitten, dass recht schnell ein Fokus auf die Messung gelegt wurde. Einerseits ist das „Garbage In-Garbage Out"-Prinzip in diesem Fall vielleicht noch etwas relevanter als bei anderen Risikoarten. Andererseits ergibt sich erst dann eine echte Steuerungswirkung, wenn die Governance-Strukturen dafür geeignet sind, Anreize geschaffen sind, Transparenz über die Risikolage (auch unter Einbezug qualitativer Informationen) besteht und die Risikokultur insgesamt den proaktiven Umgang mit Risiken befördert.

Ähnliches gilt auch für Reputationsrisiken, bei denen es einigen (glücklicherweise nicht der Mehrzahl!) der Aufseher mehr darum geht, ob irgendeine Zahl im ICAAP steht, anstelle ob nachweislich diese Risiken systematisch gesteuert werden. Und schließlich Geschäfts- und strategische Risiken: hier ist oft das Risikocontrolling nur am Rande beteiligt und geschäftspolitische, insbesondere strategische, Entscheidungen mit gravierenden Auswirkungen auf das Risikoprofil wurden in der Vergangenheit sehr häufig und in der Gegenwart immer noch zumindest gelegentlich ohne fundierte Betrachtung der Risikoaspekte getroffen.

Zu dem Non-Financial Risk-Zoo gehören mindestens zwei Dutzend Risikokategorien, -unterarten oder wie auch immer man sie nennen mag. Die Spezialisten für Cyber Risk, Rechtsrisiken, Compliance, Informationssicherheit etc. bedienen sich dabei oft einer sehr speziellen Fachsprache und eigenständiger Methoden – von Identifikation über Bewertung bis hin zum Reporting, in dem noch nicht einmal Ampelfarben zwangsläufig über mehrere Disziplinen hinweg die gleiche Bedeutung haben. Ich will die Bedeutung fachlicher Tiefe in Informatik, Jura, Mathematik etc. nicht gering schätzen. Oft kommt jedoch dabei zu kurz, dass viele (wenn nicht gar alle) Informationen und Bewertungen im Kontext Non-Financial Risk von Menschen zusammengetragen bzw. gemacht werden – mit allen inhärenten Herausforderungen. Ferner werden Steuerungsentscheidungen – in absehbarer Zeit zumindest – weiterhin von Menschen getroffen und sind damit in aller Regel nicht automatisierbar, wenngleich KI zumindest als Entscheidungsunterstützung zunehmend Verbreitung findet.

Und schlussendlich gilt: Risk Management is about **managing** risk: das Treffen fundierter Entscheidungen auf Basis bestmöglicher Informationen (quantitativ und qualitativ) ist der eigentliche Zweck des Risikomanagements – Methoden und Verfahren sind nur Mittel zu diesem Zweck.

Ich möchte mich sehr herzlich bei Dr. Christian Einhaus und Robert Hübner bedanken, die Entwürfe des Buchs aus recht unterschiedlichen Blickwinkeln kritisch beäugt haben. Kommentare der beiden habe ich im Rahmen meiner Möglichkeiten verarbeitet – evtl. verbleibende Restunschärfen verbleiben in meiner Verantwortung (auch wenn man die im Finanzwesen ja gerne über Gremien sozialisiert). Ich möchte dem Springer-Verlag – insbesondere Herrn Guido Notthoff – für die professionelle Begleitung dieses Buchprojekts danken. Ein besonderer Dank an alle, die mich in dem ca. Vierteljahrhundert Non-Financial Risk/Operational Risk Management begleitet haben. Um die Liste nicht zu lang werden zu lassen beschränkt auf die deutschsprachigen (Ex-)Kolleginnen und Kollegen, und natürlich nur eine Auswahl in alphabetischer Reihenfolge – und in vielen Fällen bezieht sich das nicht auf die aktuelle (und ohnehin nicht genannte) Affiliation:

Prof. Dr. Ulrich Anders, Dr. Michael Auer, Dr. Helmut Beeck, Dr. Frank Beekmann, Thomas Beil, Tilo Bellof, Christian Böing, Thomas Braun, Dr. Patrik Buchmüller, Dr. Steffen Bunnenberg, Peter Bürger, Marion Bürgers, Andreas Duldinger, Walter Dutschke, Dr. Christian Einhaus, Prof. Dr. Günter Franke, Dr. Jörg Fritscher, Dr. Sebastian Fritz-Morgenthal, Dr. Andreas Gottschling, Carsten Groß, Marcus Haas, Jonas Hampl, Jörg Hashagen, Wolfgang Hartmann, Anja Hirt, Dr. Stefan Hirschmann, Robert Hübner, Peter Jeuck, Dr. Michael Kalkbrener, Thilo Kasprowicz, Eckart Koerner, Marc Felix Köhne, Dr. Hans-Werner Ladynski, Dr. Bina Lehmann, Dr. Carsten Lehr, Dr. Björn Lenzmann, Stefan Loedorf, Hans Löffelmann, Dr. Stefan Look, Dr. Peter Luksch, Dr. Laura Mervelskemper, Claudia Meyer, Thomas N. Müller, Dr. David Nicolaus, Myriam Nied, Klaus Ott, Dr. Hagen Rafeld, Frank Romeike, Dr. Ingo Schäl, Prof. Dr. Christian Schlag, Rainer Sprengel, Petra Obermann, Dr. Wilfried Paus, Joachim Pfeifer, Dr. Thomas Poppensieker, Markus Quick, Christoph Reitze, Mareike Reus, Dr. Sebastian Rick, Heidi Rudolph, Dr. Andreas Saemann, Karin Sagner-Kaiser, Bodo Schmidt, Hartwig Schnöckel, Dr. Gerhard Schröck, Tatjana Schulz, Andreas Seibt, Stefan Selig, Dr. Carsten Steinhoff, Prof. Dr. Daniel Sommer, Sylvia Trimborn-Ley, Dr. Gerrit Jan van den Brink, Dr. Johannes Voit, Prof. Dr. Mark Wahrenburg, Carsten Zecher.

Ich bitte alle zu Unrecht nicht Genannten um Entschuldigung für das Versehen – OpRisk, RepRisk bzw. Non-Financial Risk eben!

Ich wünsche Ihnen, liebe Leserin und lieber Leser, viel Freude und wertvolle Inspirationen bei der Lektüre,

Steinbach (Taunus), Deutschland Prof. Dr. Thomas Kaiser
April 2023

Einführung

Bislang scheint es keine deutschsprachigen Bücher zu Non-Financial Risk Management in der Breite zu geben. Dabei wird Non-Financial Risk – wie in Abschn. 2.3 ausführlicher dargestellt – als Vereinigungsmenge von operationellen Risiken (einschließlich deren Unterrisiken wie Cyber Risk, Conduct Risk), Reputationsrisiken sowie strategischen Risiken gesehen. Einige Bücher zu Operational Risk Management sind verfügbar, die aber i. d. R. veraltet (siehe z. B. Kaiser und Köhne 2004) oder sehr stark auf Quantifizierungsthemen fokussiert sind (siehe z. B. Cruz 2002). Ziel des vorliegenden Buches ist, die Entwicklung der Fachdisziplin Non-Financial Risk Management mit all ihren Facetten aufzuzeigen sowie Entwicklungstendenzen darzustellen. Naturgemäß kann das Werk nicht in allen Themen in die Tiefe gehen – nicht umsonst gibt es zahlreiche eigenständige Bücher zu Themen wie bspw. Cyber Risk und Compliance. Es zeigt sich jedoch immer mehr, dass nur eine vernetzte Denkweise wirklich erfolgreich ist, sodass die Darstellung der Zusammenhänge der einzelnen Themenkomplexe wichtig ist.

Das Buch beginnt naturgemäß mit der **Vergangenheit des Non-Financial Risk Management**. Einerseits waren **Verluste** schon immer Trigger für Management-Aktivitäten – teilweise unter den Stichworten Qualitätsmanagement oder Prozessoptimierung. In Einzelthemen (bspw. Kreditkartenbetrug) erfolgte recht früh eine datengestützte, quantitative Analyse. Erst spät setzte jedoch eine systematische Auseinandersetzung in der Breite mit Verlusten aus operationellen Risiken und anderen Non-Financial Risks ein. Dies liegt teilweise an den psychologischen Effekten – der Treiber Mensch ist oft eine wesentliche Komponente in der Entstehung von Verlustereignissen. Das **Aufsichtsrecht**, das sich seit den frühen 2000er-Jahren zunehmend mit Non-Financial Risk beschäftigt, ist als Treiber für Investitionen nicht zu unterschätzen. Leider beginnen viele Finanzinstitute erst dann mit der Entwicklung neuer Prozesse und Verfahren, wenn dies aufsichtsrechtlich erforderlich sind (und ignorieren dabei oft den betriebswirtschaftlichen Nutzen, den solche Aktivitäten stiften können). Und schließlich lohnt ein Blick über den Tellerrand: **Enterprise Risk Management** ist in Industrieunternehmen seit langem etablierte Praxis. Da dieses üblicherweise einerseits vernetzt aufgebaut und andererseits eng in die Kernprozesse des Unternehmens eingebunden ist, können gerade für eher qualitative Themen wie Non-Financial Risks hiervon gute Impulse abgeleitet werden.

Das zweite Kapitel des Buchs beschäftigt sich mit **Gegenwart des Non-Financial Risk Management – Rahmenwerk**. Die **Risikokultur** sollte eine Art „Unternehmens-DNA" darstellen, die zwar nicht ausschließlich für Non-Financial Risks relevant ist, jedoch in besonderem Maße für diese. Nur wenn risikobewusstes Verhalten internalisiert wird, kann von einem effektiven Risikomanagement ausgegangen werden. **Risikostrategie und -appetit** sollten die Marschrichtung für NFR vorgeben. Auch dieser Themenkomplex ist risikoartenübergreifend. Da Non-Financial Risks jedoch eher schwer mit quantitativen Metriken beherrschbar sind, ist dieses Thema besonders herausfordernd. Es müssen teilweise qualitative, jedoch trotzdem hinreichend greifbare und überprüfbare Vorgaben gemacht werden. Non-Financial Risk besteht – wie bereits erwähnt und im dritten Kapitel ausführlicher dargestellt – aus vielen Einzeldisziplinen. Diese haben oft ihre eigene Terminologie und Verfahrensweisen. Eine klare Sprachregelung, also insbesondere eine **Taxonomie** der NFR, ist wesentlich, um Konsistenz zu erreichen. Das erfolgreiche Management der Non-Financial Risk erfordert ein gutes Zusammenspiel zahlreicher Bereiche, Abteilungen, Beauftragten etc. Definierte Verantwortlichkeiten durch klare **NFR-Risikogovernance** ist daher wesentlich. Wie bereits erwähnt ist die **Qualitative Identifikation und Bewertung der NFR** besonders wichtig. Dies startet mit der Risikoinventur und umfasst verschiedene Spielarten von Self-Assessments (tw. Risk & Control Self Assessment, RCSA genannt). Für Einzeldisziplinen gibt es oft eigenständige Bedrohungs-, Gefährdungs- und Risiko-Analysen. Daneben gibt es auch eine **Quantitative Identifikation und Bewertung der NFR**. Hierzu zählen die (meist semi-quantitative) Szenarioanalyse, Modelle – bis zur Abschaffung des fortgeschrittenen Messansatzes (AMA) für regulatorisches Kapital, auch darüber hinaus für ökonomisches Kapital – sowie verschiedene Spielarten des Stresstestings. Für systematische Analysen und Modelle sind Datenbanken und andere **IT-Unterstützung** für den Risikomanagement-Prozess wesentlich. Die Vielzahl an Datenquellen und die oft manuelle Erhebung derselben stellen weiterhin eine große Herausforderung dar. **Risikoreporting und -steuerung der NFR** stellt die eigentliche Königsdisziplin dar. Daten zu erheben und Berechnungen anzustellen sollte kein Selbstzweck (und auch nicht eine aufsichtsrechtliche Pflichtübung) sein, sondern das aktive Management der Risiken unterstützen. Daher sollte das Risikoreporting auch der Steuerung dienen und nicht als Tätigkeitsbericht verschiedener Risikocontrolling-Einheiten missverstanden werden. Die meisten Non-Financial Risks ändern sich fortlaufend und die Effektivität von Steuerungsmaßnahmen ist nicht immer im Vorhinein genau abschätzbar. Daher ist die regelmäßige **Risikoüberwachung der NFR** wichtig. Neben der Überwachung des Verlustprofils gehören insbesondere Risikoindikatoren zum klassischen Instrumentarium hierfür.

Das dritte Kapitel beschäftigt sich mit ebenfalls mit der **Gegenwart des Non-Financial Risk Management** nun jedoch mit dem Fokus auf **wichtige Einzelthemen**. Zunächst kann die Bedeutung von **Behavioural Risk Management** für NFR gar nicht hoch genug eingeschätzt werden. Einerseits entstehen die meisten Verluste aus Non-Financial Risk aus (grober) Fahrlässigkeit – teilweise auch aus Vorsatz – oder werden zumindest durch solche Faktoren begünstigt. Andererseits spielen Menschen und deren Entscheidungen eine

fundamentale Rolle bei der Steuerung der Non-Financial Risks. Eine vollautomatische Risikosteuerung (wie sie teilweise für Finanzrisiken etabliert werden konnte) scheint für die allermeisten Non-Financial Risk-Themen unerreichbar zu sein. Unter den Non-Financial Risks spielen **Reputationsrisiken** eine besondere Rolle. Diese sind gewissermaßen Katalysatoren der Risikolandkarte – die erfolgreiche Steuerung eines Risikos kann sich über den Wirkungskanal der Reputationsrisiken als Risiko in einer anderen Risikoart (insbesondere Liquiditäts- und Geschäftsrisiken) manifestieren. Ein sehr bedeutender Themenkomplex der operationellen Risiken sind **NFR im Rechtsumfeld**. Hierzu zählen im Mindesten die (nicht sauber trennbaren) Fachgebiete Compliance, Conduct und Legal. Bewusste oder unbewusste Verstöße gegen geltendes Recht, aber auch gegen Marktgepflogenheiten und interne Anweisungen, haben in der Vergangenheit zu den größten Einzelverlusten geführt – und ein Ende ist nicht in Sicht. Das zweite große Feld mit steigender Bedeutung ist **NFR im IT-Umfeld**. Hierzu zählen insbesondere Informationssicherheitsrisiken, I(K)T-Risiken und Cyberrisiken. Auch hier ist eine klare Trennung der Einzelthemen kaum möglich. Business Continuity Management als Steuerungsmaßnahme für operationelle Risiken hat eine lange Tradition. In jüngster Zeit hat sich Operational Resilience als ganzheitliche Sicht auf das Business Continuity Management etabliert. Insbesondere im Hinblick auf aktuelle (und leider auch künftig zu erwartende) Krisen erscheint dieser Ansatz sehr wichtig zu sein. **ESG-Risiken** sind aus NFR-Sicht im Vergleich zu den beiden anderen genannten Risikofeldern sozusagen „Neuland“. Es zeigt sich, dass zahlreiche Verbindungen – nicht nur, aber in besonderem Maße zu Reputationsrisiken – bestehen. Aktuell fokussieren Finanzinstitute im Zusammenhang mit ESG-Risiken auf Finanzrisiken – hier besteht noch Nachholbedarf auf der Non-Financial Risk-Seite.

Das letzte Kapitel beschäftigt sich naheliegenderweise mit der **Zukunft des Non-Financial Risk Management**. Zunächst ist es spannend, die **Einflüsse von Megatrends** (Digitalisierung, ESG, Agiles Arbeiten etc.) auf das NFR-Management zu untersuchen. Hier liegen geplante Änderungen an Geschäftsmodellen und -abläufen zugrunde, die erhebliche Auswirkungen auf das NFR-Profil von Finanzinstituten haben und entsprechend gesteuert werden müssen. Strategische Risiken werden nicht einheitlich als Bestandteil der Non-Financial Risks gesehen. Gerade im Licht dieser Entwicklungen erscheint das Thema jedoch sehr wichtig zu sein – und hat wiederum zahlreiche Verflechtungen mit anderen Non-Financial Risks. Eher reaktiv zu sehen sind die **Auswirkungen aktueller Entwicklungen** (COVID-19, geopolitische Krisen). Auch hier kommt es – allerdings ungeplant – zu signifikanten Veränderungen der Rahmenbedingungen, unter denen Finanzinstitute sowie deren Kunden und Geschäftspartner agieren. Wie im ersten Kapitel erwähnt, spielt das Aufsichtsrecht eine große Rolle für stark regulierte Unternehmen wie Banken, Versicherungen und andere Finanzdienstleister. Daher gehört zu einer zukunftsorientierten Sicht auch ein Blick auf sich abzeichnende Änderungen an regulatorischen Vorgaben. Schlussendlich stellt sich die Frage, wie stark die Einzeldisziplinen der Non-Financial Risks miteinander verbunden werden können und ob die aktuelle Trennung zwischen Finanzrisiken einerseits und Non-Financial Risks andererseits auf Dauer sinnvoll ist. **Effizienzgewinne durch integrierte Ansätze** ist hier das Schlagwort.