

Risk & Compliance Advisory

# Non-Financial-Risk Management

Der Weg zum integrierten Risikomanagement



# Steigende Bedeutung von Non-Financial-Risks

Non-Financial-Risks (NFR) haben in den letzten Jahren stark an Bedeutung für Finanzinstitute gewonnen. IT-Ausfälle, regulatorische oder ethische Verstöße zeigen eindrücklich, dass Risiken jenseits klassischer Finanzkennzahlen erhebliche Auswirkungen auf Reputation, Stabilität und Ertragskraft haben können. So ereignete sich bspw. Ende letzten Jahres bei einem deutschen Finanzinstitut ein Betrugsskandal, der dazu führte, dass ein Vorstandsmitglied sein Mandat niederlegte.

Die zunehmende Komplexität regulatorischer Anforderungen sowie der technologische Wandel verschärfen die Notwendigkeit, NFR systematisch zu identifizieren, zu bewerten und zu steuern. Anders als bei finanziellen Risiken fehlen jedoch häufig standardisierte Bewertungsmethoden und klare Verantwortlichkeiten. Um dem gerecht zu werden, bedarf es einer strukturierten und ganzheitlichen Auseinandersetzung mit den Hauptkategorien von Non-Financial-Risks sowie deren gezielter Berücksichtigung im Risikomanagement.

## Systematik von Non-Financial-Risks

NFR definieren sich darüber, dass sie alle Risiken zusammenfassen, die nicht explizit finanzielle Risiken sind. Dabei können sich die Risiken in den einzelnen NFR-Kategorien überlappen. So wirken beispielsweise ESG-Risiken als horizontale Risikotreiber auf andere Risiken ein. Daher ist von Anfang an eine strukturierte Aufschlüsselung der Risiken und Zuordnung zu einer Risikokategorie essenziell. Wir unterscheiden sechs Hauptkategorien von NFR: operationelle, reputative, Compliance-, rechtliche, strategische und ESG-Risiken. Operationelle Risiken werden gemäß der CRR III als Risiken definiert, die aus Verlusten entstehen, die durch unangemessene Prozesse oder fehlerhafte Prozessausführungen, Personen und Systeme oder externe Ereignisse verursacht werden. Der Artikel 4 Nr. 52 der CRR III schließt dabei rechtliche Risiken in die operativen Risiken mit ein. Im Rahmen des NFR-Managements ist es jedoch sinnvoll, Rechtsrisiken als separate Kategorie zu würdigen, da diese Risiken eigene Bewertungsmethoden nach sich ziehen können. Aus den NFR-Kategorien lassen sich zur genaueren Unterscheidung folgende Unterkategorien ableiten:

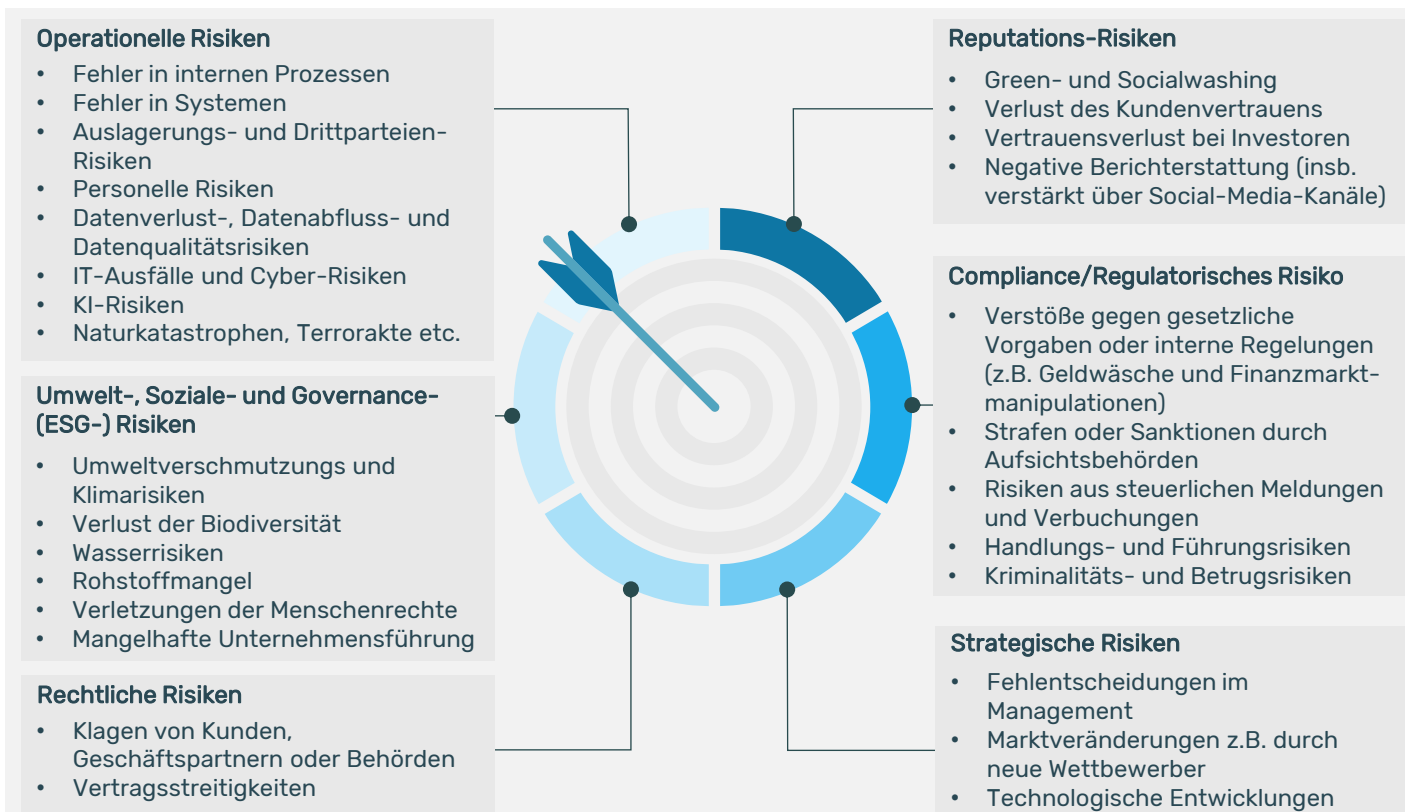


Abb. 1: Darstellung der Systematik von Non-Financial-Risks

Diese Risikokategorien können in der Risikoinventur als erster Ansatz zur Identifikation von operationellen Risiken im Bankrisikomanagement genutzt werden. So gelten mit der Finalisierung der CRR III ab dem 01.01.2025 neue Regelungen für Institute zur Berechnung der Eigenmittelanforderungen in Bezug auf operationelle Risiken. Die tradierten Ansätze wurden durch den „standardised measurement approach“ (SMA) ersetzt. Im SMA werden die OpRisk-Kapitalanforderungen durch den Geschäftsindikator (BI) ermittelt, welcher auf Finanzkennzahlen der Bilanz sowie der Gewinn- und Verlustrechnung der Institute basiert. Zudem sind Institute mit einem BI größer gleich 750 Mio. € verpflichtet, eine 10-jährige Verlustdatenbank über ihre eingetretenen operativen Verluste aufzubauen. Hierzu entwickelt die EBA derzeit eine neue Risikotaxonomie zur Einstufung dieser Verlustereignisse, welche spätestens am 10.01.2026 an die EU-Kommission zur Verabschiedung übermittelt wird.



# Berücksichtigung von Non-Financial-Risks im Risikomanagement

Die Non-Financial-Risks sind regulatorisch getrieben, fester Bestandteil im heutigen Risikomanagement der Institute. So werden NFR zwar von den Instituten bewertet und gesteuert, allerdings variiert die Methodik, Berichtsformate und Governance häufig in den einzelnen NFR-Kategorien stark und weist oftmals unterschiedliche Reifegrade auf. Dadurch entstehen Ineffizienzen und Qualitätsverluste. Der Schlüssel zu einem ganzheitlichen NFR-Management liegt in der Vereinheitlichung der Methodik und in einer übergreifenden Steuerung wo sinnvoll implementierbar.

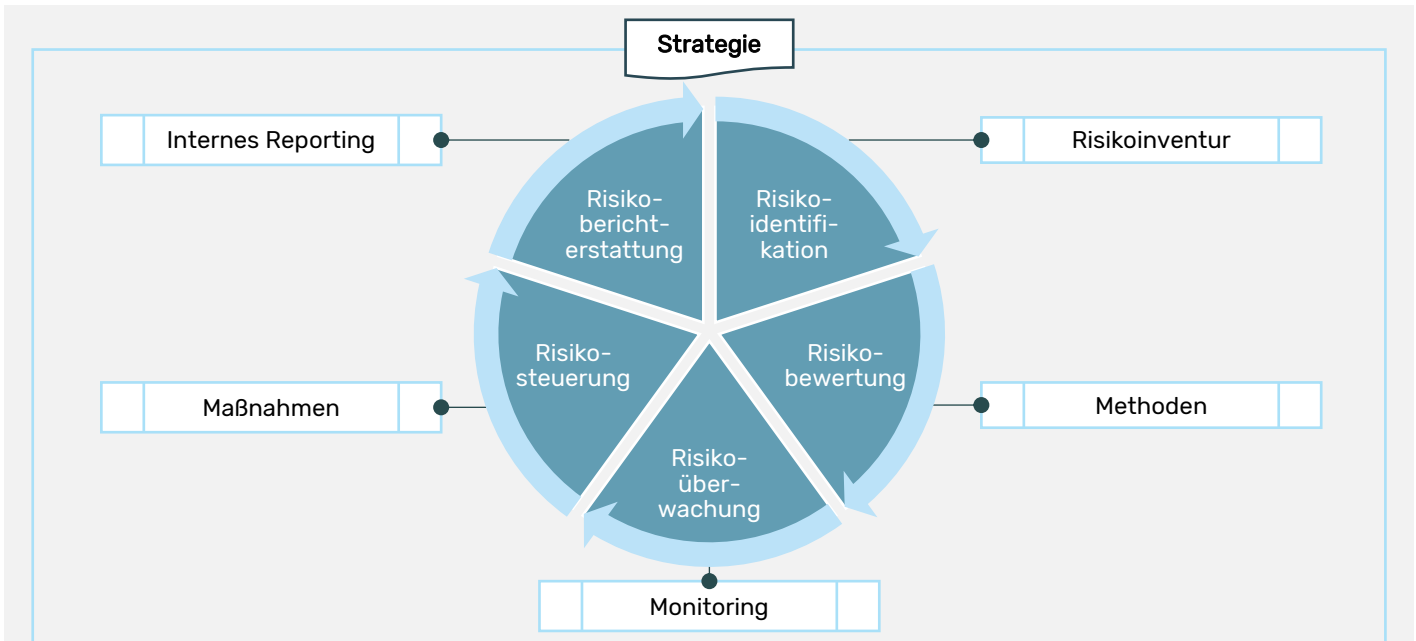


Abb. 2: Darstellung des Risikomanagementansatzes

## Aktuelle aufsichtliche Schwerpunkte im NFR-Bereich

### ESG-Risiken

Die Aufnahme der ESG-Risiken in die MaRisk im Jahr 2023, die Diskussionen über das Omnibus-Verfahren zur CSRD und CSDDD, die neuen Greenwashing-Vorgaben durch die EmpCo-RL, die stichprobenartigen Überprüfungen der SFDR-Berichte durch die BaFin sowie weitere ESG-bezogene Aufsichtsschwerpunkte für das Jahr 2025 führen dazu, dass das Thema ESG-Risiken immer umfangreicher und bedeutender für Finanzinstitute wird. [\(Siehe Flyer 7. MaRisk-Novelle\)](#)

### AML-Risiken

Die BaFin hat am 29. November 2024 ihre AuAs zum GwG überarbeitet und veröffentlicht. Dies bringt weitgreifende Änderungen für die verpflichteten Institute mit sich. Zusätzlich wurde auf der EU-Ebene eine Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AMLA) eingerichtet, sowie nationale AML-Vorschriften durch die AML-Verordnung harmonisiert und verschärft. [\(Siehe Flyer AML-Umfrage\)](#)

### Regulatory Compliance Risk

Die rechtlichen Rahmenbedingungen im Bankensektor sind komplex und vielfältig. So unterliegen Banken den Anforderungen der nationalen und internationalen Finanzaufsicht. Infolge dieser Regulierungsflut können Überlastungseffekte in den Compliance-Abteilungen auftreten. Verstöße oder Falschinterpretationen regulatorischer Anforderungen stellen wiederum selbst ein NFR dar. [\(Siehe Flyer Regulatorische Agenda 2025\)](#)

### IKT- und Cyberrisiken

Mit DORA, NIS2 und CRA wächst der regulatorische Druck auf Unternehmen nahezu aller Sektoren und ihre Lieferketten zur Umsetzung wirksamer Sicherheitsmaßnahmen und den Aufbau von Risiko Managementsystemen. Neben technischen und organisatorischen Maßnahmen gängiger Standards fordert die Aufsicht eine Stärkung der digitalen operativen Resilienz. [\(Siehe Flyer DORA Prüfungsvorbereitung\)](#)

### Fraud Risk

Obwohl die 8. MaRisk-Novelle 2024 keine spezifischen Änderungen im Bereich der Betrugsrisiken (Fraud-Risiken) enthält, wird das Thema für ein angemessenes Risikomanagement zur Vermeidung von NFR für die BaFin voraussichtlich an Bedeutung gewinnen. Im Bereich des Kundenmonitorings sehen wir bei den Finanzinstituten einen erhöhten Nachholbedarf, insbesondere in Bezug auf die Nutzung von KI.

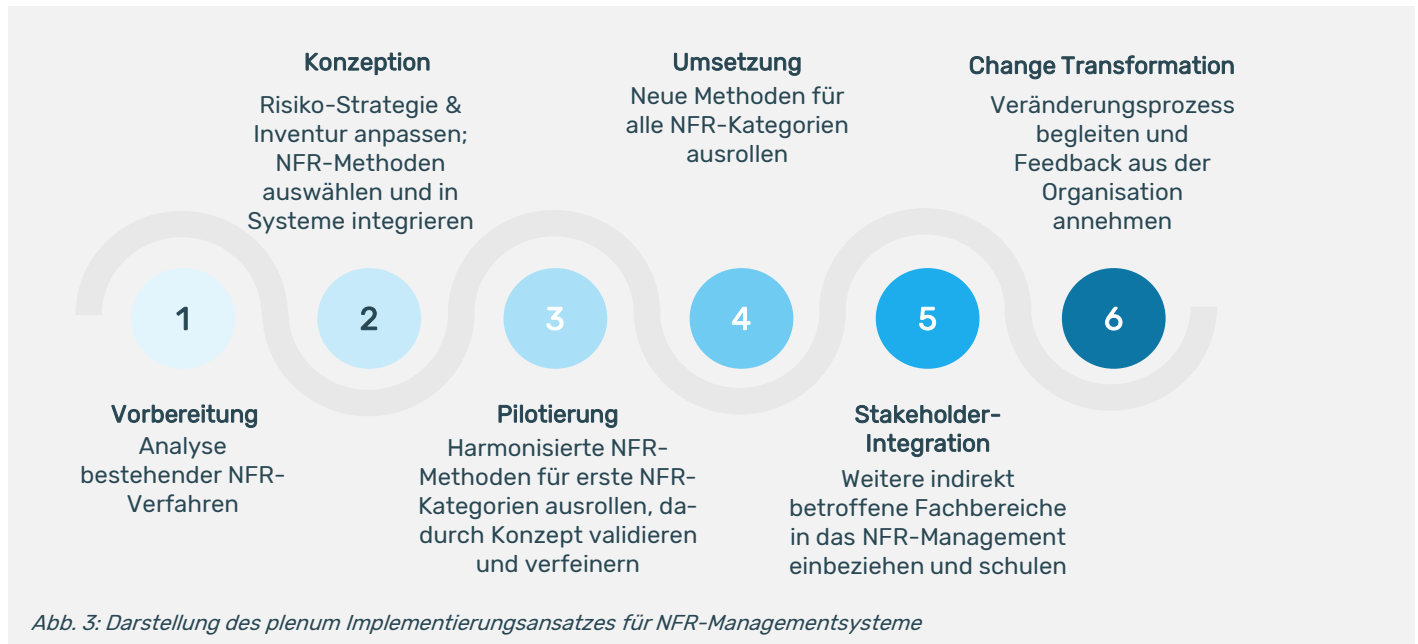
### Outsourcing Vendor Risk

Das Risiko durch Auslagerungen und die damit beauftragten Drittparteien wird für Finanzinstitute immer komplexer, nicht erst seit der Meldepflicht für wesentliche Auslagerungen seit 2022, sondern auch durch den Aufsichtsfokus 2025. Die BaFin hat explizit die Themen Ausfallrisiko von Mehrmandanten-Dienstleistern, Konzentration bei den Dienstleistern und Weiterverlagerung benannt.



## plenum Beratungsansatz

Unser Vorgehen zielt auf eine Verbesserung der NFR-Klammerfunktion für das Bank-Risikomanagement ab. Hierzu werden zunächst die unterschiedlichen Verfahren zur Steuerung der NFR abgeglichen. Im Anschluss wird eine einheitliche Methodik für das Management von NFR-Risiken konzeptioniert (z.B. Harmonisierung von Risikomatrizen). Darauf folgend wird die vereinheitlichte NFR-Methodik im Zuge der Phasen Pilotierung, Umsetzung und Stakeholder-Integration in den Fachbereichen implementiert. Hierdurch ausgelöste organisatorische Veränderungen sind durch einen Change-Prozess kulturell im Unternehmen zu verankern.



## Integriertes Risikomanagement

Finanzinstitute müssen im Rahmen der NFR zwei Stränge des Risikomanagements umsetzen. Zum einen das klassische Risikomanagement mit der Berechnung der Tragfähigkeit und der benötigten Eigenkapitalmittel gemäß den bankaufsichtsrechtlichen Vorschriften. Zum anderen die NFR-Managementanforderungen aus branchenübergreifenden gesetzlichen oder regulatorischen Anforderungen, wie DORA, CSRD, EmpCo-RL. Für beide Stränge gibt es überschneidende Methoden, aber auch dezidierte Methoden, die angewandt und validiert sein müssen. Hieraus ergeben sich für die Finanzinstitute zunehmend komplexere Prozesse und Verfahren, die in die vorhandenen Strukturen integriert werden oder für die neue Strukturen aufgebaut werden müssen.

## Pilotierungsansatz

Im Rahmen der Implementierung erfolgt zunächst die Pilotierung der harmonisierten NFR-Methoden für ausgewählte NFR-Risikokategorien. Durch diesen Ansatz können frühzeitig Rückmeldungen aus der Organisation und erste Erfahrungen mit den angepassten NFR-Methoden vor dem Roll-Out in die Gesamtorganisation zur Validierung und Verfeinerung der NFR-Methodik genutzt werden. Hierdurch wird der hohen Komplexität Rechnung getragen, die sich aus der Heterogenität der NFR-Risiken und der unterschiedlichen betroffenen Fachbereiche bei der Implementierung eines NFR-Risikomanagement-Ansatzes ergibt. Gleichzeitig führt der Pilotierungsansatz auch zu einer schnelleren Produktivnahme der NFR-Methoden in den Risikokategorien unter Vermeidung langer Implementierungszyklen. So werden durch das gewählte Vorgehen die Risiken aus mangelhaften Prozessen rechtzeitig erkannt und die Kosten für deren Änderungen reduziert.

Kommen Sie auf uns zu. Wir begleiten Sie mit unserem kompetenten und motivierten Beratungsteam von mehr als 150 Berater:innen und mit über 35 Jahren Erfahrung im Bereich Risk & Compliance bei führenden Finanzdienstleistern.

## Kontakt

Sprechen Sie gerne unser Risk & Compliance-Team an

[nfr@plenum.de](mailto:nfr@plenum.de)