ppi

Discussion Paper

IKT zwischen ESG-Risikomanagement und Data-Governance

Data Driven Finance im Wertschöpfungsprozess von Finanzdienstleistern

Jonas Martin, Mario H. Sladek, Aristedeus Tumaini

Wettbewerbsfaktor Informations- und Kommunikationstechnologie

Daten als Erfolgs- und Wertschöpfungsfaktor spielen eine immer wichtigere Rolle in Unternehmen und Banken. Sie sind der Kraftstoff, der den Motor, sprich die betrieblichen und Risikomanagementprozesse, antreibt. Die Fähigkeit, Informationen zu generieren und dadurch die Geschäftsziele zu erreichen, ist ob der Komplexität eine strategische Herausforderung und ein Wettbewerbsvorteil gleichermaßen.

Aus Unternehmenssicht ist die Datenverarbeitung auf Basis moderner Plattformtechnologien genauso bedeutend wie die Daten selbst. Die verarbeiteten Mengen nehmen dabei exponentiell zu. Das Data Warehouse ist ein seit Jahren geflügeltes Wort. Inzwischen kursieren aber auch Begriffe wie Data Lakes, quasi immer größer werdende Auffangbecken für enorme Mengen aufzuarbeitender Rohdaten. Die Rede ist von Big Data. Laut Prof. Joachim Wuermeling, Vorstandsmitglied der Deutschen Bundesbank, lag der Sektor Finanzdienstleistungen im Branchenvergleich mit 2,1 Zettabyte bereits 2018 auf Platz drei der größten Datenproduzenten. Das alles geschieht auf Grundlage fortschrittlicher Technologien wie Cloud-Lösungen oder algorithmenbasierter Verfahren. Beispiele für Letztere sind Advanced Analytics, Artificial Intelligence und Machine Learning. Alle diese Techniken können große, komplexe, strukturierte wie

unstrukturierte Datenmengen analysieren und interpretieren. Mithilfe von Advanced Analytics lassen sich tiefe Einblicke gewinnen, Vorhersagen treffen oder Empfehlungen geben, die weit über die Ergebnisse traditioneller Business Intelligence hinausgehen. Fast stakkatoartig schießen neue Lösungen und Anbieter aus dem Boden. Damit wird aber auch klar, dass die Wertschöpfung aus den Datenmengen deutlicher Leitplanken bedarf, sowohl organisatorisch als auch von aufsichtlicher Seite.

Erfolgs- und Risikofaktoren von IKT

Die Wertschöpfung von Banken hängt also in sehr hohem Maße vom Thema IKT und dem Management der inhärenten Risiken ab. Wenig verwunderlich, dass dieser Bereich immer stärker in die Prüfungsschwerpunkte der Aufsicht einfließt. Aber auch beim großen Zukunftsthema ESG als Beitrag der Banken zum nachhaltigen Wandel der Gesellschaft wird IKT zum Schlüsselfaktor. Denn ohne Digitalisierung ist eine Umsetzung der Anforderungen an die Steuerung von Nachhaltigkeitsrisiken unmöglich. Die Beherrschung von IKT-Risiken ist somit auch eine Grundvoraussetzung für ein umfassendes Nachhaltigkeits- beziehungsweise ESG-Risikomanagement in der Finanzbranche.

Unterschiedliche Wirkrichtungen

Der Begriff IKT-Risiko bezieht sich dabei auf das Risiko eines Verlustes aufgrund einer Vertraulichkeitsverletzung, eines Integritätsverlustes oder fehlender Leistungsfähigkeit und Verfügbarkeit von Systemen und Daten. Aber auch die (Un-)Fähigkeit, die IT in einem angemessenen Zeit- und Kostenrahmen an wandelnde Umfeld- oder Geschäftsanforderungen anzupassen, ist ein Risikofaktor. Dies betrifft nicht zuletzt transitorische Risiken durch den ökologisch nachhaltigen Wandel sowie die erkennbar zunehmenden Umwelt- und Klimarisiken. Dabei sind zwei Wirkrichtungen zu unterscheiden: einmal Outside-in, also in Richtung der Bank, und einmal vom Institut ausgehend. Bei Letzterem wird die Wirkung der Bank auf exogene Faktoren als Wirtschaftssubjekt selbst betrachtet. In dieser Kategorie kann sich auch das IKT-Risiko niederschlagen. Kann eine Bank ihre Kompetenz zur Beherrschung technologischer Herausforderungen im Nachhaltigkeitsmanagement nicht unter Beweis stellen, drohen neben einem Reputationsverlust noch weitere negative Folgen.

Die EBA hat bereits im Juli 2014 IT-Risiken in den Supervisory Review and Evaluation Process (SREP) aufgenommen und im Mai 2017 ein separates IT-SREP-Verfahren für bedeutende – Significant Institutes (SIs) – und weniger bedeutende Banken – Less Significant Institutes (LSIs) – initialisiert. Dadurch hat sich die Risikolandkarte für die Institute entsprechend erweitert. Ende Oktober 2017 wurden auch die Mindestanforderungen an das Risikomanagement (MaRisk) dahingehend überarbeitet und die Anforderungen des § 25a Kreditwesengesetz (KWG) gemeinsam mit den Bankaufsichtlichen Anforderungen an das IT-Management (BAIT) prinzipienbasiert konkretisiert.

Daten sind längst Vermögenswerte

Die aufsichtliche Bewertung achtet hierbei besonders auf IT-Governance und IT-Strategie der Banken. Dass die IKT-Risiken eine zentrale Bedeutung haben, ist inzwischen klar, da es der Aufsicht längst nicht mehr nur um die Sicherheit des den Banken anvertrauten Vermögens in Form von Kapital und Bargeld geht. Heute sind die den Banken anvertrauten und verarbeiteten Daten die neuen Vermögenswerte. Die Frage ist, wie IKT-Risiken aufgrund ihrer Bedeutung sowohl im Wertschöpfungsprozess von Banken als auch im SREP neben Geschäftsmodellanalyse (GMA), Governance, ICAAP[1] und ILAAP[2] als wesentliche Non-Financial Risks bewertet werden können. Die Elemente, die Funktionsfähigkeit und Effektivität des Three-Lines-of-Defence-Modells (TLoD) zur Steuerung von IKT-Risiken werden im Rahmen des SREP einem Assessment unterzogen und hinsichtlich ihrer Angemessenheit beurteilt. Bei Mängeln droht eine Sanktionierung durch die Aufsicht in Form einer höheren Risikoprofilnote respektive durch Kapitalzuschläge. Da sich SREP-Zuschläge als Äquivalent zu Risikogewichteten Aktiva (RWA) in der Säule 2 niederschlagen, sind diese als Materialitätskriterium zur Beurteilung der Wesentlichkeit von IKT-Risiken geeignet. Dies betrifft primär die Betrachtung der Vermögens- und Finanzlage im Rahmen der Risikotragfähigkeitsbetrachtung des Instituts.

Ohne Outsourcing beziehungsweise Leistungsbezug von Drittanbietern wären die IKT-Entwicklungs- und IKT-Betriebskosten von einzelnen Instituten kaum noch zu stemmen. Das bedeutet aber auch, dass die Leistungsbezieher weiterhin umfangreiche organisatorische und im Hinblick auf das Risikomanagement verbleibende Anforderungen erfüllen müssen. Die Relevanz der sogenannten Retained Organisation als wichtiges Instrument zur Performance- und Risikomessung für das Interne Kontrollsystem (IKS) beziehungsweise an der Schnittstelle zum Outsourcing-Anbieter steigt. Sparen an den dafür notwendigen Ressourcen ist nicht möglich, sie sind daher unbedingt in einer nachhaltigen Budgetplanung zu berücksichtigen. Im Ergebnis ist ohne ein effektives IKT-Risikomanagement und dessen Verankerung im IKS der Bank auch die Integration von ESG-Risiken in die Banksteuerung nicht angemessen darstellbar. Nachgelagert betrifft dies auch die Erfüllung diesbezüglicher Melde- und Offenlegungspflichten.

[1] Internal Capital Adequacy Assessment Process
[2] Internal Liquidity Adequacy Assessment Process

Interne Verfahren auf dem Prüfstand

Die Aufsicht hat zum Management von Nachhaltigkeitsrisiken bereits angekündigt, auch die Angemessenheit interner Verfahren zur Verarbeitung und Aggregation von Umwelt- und Klimarisikodaten zu überprüfen. Die Beurteilung entsprechender IKT-Risiken und insbesondere eine hinreichende ESG-Daten-Governance wird sich früher oder später auch in der SREP-Benotung niederschlagen. Bislang hat die Aufsicht ihre Erwartungshaltung nur an die Großen der Zunft adressiert. Mit Veröffentlichung der 7. MaRisk-Novelle bei den Verfahren zum ESG-Risikomanagement gilt die Prüfungsrelevanz nunmehr für alle Institute. Dies schließt eine diesbezügliche IT-Organisation und das Datenmanagement selbstredend mit ein.

Effektive Data-Governance für ein wirksames Management von ESG-Risiken

Die Aufsicht fordert von den Instituten die Entwicklung eines ganzheitlichen Ansatzes für die Daten-Governance, auch im Hinblick auf Klima- und Umweltrisiken. Denn Identifikation, Messung, Steuerung und Reporting beziehungsweise Offenlegung von Umwelt- und Klimarisiken erfordern valide Daten. In Zukunft kommen auch soziale Kriterien (Social) und Faktoren zur Beurteilung der Unternehmensführung (Governance) hinzu. Eine Auseinandersetzung vor allem mit steuerungsrelevanten Risikodaten und Bestimmungsfaktoren, der Fähigkeit zu deren Aggregation sowie den Berichtsverfahren im Zusammenhang mit ESG-Risiken ist Pflicht und Kür zugleich.

Die Einrichtung eines fortlaufenden und transparenten Prozesses für die interne und externe Berichterstattung dient der zeitnahen, präzisen, verständlichen und aussagekräftigen Erstellung der notwendigen Meldungen. Diese Berichte sollten wesentliche Informationen über die Ermittlung, Messung, Beurteilung, Überwachung und Steuerung von ESG-Risiken enthalten. Die dazu erforderlichen Daten und deren ergebnis- und risikoorientierte Verarbeitung sind das Fundament und Voraussetzung für die wirksame Überwachung und Steuerung von Nachhaltigkeitsrisiken.

Die Schaffung entsprechender Rahmenbedingungen für die Berichterstattung zu Klima- und Umweltrisiken in Verbindung mit den entsprechenden Kennzahlen ist keine Formalie. Hier kommt es insbesondere darauf an, Letztere konsistent zum Risikoappetit sowie im Risikomanagementprozess zu verorten. Mit einem soliden Berichtsverfahren lassen sich die Leistungen der Bank in Bezug auf Klima- und Umweltrisiken anhand valider Key-Performance-Indikatoren (KPIs) und der Offenlegung diesbezüglicher Informationen unterstützen.

Die Datenflut beherrschen

Aufgrund der sehr komplexen Bestimmungsfaktoren von Klima- und Umweltrisiken und einer regelrechten Datenflut ist eine Anpassung oder Weiterentwicklung der im Einsatz befindlichen IT-Systeme unvermeidbar. Jedes Institut sollte sich fragen, ob es bereits zu einer systematischen Erhebung und Aggregation erforderlicher Umwelt- und Klimarisikodaten in der Lage ist. Manche Banken hegen irrtümlicherweise die Erwartung, dass die Datentaxonomie diese Risiken in Zukunft per se einbezieht und quasi frei Haus aufbereitet.

Dabei liegt es in der Verantwortung der Institute, aggregierte und aktuelle Daten zu Klima- und Umweltrisiken zeitnah zusammenstellen zu können. Diese Erwartung deckt sich mit den EBA-Leitlinien, nach denen Institute künftig über wirksame und zuverlässige Informations- und Kommunikationssysteme verfügen müssen, die eine Sammlung von Risikodaten sowohl im normalen Geschäftsbetrieb als auch in Stressperioden zulassen. Die zeitnahe Bereitstellung muss transitorische Risiken, etwa im Zuge eines plötzlichen Übergangs zu einer kohlenstoffarmen Wirtschaft, berücksichtigen. Genauso ist die Einbeziehung möglicher physischer Einflüsse, seien es bei Unwetter- oder Umweltkatastrophen, auf den Geschäftsbetrieb eines Instituts obligatorisch.

Die Anpassungsfähigkeit – Agilität – der Institute wird hierbei auf die Probe gestellt. Es muss gewährleistet sein, dass aggregierte Daten zu Klima- und Umweltrisiken berichtet werden, um auch unterschiedlichste Ad-hoc-Datenanfragen bedienen zu können. Dazu zählen angesichts eines steigenden Bedarfs an Informationen zu Klima- und Umweltrisiken auch Anfragen in Stress- oder Krisenzeiten, solche aufgrund eines geänderten internen Bedarfs sowie die Beantwortung aufsichtlicher Informationsersuchen.

Daueraufgabe Datenvalidierung

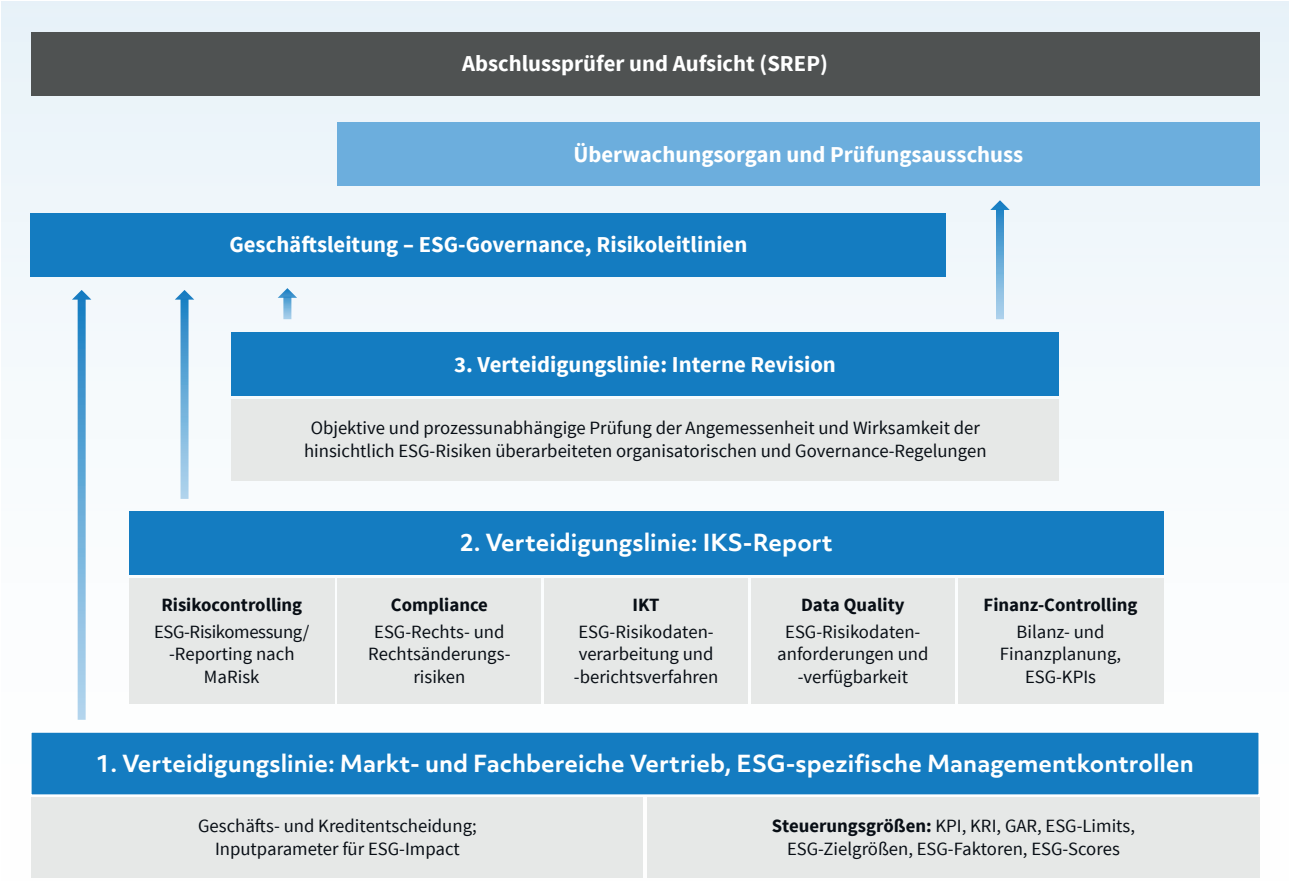
Künftig stehen erwartbar immer mehr Daten zur Ermittlung und Messung von Klima- und Umweltrisiken zur Verfügung. Daher wird im Kontext mit den Risikomanagementprinzipen unterstellt, dass Institute die Angemessenheit und Qualität vorhandener Datenquellen und Methoden regelmäßig validieren. Dies gilt unabhängig davon, ob die Informationen eingekauft oder eigenentwickelt sind. Diese Überprüfung ist eine Nagelprobe für die Überwachungsfähigkeiten im Rahmen des IKS, die Aussagefähigkeit verwendeter Kennzahlen und Angemessenheit von Limits zur Risikobegrenzung. Schlussendlich steht das Rahmenwerk für den Risikoappetit, die Risikotragfähigkeit und die Daten-Governance regelmäßig auf dem Prüfstand.

Im Einklang mit den Erwartungen der Aufsicht sollte sich in Zukunft der ESG-Risikoappetit gemäß der geschäfts- und risikostrategischen Maßgaben zur Berücksichtigung von Klima- und Umweltfaktoren in der Preisgestaltung von Krediten wiederfinden. Denkbar wäre etwa ein Zuschlagsfaktor einer ESG-risiko-adjustierten Ausfallwahrscheinlichkeit – Probability of Default (PD). Dorthin führende Verfahren sind Bestandteil des Kreditprozesses. Die relevanten Umwelt- und Klimadaten für das Risikomanagement, Controlling und Reporting von Adressrisiken müssen als wesentliches Element dafür im Datenhaushalt hinreichend enthalten sein.

Das Interne Kontrollsystem im Zielbild der IT-Governance

Durch die fortschreitende Digitalisierung bankgeschäftlicher Prozesse und Wertschöpfungsketten wächst die Bedeutung der Risiko- und Kontrollstruktur in Form des IKS. Das Beherrschen und Steuern von IKT-Risiken ist nicht nur eine aufsichtsrechtliche Anforderung, sondern Kernelement der Risiko- sowie Geschäftsstrategie. Eine effektive Kontrolle durch die Geschäftsleitung im Rahmen der Governance sowie eine Verankerung im Risikokulturprozess und Risk Appetite Framework (RAF) der Bank muss sichergestellt sein. Die einzelnen Aufgabenstellungen, Schnittstellen und Verantwortungsbereiche des IKT-Managements sind prozess- und funktionsübergreifend für eine funktionierende Governance verantwortlich. Ein entscheidendes Element der Unternehmensüberwachung und -steuerung von IKT-Prozessen und -Risiken ist das TLoD-Modell zur Abbildung von Aufbau, Zusammenwirken und Koordination innerhalb des IKS der Bank.

Three-Lines-of-Defence-Modell im ESG-Risikomanagement



Stresstests auch für IKT-Risiken

Die Prozesse des IKS stellen die Berücksichtigung von IKT-Risiken als wesentliche beziehungsweise sonstige materiell wichtige Risikoart im Rahmen der Risikotragfähigkeit sowie bei den Quantifizierungsverfahren sicher. Entsprechend der MaRisk sind Stresstests ein wesentliches Element des IKS. Aufgrund ihrer für die Aufrechterhaltung des Geschäftsmodells maßgeblichen Bedeutung und der intrinsisch hohen Schadenpotenziale sind IKT-Risiken grundsätzlich in interne Stresstestverfahren einzubeziehen. Ein weiterer elementarer Bestandteil sind Leitlinien zur Ermittlung und Kategorisierung wesentlicher IKT-Risiken in Übereinstimmung mit den EBA Guidelines für das Management von IKT- und Sicherheitsrisiken. Die Geschäftsleitung ist im Rahmen des TLoD-Modells für die wirksame Umsetzung von Regelungen zur IT-Governance institutsintern und gegenüber Dritten verantwortlich. Sie muss auch für eine angemessene Personalausstattung sorgen – insbesondere im Informationsrisiko- und Informationssicherheitsmanagement, im IT-Betrieb und der Anwendungsentwicklung. Hier liegt auch ein Schwerpunkt der Aufsicht.

Diese will so das Risiko einer qualitativen oder quantitativen Unterausstattung der genannten Bereiche frühzeitig erkennen und bekämpfen. Aus demselben Grund enthalten die BAIT die Anforderung, unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation zu vermeiden.

Self Assessment institutionell verankern

Dem IKS kommt dabei die entscheidende Aufgabe zu, die Einhaltung der IT-Governance prozess- und funktionsübergreifend sicherzustellen und die Verantwortungsstruktur für das IKT-Risikomanagement transparent abzubilden. Bei turnusmäßigen Review-Analysen sollte daher der Schwerpunkt auf der Beurteilung der Funktionsfähigkeit und Effektivität des TLoD-Modells zur Steuerung der IKT-Risiken unter Berücksichtigung von Angemessenheit und Risikokonzentrationen liegen. Im Anschluss lassen sich, entsprechend dem Risikoprofil, institutsspezifische Handlungsbedarfe ableiten, um eine Funktionsfähigkeit zu gewährleisten. In der Praxis ist hier das hauptsächlich im OpRisk-Managementprozess implementierte Self Assessment als spezifisches Instrument der Risikoinventur im Einsatz. Die hierfür erforderlichen Prozesse und Methoden sollten proportional zu den Anforderungen des jeweiligen Instituts definiert und in der schriftlich fixierten Ordnung verankert werden.

Fazit

Für die effektive und effiziente Steuerung von Umwelt- und Klimarisiken ist die rechtzeitige und umfassende Schaffung einer validen und konsistenten Geschäfts- und Risikodatenstruktur unter Gewährleistung der Datenqualität von immenser Bedeutung. Die Aufzeichnung klima- und umweltbezogener, extern und intern verarbeiteter Risikodaten gemäß ihrer Kategorisierung und Relevanz für das Geschäftsmodell ist eine umfassende und komplexe Aufgabe. Nur dadurch wird die Weiterentwicklung von entsprechenden Risikomodellansätzen, die Umwelt- und Klimarisiken als relevante Bestimmungsfaktoren abbilden, ermöglicht. Es gilt, die notwendigen Ressourcen für effektives ESG-Risikodatenmanagement rechtzeitig bereitzustellen. Dieses muss in eine strategiekonforme Data-Governance eingebunden sein und auf einer zukunftsgerichteten IKT aufbauen. Ähnlich wie bei neuen Produkten, Märkten oder zu implementierenden Prozessen müssen die Institute einen MaRisk-konformen, ganzheitlichen Anpassungs- und Weiterentwicklungsprozess durchlaufen.

Ansprechpartner

Jonas Martin
Senior Consultant
M +49 151 64189252
jonas.martin@ppi.de

Mario H. Sladek
Manager
M +49 175 2692789
mario.sladek@ppi.de

Aristedeus Tumaini
Senior Consultant
M +49 175 9315987
aristedeus.tumaini@ppi.de

Stand: Oktober 2022

www.ppi.de