

Zeitschrift für das gesamte
REDITWESEN

77. Jahrgang · 1. September 2024

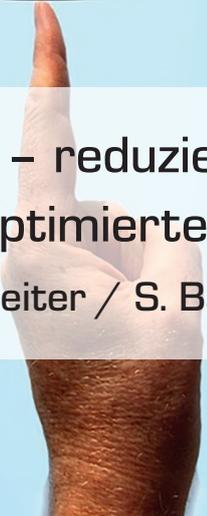
17-2024

**Digitaler
Sonderdruck**

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019



Externe Einflüsse auf das Bankgeschäft



Heuristik durch Holistik – reduzierte regulatorische
Aufwände und optimierte Steuerung

H. T. Renz / A. M. Marbeiter / S. Barth / S. Langhof

H. T. Renz / A. M. Marbeiter / S. Barth / S. Langhof

Heuristik durch Holistik – reduzierte regulatorische Aufwände und optimierte Steuerung

Seit Jahren nimmt die Anzahl von Daten, die Banken für Ihre kundenbezogenen Geschäfte aufsichtsrechtlich benötigen zu. Ein prägendes Beispiel hierfür sind die Anforderungen an die Kreditdatenstatistik (Analytical Credit Datasets – AnaCredit).¹⁾ Diese beinhalten beispielsweise 95 einzelne Vertrags- und Kreditdaten zur Meldung an das zentrale EZB-Kreditregister und betreffen im ersten Schritt nur juristische Personen.²⁾ Dies erschwert sowohl die Steuerung des Bank-, insbesondere des Kreditgeschäfts an sich, aber auch und gerade die Steuerung der, in diesem Fall kreditbezogenen, Risiken, die sich aus den datenbezogenen Prozessen der Banken ergeben können. Wenn dann noch eine nicht adäquate, in manchen Fällen sogar mangelhafte Qualität von Daten hinzukommt, stellt dies sowohl die Banksteuerung als auch das Risikomanagement vor erhebliche Herausforderungen.

Aufsichtsbehörden sehen diese Entwicklung sehr kritisch. Die BaFin hatte dies beispielsweise im Jahr 2021 in ihre Aufsichtsschwerpunkte aufgenommen. Sie beabsichtigte, auf die beaufsichtigten Unternehmen einzuwirken, ihre Datenqualität zu verbessern. Dabei standen 2021 die gesetzlichen Anforderungen an das Abwicklungsmeldewesen im Blickpunkt, die aus der Umsetzung des europäischen Bankenpakets im Risikoreduzierungsgesetz resultierten.³⁾

Aufsichtsschwerpunkte. Auch die EZB hatte beispielsweise im Jahr 2023 Datenqualität mit einem besonderen Fokus versehen. Zu den Aufsichtstätigkeiten zählten in diesem Jahr die Pilotphase des Managementberichts zur Daten-Gover-

nance und Datenqualität.⁴⁾ Die Bank for International Settlements (BIS) hatte dies im Jahr 2013 bereits mit dem BCBS 239 aufgegriffen.⁵⁾ Aufgabe der BIS ist es, die Zentralbanken in ihrem Streben nach Währungs- und Finanzstabilität durch internationale Zusammenarbeit zu unterstützen und als Bank für Zentralbanken zu agieren.⁶⁾ Der BCBS 239 legt die Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung aus Sicht des Basler Ausschusses für Bankenaufsicht (Basel Committee on Banking Supervision – BCBS) fest.⁷⁾

Die EZB hat sich nun aufgrund ihrer Erkenntnisse aus ihrer Aufsichtstätigkeit 2023 dieses Themas erneut angenommen und am 3. Mai 2024 den Leitfaden für effektive Risikodaten Aggregation und Risikoberichterstattung (Guide on effective risk data aggregation and risk reporting – RDARR) veröffentlicht.⁸⁾ Der Leitfaden skizziert die Voraussetzungen für eine wirksame Risikodatenaggregation und Risikoberichterstattung, um die Banken bei der Stärkung ihrer Fähigkeiten zu unterstützen, wobei er auf den in der Branche beobachteten bewährten Verfahren aufbaut.

Der Leitfaden soll die Erwartungen der Aufsichtsbehörden in diesem Bereich präzisieren und verstärken, wobei BCBS 239 hierbei berücksichtigt wird. Der Leitfaden ergänzt und ersetzt allerdings nicht die bereits seit 2016 schon in öffentlichen Mitteilungen und bei institutsspezifischen Aufsichtstätigkeiten gegebenen Hinweise der EZB.⁹⁾ Diese Vorgaben finden sich in der Aufsichtspraxis der BaFin über MaRisk AT 4.3.4¹⁰⁾ selbstverständlich auch für die von ihr hierzu beaufsichtigten Institute wieder.

Die Finanzbranche steht unter zunehmendem Druck, sowohl komplexe regulatorische Anforderungen zu erfüllen als auch effiziente und effektive betriebliche Prozesse aufrechtzuerhalten. In diesem Spannungsfeld spielt die Qualität der zugrunde liegenden Daten eine entscheidende Rolle. Insbesondere für das Topmanagement und die Führungskräfte ist es unerlässlich, die Bedeutung einer holistischen Herangehensweise an Datenqualität zu verstehen. Ein solcher Ansatz kann nicht nur den regulatorischen Aufwand erheblich reduzieren, sondern auch die gesamte Unternehmenssteuerung optimieren.

Zunehmende regulatorische Anforderungen

Ein politisch kommunizierter und von vielen Instituten aber auch Verbrauchern gewünschter Bürokratieabbau ist (noch) nicht ersichtlich. Gerade in der Finanzindustrie nehmen die regulatorischen Anforderungen sogar immer noch zu. Ein Paradebeispiel hierfür ist die europäische Verordnung zur digitalen operationellen Resilienz von Unternehmen der Finanzindustrie (Digital Operational Resilience Act – DORA¹¹⁾), der am 17. Januar 2025 von den betroffenen Instituten in der EU umgesetzt sein muss und in Deutschland beispielsweise die von der BaFin veröffentlichten Bankaufsichtlichen Anforderungen an die IT (BAIT¹²⁾) ablösen wird.

In der europäischen Regulatorik ist es mittlerweile Usus, auch bei in allen EU 27 Staaten direkt geltenden Verordnungen, eine Vielzahl sogenannter regulatorisch-technischer und implementierungs-tech-



nischer Standards (RTS/ITS) zu verabschieden. Ein RTS soll eine EU-Verordnung beziehungsweise eine EU-Richtlinie präzisieren. Ein ITS als technischer Durchführungsrechtsakt soll die einheitliche Anwendung gewisser Bestimmungen im zugrunde liegenden Rechtsakt sicherstellen. Bei der DORA sind aktuell insgesamt 12 RTS/ITS/Guidelines zur näheren Präzisierung der DORA-Vorgaben geplant. Dieses Thema ist der BaFin mittlerweile so bedeutend, dass sie für DORA mittlerweile eine eigene Website eingerichtet hat.¹³⁾

Nicht nur die Regulatorik an sich nimmt zu, auch die Anzahl der Aufsichtsbehörden, die für deren Einhaltung und die Überwachung der hiervon betroffenen Institute zuständig sind. Ein aktuelles Beispiel dafür ist die Geldwäscheprevention, die derzeit einen besonderen Fokus in der aufsichtsrechtlichen Überwachung durch die BaFin einnimmt.¹⁴⁾ Das Finanzkriminalitätsbekämpfungsgesetz bildet die Grundlage, eine Bundesoberbehörde zur Bekämpfung von Finanzkriminalität zu errichten.¹⁵⁾ Wesentlicher Teil ist die Errichtung eines Ermittlungszentrums Geldwäsche (EZG).¹⁶⁾ Das neue Bundesamt zur Bekämpfung von Finanzkriminalität (BBF) werde mit dem Bundeskriminalamt (BKA) durch die Errichtung einer Gemeinsamen Ermittlungsgruppe (GEG) verzahnt.¹⁷⁾ Die künftige Organisationsstruktur beinhaltet die Zentralstelle für Sanktionsdurchsetzung (ZfS) und die Zentralstelle für Finanztransaktionsuntersuchungen und diese werden von der Generalzolldirektion (GZD) in das BBF am 1. Juni 2025 überführt.¹⁸⁾ Im BBF solle es künftig eine Zentralstelle für Geldwäschaufsicht (ZfG) geben.¹⁹⁾ Dies diene der „Stärkung eines einheitlichen, stringenten risikobasierten Ansatzes bei der Geldwäschaufsicht über den Nichtfinanzsektor sowie der bundesweiten Koordinierung und Unterstützung von geldwäscherechtlichen Aufsichtsmaßnahmen“.²⁰⁾

Darüber hinaus wird Mitte 2025 auch die Anti-Money Laundering Authority (AMLA) als zuständige Geldwäschepreventionsbehörde für die EU in Frankfurt am Main ihre Tätigkeit aufnehmen.²¹⁾ Die AMLA wird auch die direkte Aufsicht über wenige ausgewählte (erheblich risikoreiche) Fi-

nanzunternehmen – bezogen ebenso auf Anbieter von Kryptowertedienstleistungen – übernehmen.²²⁾ Ein politisch gewolltes komplexes Aufsichtskonstrukt, dem sich als betroffenes Institut nur begegnen lassen wird, wenn man auf Basis eines Datenhaushaltes mit adäquater Datenqualität seine Risikosteuerung auch und gerade auch zur Steuerung von Risiken aus der Geldwäscheprävention optimiert ausrichten kann.

Die Bedeutung von Data Governance

Data Governance ist der Eckpfeiler jeder Strategie zur Verbesserung der Datenqualität. Sie umfasst die Schaffung von Richtlinien, Prozessen und Verantwortlichkeiten, die sicherstellen, dass Daten innerhalb einer Organisation auf konsistente, genaue, verlässliche und sichere Weise verwaltet werden. Data Governance ist nicht nur eine technische oder IT-Aufgabe, sondern ein unternehmensweiter Auftrag, der stark von der Führungsebene getragen werden muss.

Eine solide Data Governance beginnt mit der Definition klarer Datenstandards und der Etablierung von Rollen, die für die Pflege und Überwachung der Datenqualität verantwortlich sind. Diese Standards müssen regelmäßig überprüft und aktualisiert werden, um den sich ändernden Anforderungen gerecht zu werden. Effektive Data Governance stellt sicher, dass Daten entlang der gesamten Datenstrecke konsistent und zuverlässig sind, was die Grundlage für alle weiteren Schritte in der Datennutzung und im Datenmanagement bildet.

Datenqualität und die Erfüllung regulatorischer Anforderungen

Für das Management bedeutet dies, dass die aus einer starken Data Governance resultierende hohe Datenqualität nicht nur die operative Effizienz verbessert, sondern auch das Vertrauen in die Daten und alle daraus resultierenden Entscheidungen stärkt. Eine gut implementierte Data Governance hilft, (Daten-)Silos²³⁾ aufzubrechen und eine unternehmensweite

RA Hartmut T. Renz



Partner Regulatory, Risk & Compliance Advisory, STRATECO GmbH, Bad Homburg v. d. Höhe

Andreas M. Marbeiter



Director Regulatory, Risk & Compliance Advisory, STRATECO GmbH, Bad Homburg v. d. Höhe,

Sebastian Barth

Senior Manager Advisory – Data & Analytics, STRATECO GmbH, Bad Homburg v. d. Höhe

Sebastian Langhof

Director Advisory – Data & Analytics, STRATECO GmbH, Bad Homburg v. d. Höhe

Seit Jahren nimmt die Anzahl von Daten, die Banken für ihre kundenbezogenen Geschäfte aufsichtsrechtlich benötigen, zu. Wenn dann noch eine nicht adäquate, in manchen Fällen sogar mangelhafte Qualität von Daten hinzukomme, stelle dies laut den Autoren sowohl die Banksteuerung als auch das Risikomanagement vor erhebliche Herausforderungen. Zur Verbesserung der Datenqualität empfiehlt der Beitrag eine „Data Governance“. Diese beginne mit der Definition klarer Datenstandards und der Etablierung von Rollen, die für die Pflege und Überwachung der Datenqualität verantwortlich sind. Zudem raten die Autoren zu einer holistischen Herangehensweise. Ein „weiter so“ im Rahmen fragmentierter Implementierungsprozesse bei der Regulatorik könne am Ende auch Haftungsrisiken für Vorstände und Aufsichtsräte bedeuten. (Red.)

Datenkultur zu fördern, die auf Qualität und Genauigkeit ausgerichtet ist.

Die Qualität der Daten ist von zentraler Bedeutung für die Einhaltung regulatorischer Vorgaben, insbesondere im Kontext von RDARR (Risk Data Aggregation and Risk Reporting)²⁴⁾ und den BCBS 239 Grundsätzen²⁵⁾ des Basler Ausschusses. Diese internationalen Standards verlangen von Banken, dass sie ihre Risikodaten aggregieren und präzise berichten können, um fundierte Entscheidungen zu treffen und potenzielle Risiken frühzeitig zu identifizieren. Ohne eine hohe Datenqualität ist es nahezu unmöglich, diesen Anforderungen gerecht zu werden.

BCBS 239 legt fest, dass Daten vollständig, korrekt, aktuell und für die Nutzer

zugänglich sein müssen. Dies setzt eine Infrastruktur voraus, die sicherstellt, dass Daten richtig erhoben, gespeichert und verarbeitet werden. Fehlerhafte oder unvollständige Daten können nicht nur zu falschen Risikoeinschätzungen führen, sondern auch zu erheblichen regulatorischen Sanktionen. Daher ist es entscheidend, dass Banken und Finanzinstitute die Qualität ihrer Daten kontinuierlich überwachen und verbessern.

Eine adäquate Datenqualität erfordert eine systematische Herangehensweise, bei der Daten regelmäßig auf ihre Konsistenz und Genauigkeit überprüft werden. Dies beinhaltet auch die Implementierung von Datenqualitäts-Management-Tools, die automatisierte Prüfungen und Bereinigungen ermöglichen. So können Datenfehler frühzeitig erkannt und behoben werden, bevor sie zu größeren Problemen führen.

Die Rolle der MaRisk in Deutschland

Neben den internationalen Anforderungen durch BCBS 239 müssen sich Banken und Wertpapierinstitute in Deutschland auch an die Mindestanforderungen an das Risikomanagement (MaRisk²⁶) der BaFin halten. Diese Anforderungen sind spezifisch auf die nationale Regulierung zugeschnitten und ergänzen die internationalen Vorgaben. Die MaRisk betonen insbesondere die Bedeutung einer robusten Dateninfrastruktur, die es ermöglicht, Risikodaten genau und zeitnah zu erfassen und zu verarbeiten.

Für das Topmanagement bedeutet dies, dass eine enge Abstimmung zwischen den operativen Einheiten und dem Risikomanagement erforderlich ist, um sicherzustellen, dass alle relevanten Daten den regulatorischen Anforderungen entsprechen. Eine Missachtung der MaRisk kann nicht nur zu rechtlichen Konsequenzen führen, sondern auch das Vertrauen der Aufsichtsbehörden in die Bank untergraben. Die Sicherstellung einer hohen Datenqualität ist daher nicht nur eine Frage der Compliance, sondern auch eine strategische Notwendigkeit, um langfristig wettbewerbsfähig zu bleiben. Banken, die ihre Datenqualität vernachlässigen, riskieren nicht nur regulatorische

Sanktionen, sondern auch eine ineffiziente Steuerung ihrer Geschäftsprozesse.

Verbesserung der Datenqualität und Risikobewertung

Data Analytics ist ein mächtiges Werkzeug, das nicht nur zur Sicherstellung, sondern auch zur kontinuierlichen Verbesserung der Datenqualität eingesetzt werden kann. Durch die Analyse großer Datenmengen können Muster, Trends und Anomalien identifiziert werden, die auf potenzielle Probleme hinweisen. Data Analytics ermöglicht es, Fehlerquellen zu erkennen, bevor sie zu größeren Problemen führen, und so die Datenqualität proaktiv zu verbessern.

Ein weiterer Vorteil von Data Analytics ist die Fähigkeit, prädiktive Analysen durchzuführen. Diese Analysen ermöglichen es Banken, zukünftige Trends und Risiken zu antizipieren und entsprechende Maßnahmen zu ergreifen. Dies ist besonders im Kontext von RDARR und BCBS 239 von Bedeutung, da diese Standards einen proaktiven Ansatz zur Risikobewertung erfordern.

Schritte zur Sicherstellung adäquater Datenqualität

Für das Management bedeutet der Einsatz von Data Analytics, dass Entscheidungen auf einer fundierten Datenbasis getroffen werden können. Dies führt zu einer höheren Genauigkeit in der Risikobewertung und einer besseren Steuerung der Geschäftsprozesse. Data Analytics trägt somit nicht nur zur Erfüllung regulatorischer Anforderungen bei, sondern auch zur Verbesserung der operativen Effizienz und Effektivität.

Um eine adäquate Datenqualität zu gewährleisten, sind mehrere strategische Maßnahmen erforderlich. Diese Schritte sollten als kontinuierlicher Prozess verstanden werden, der ständiger Überprüfung und Anpassung bedarf. Hier sind die wichtigsten Maßnahmen, die Banken und Finanzinstitute ergreifen sollten:

Etablierung einer umfassenden Data Governance: Dies ist der erste und wichtigste

Schritt zur Sicherstellung der Datenqualität. Data Governance umfasst die Definition klarer Datenstandards, die Implementierung von Prozessen zur Datenüberwachung und -pflege sowie die Festlegung von Verantwortlichkeiten. Eine effektive Data Governance stellt sicher, dass Daten konsistent, genau und für die richtigen Nutzer zugänglich sind.

Implementierung von Datenqualitäts-Management-Tools: Diese Tools ermöglichen die kontinuierliche Prüfung der Daten auf Konsistenz, Genauigkeit und Vollständigkeit. Sie identifizieren fehlerhafte Datenfehler und Inkonsistenzen und bieten Lösungen zur Korrektur an. Automatisierte Tools können einen Großteil der manuellen Arbeit bei der Datenpflege ersetzen und so die Effizienz steigern.

Kontinuierliche Schulung und Sensibilisierung: Mitarbeiter auf allen Ebenen sollten regelmäßig geschult werden, um das Bewusstsein für die Bedeutung der Datenqualität zu schärfen. Schulungen sollten sich nicht nur auf technische Aspekte konzentrieren, sondern auch auf die strategische Bedeutung von Datenqualität für das gesamte Unternehmen.

Integration von Data Analytics: Data Analytics kann eine wichtige Rolle bei der Sicherstellung der Datenqualität spielen, indem es Muster und Anomalien in den Daten identifiziert, die auf potenzielle Fehler oder Risiken hinweisen. Durch den Einsatz von Analysetools können Unternehmen ihre Daten besser verstehen und gezielte Verbesserungen vornehmen.

Adäquate Datenqualität als Schlüssel zum Erfolg

Die Sicherstellung einer adäquaten Datenqualität ist von entscheidender Bedeutung für das Risikomanagement und die Erfüllung regulatorischer Anforderungen. Ohne qualitativ hochwertige Daten ist es unmöglich, die Anforderungen von BCBS 239, RDARR und MaRisk zu erfüllen und gleichzeitig eine effiziente und effektive Unternehmenssteuerung sicherzustellen. In der Vergangenheit lag der Fokus oft zu stark auf vergangenheitsbezogenen



Daten. Doch die Aufsichtsbehörden erwarten zunehmend einen zukunftsorientierten („looking forward“) Ansatz im Risikomanagement, der nur auf der Grundlage einer soliden Datenbasis möglich ist. Mit einer adäquaten Datenqualität können Banken nicht nur die Anforderungen der Aufsichtsbehörden erfüllen, sondern auch ihre internen Prozesse effizienter gestalten und so Kosten und Ressourcen schonen.

Die positiven Folgen einer hohen Datenqualität sind weitreichend: Sie führt zu einer höheren Qualität in der Banksteuerung, im Risikomanagement und in der regulatorischen Compliance. Darüber hinaus trägt sie zur Haftungsvermeidung für Führungskräfte bei, indem sie sicherstellt, dass alle relevanten Risiken frühzeitig erkannt und adressiert werden können. In einer zunehmend komplexen und regulierten Finanzwelt ist es daher unerlässlich, die Datenqualität als strategischen Erfolgsfaktor zu betrachten. Ein holistischer Ansatz, der auf einer robusten Data Governance und dem gezielten Einsatz von Data Analytics basiert, bietet die Grundlage, um regulatorische Aufwände zu reduzieren und gleichzeitig die langfristige Wettbewerbsfähigkeit zu sichern.

Reduzierung von regulatorischen Aufwänden

So simpel und sachlogisch sich der Ruf nach zuverlässiger Datenqualität auch anhört, in der Realität stehen die meisten Häuser vor komplexen Herausforderungen. Und dabei geht es nicht nur um die Datenhaushalte per se, sondern um die fachlichen Notwendigkeiten ihrer Genese. Und diese hat mehrere Gründe und Prämissen:

– Unternehmen, die schon längere Zeit bestehen, starten nicht mehr auf einer grünen Wiese. Im Gegenteil. Der laufende Betrieb beruht oftmals auf jahrebeziehungsweise jahrzehntelang gewachsenen Datenstrukturen. Diese haben im Laufe der Zeit hunderte von Schnittstellen generiert und reflektieren mittlerweile eine Vielzahl verschie-

dener Datentöpfe, die eine mehr oder minder große gemeinsame Schnittmenge haben, jedoch je nach Ziel und Vorgabe ihrer fachlichen Existenz eine individuelle Anreicherung von Informationen erfahren haben.

– Diese Datentöpfe werden in der Regel immer größer und komplexer, dies bedingt durch die permanente Weiterentwicklung in Bezug auf die fachliche Notwendigkeit, aufgrund derer diese Datentöpfe geschaffen wurden. Eine Rückkopplung und laufende Aktualisierung in Richtung der „Master-Datei“, aus der dieser Datentopf entstanden ist, findet nur in wenigen Fällen – wenn überhaupt – statt.

– Fachlich findet zwischen den Abteilungen, die eine individuelle Entwicklung ihrer Datenhaushalte vorantreiben, kaum ein Austausch über gemeinsame fachliche Zielsetzungen statt. Zu dringlich werden die jeweils individuellen, in aller Regel regulatorisch getriebenen, Fachanforderungen eingestuft. Die Genehmigung eines individuellen Budgets ist die oberste Prämisse, die eigene Verantwortlichkeit erfüllen zu können.

– Dabei ist es den Aufsichtsbehörden selbst vollkommen klar, dass es keine Kontrollsicherheit gibt, die 100 Prozent Abdeckung gewährleistet. Deshalb wird diese auch nicht gefordert. Wichtig ist aber eine organisatorische Struktur, anhand derer es eine angemessene und akzeptierte Risikoabdeckung gibt, die entsprechend dokumentiert ist.

– Diese 100-Prozent-Kontrollabdeckung ist oftmals betriebswirtschaftlich so teuer und aufwendig zu realisieren, dass sich hier die Frage nach ihrer unternehmerischen Sinnhaftigkeit stellt.

– Die Addition der beiden vorgenannten Punkte ergibt in der Summe das Ergebnis, dass es ab einer gewissen Größenordnung der Kontrollerledigung nicht mehr sinnvoll, wirtschaftlich und auch unter Risikogesichtspunkten erforderlich ist, faktische Prüfungen vorzunehmen. Stattdessen ist eine Einschätzung auf Basis der bisherigen Ergebnisse, Daten und

Erfahrungen durchaus zielführend. Dieser Ansatz für die Lösung komplexer Probleme durch das intuitive Ausprobieren und Anwenden spezifischer Strategien ist jedoch umso effektiver, je belastbarer die Erkenntnisse aus den etablierten und mittels faktischer Kontrollen gewonnener Ergebnisse sind. Spätestens an dieser Stelle vereinen sich der Nutzen und die Effektivität von Heuristik, Holistik und Datenqualität.

– Die Komplexität der regulatorischen Anforderungen nimmt immer mehr zu. So widersprüchlich es sich ausnehmen mag, so real ist doch der Fakt, dass gerade im Zuge des Vorhabens nach europäischer Harmonisierung immer mehr Stakeholder seitens der Kontrollorgane und der Regelentwickler ihre Finger im Spiel haben. Die Kombination europäischer und deutscher Normengeber trägt somit erst recht zu einer aufsichtlichen Komplexität bei – mögliche Widersprüche nicht ausgenommen.

Hausinterne Prozesse bieten viele Ansatzpunkte

Viel wichtiger als eine reine Aufzählung aller relevanten Gesetze und Vorgaben, die sich ohnehin alle in der Risikoanalyse des Unternehmens wiederfinden müssten, ist die Allokation der hausinternen Zuständigkeiten an die jeweiligen Fachabteilungen und ob es hierüber einen regelmäßigen Austausch gibt. Es ist und bleibt leider illusorisch, darauf zu hoffen, dass es eine Möglichkeit der Einflussnahme auf Behörden, Regulatoren und politische Gremien gibt, eine Vereinheitlichung zugleich mit einer Komplexitätsreduktion einhergehen zu lassen. Mit Blick auf das eigene Unternehmen jedoch ist eine direkte Einflussnahme nicht nur möglich, sondern sogar zwingend erforderlich. Warum also nicht dort beginnen, wo das Formulieren von Vorgaben und die Gestaltung von Prozessen in der eigenen Hoheit liegt?

Die Nutzung externer Software zur Einhaltung geforderter Kontrollerfordernisse ist in der heutigen Zeit unumgänglich. Allerdings fordert jede neue Software

eine weitere Schnittstelle an bestehende Datenhaushalte einerseits und kreiert andererseits neue Datenhaushalte, die in ihrer Konsistenz spätestens ab t+1 nicht mehr mit den ursprünglichen Datenhaushalten in anderen Bereichen des Unternehmens kompatibel sind.

Weitere Parameter wären dieser Aufstellung sicherlich noch hinzuzufügen. Die Ausgangslage ist aber bereits anhand der hier dargestellten Aufzählung deutlich. Dabei ist die alles entscheidende Frage, ob diese Aufgabe überhaupt lösbar ist.

Die Bedeutung einer holistischen²⁷⁾ Herangehensweise in der Regulatorik

Auf den ersten Blick ist es alles andere als offensichtlich, welche Gemeinsamkeiten ein Compliance-Beauftragter nach WpHG mit einem(r) Compliance-Beauftragten nach MaRisk, einem(r) Geldwäschebeauftragten, einem(r) Informationssicherheitsbeauftragten, einem(r) Datenschutzbeauftragten oder einem(r) Auslagerungsbeauftragten haben. Zu unterschiedlich sind die einzelnen Zielrich-

tungen für die jeweiligen Kontrollergebnisse, die aus den einschlägigen Gesetzen und Verordnungen in diesem Themengebiet zu berücksichtigen sind. Dieses Bild ändert sich aber schlagartig, wenn nicht die reine Fachlichkeit im Fokus der Betrachtung steht, sondern die Methodik, die zu der jeweiligen Zielerreichung angewandt wird. Die Suche nach gemeinsamen Nennern bringt erstaunliche Ergebnisse hervor:

- Die Ausgangsdaten sind für nahezu alle Bereiche identisch. Es geht um Daten der Kunden, um Daten der angebotenen Produkte und Dienstleistungen in Verbindung mit den technisch eingesetzten Verfahren, um Unternehmensdaten, die mit Produkten und Technik in Verbindung stehen, um erforderliche Lizenzen und Erlaubnisse für die angebotenen Dienstleistungen, um die geforderte Fortsetzung des operativen Betriebs im Falle von Störfällen und um den geforderten Schutz für Kunden- und Unternehmensdaten.
- Auf Basis der einschlägigen Gesetzgebungen müssen alle Funktionen zunächst einmal eine unternehmensspezi-

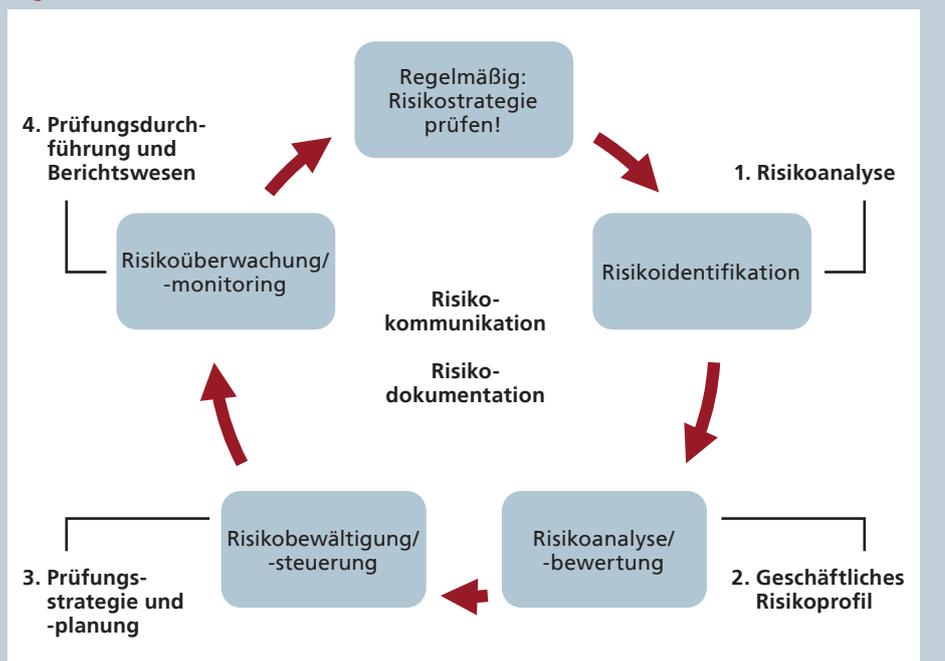
fische Risikosituation ermitteln, um die potenziellen Einfallstore und damit das Bruttoisiko im Unternehmen ermitteln zu können. Dabei haben alle Bereiche viele Gemeinsamkeiten. Es geht um den gleichen Kundenbestand, die gleiche Technik, die gleichen Schutzmaßnahmen für die „Basisdaten“ und die gleichen Stakeholder in den Themenbereichen. Eine jeweils bereichsinterne Bewertung der gemeinsamen Basiskomponenten ist somit nicht (mehr) erforderlich. Sie bringt sogar die Gefahr mit sich, dass unterschiedliche Bereich die gleichen Sachverhalte unterschiedlich bewerten.

- Im nächsten Schritt ermitteln alle Bereiche die erforderlichen Sicherungsmaßnahmen²⁸⁾, die es benötigt, um das Bruttoisiko angemessen zu reduzieren.
- Danach erfolgt die Entwicklung eines eigenen Kontrollplans, mit dem die Effektivität der Sicherungsmaßnahmen und der damit verbundenen Kontrollhandlungen in Stichproben geprüft werden soll. Dies fällt umso leichter, wenn es ein hausintern funktionierendes internes Kontrollsystem gibt, das an den kritischen Schnittpunkten der Prozesse hinreichende Schlüsselkontrollen etabliert hat.

- Als nächster Schritt erfolgt die operative Abarbeitung des eigenen Kontrollplans, die (fortlaufende) Berichterstattung und die Definition von Abhilfemaßnahmen, sofern es Auffälligkeiten gibt. Diese Arbeitsschritte sind wesentlich, wenn es um die effiziente Steuerung der Geschäftsprozesse geht. Dabei sind es in aller Regel fast überall identische Geschäftsprozesse in der operativen ersten (Verteidigungs-)Linie, auf die eine Kontrolle reflektiert, ganz gleich, ob sie vom Geldwäschebeauftragten oder einem Compliance-Beauftragten oder einem Sicherheitsbeauftragten durchgeführt wird.

- Nachfolgend beginnt der Prozess aufs Neue.

Abbildung 1: Schematische Darstellung des Vorgehens in allen regulatorischen Bereichen



Quelle: H. Renz, A. Marbeiter, S. Barth, S. Langhof



wie in Abbildung 1 dargestellt standardisieren.

Trotz unterschiedlicher Gesetzgebung lassen sich die Risiken aus der Nichteinhaltung von gesetzlichen Vorgaben einheitlich formulieren, ganz gleich, ob es sich dabei um Vorgaben aus dem WpHG, dem GWG, der MaRisk, der DSGVO oder dem IT-Sicherheitsgesetz handelt. Die Gestaltung der Fragestellung in Verbindung mit der Definition der zuzuordnenden Sicherungsmaßnahmen ist dabei von essenzieller Bedeutung.

Gibt es für diese Ansätze bereits Beispiele? Die gibt es. Ein Blick auf den Bereich der ISO-Standards²⁹⁾ (siehe Abbildung 2) zeigt eine thematische Vielfalt, die die unterschiedlichsten Themenbereiche tangieren und in denen die Finanzdienstleistungsindustrie nur einen kleinen Teilbereich ausmacht. Und dennoch haben alle ISO-Standards, nach denen sich ein Unternehmen zertifizieren lassen beziehungsweise sich daran ausrichten kann, eines gemeinsam:

Diese Darstellung, die doch stark an den oben dargelegten regulatorischen Risikomanagementkreislauf erinnert, hat nicht nur die beschriebenen Abläufe gemeinsam. Ganz gleich, welcher ISO-Standard betrachtet wird: Sogar die Nummerierung der Kapitel ist bei (nahezu) allen Standards identisch. Lediglich die zu erreichenden fachlichen Ziele variieren von Themengebiet zu Themengebiet.

Deshalb ist es auch als Unternehmen einfach, sich nach verschiedenen Standards zertifizieren zu lassen. Wenn einmal der betriebliche Kernprozess etabliert und beschrieben ist, dann lassen sich daran alle weiteren Vorgehensweisen zu unterschiedlichen Themenbereichen daran andocken.

Bedeutung der Holistik für die Datenqualität

Regulatorische Holistik ermöglicht es den Unternehmen, trotz unterschiedlicher fachlicher Inhalte und Vorgaben eine einheitliche methodische Vorgehensweise

Abbildung 2: Anforderungen an eine Managementsystemnorm



Quelle: TRECCERT

zur Zielerreichung für nahezu alle Themenbereiche eines Hauses zu etablieren.

Das stärkt die eigentliche Ausgangsbasis der Datenhaushalte und reduziert das Auseinanderdriften allein schon dadurch, dass „fachliche Abzweigungen“ erst viel später im Prozessablauf vorgenommen werden müssen und sich dadurch weniger Datensilos bilden, die am Ende trotz einheitlicher Kundendaten unterschiedliche Aussagen abbilden. Das festigt die Datenqualität. Auch die Ausgangslage für die Bewertung von Prüfungserkenntnissen basiert auf soliden und keinesfalls indifferenten Datenmustern. Damit ist die Herleitung heuristisch erlangter Erkenntnisse weitaus fundierter und ermöglicht einen zuverlässigeren Antritt für eine 100-Prozent-Abdeckung regulatorischer Anforderungen, betriebswirtschaftliche Aspekte eingeschlossen. Und es kann der Beweis erbracht werden, dass mit einem innovativen Ansatz Regulatorik und Betriebswirtschaft nicht immer diametral auseinanderlaufen müssen. Wichtig ist hierfür jedoch der Mut, bei der hausinternen Umsetzung der Regulatorik einen holistischen Weg einzuschlagen und sei er gerade zu Beginn noch so mühselig.

Ein „weiter so“ im Rahmen fragmentierter Implementierungsprozesse bei der Regulatorik gefährdet die Datenqualität, den Erkenntnisgewinn aus darauf aufbauenden Kontrollen, die darauf aufbauende Banksteuerung und die Betriebswirtschaft. Das davon ausgehende Haftungsrisiko für Geschäftsleiter und Aufsichtsräte der Institute wird an dieser Stelle nur der guten Ordnung halber noch erwähnt.

Hinsichtlich der Mitarbeiterprofile, die erforderlich sind, um diesen Weg erfolgreich einzuschlagen, ist ein Aspekt besonders wichtig: Fachkompetenz hinsichtlich der regulatorischen Grundlagen spielt nicht die Hauptrolle. Viel wichtiger für die Synthese zwischen Holistik und Heuristik sind hierfür Methoden- und Prozesskompetenz.

Die ausführliche Version dieses Beitrag mit Fußnotenverzeichnis können Sie auf unserer Homepage kreditwesens.de unter Eingabe des Titels und /oder des Autorennamens abrufen.