Hein/Scheve (Hrsg.)

Handbuch Datenmanagement

Qualität, Aggregation und Nutzbarmachung von Risikodaten in Banken und Sparkassen

2. Auflage

Finanz Colloquium Heidelberg, 2022

Zitiervorschlag:

Autor in: Hein/Scheve (Hrsg.), Handbuch Datenmanagement, 2. Auflage, RdNr. XX.

Hinweis: Zur besseren Lesbarkeit und Unterstützung des Leseflusses wurde im nachfolgenden Buch auf die Verwendung des generischen Maskulinums zurückgegriffen. Selbstverständlich schließen jedoch alle Formulierungen und Personenbezeichnungen alle Geschlechter gleichermaßen ein.

ISBN: 978-3-95725-975-2

Finanz Colloquium Heidelberg GmbH
Im Bosseldorn 30, 69126 Heidelberg
www.FCH-Gruppe.de
info@FCH-Gruppe.de
Satz: Finanz Colloquium Heidelberg GmbH
Druck: VDS-VERLAGSDRUCKEREI SCHMIDT,
Neustadt an der Aisch

Hein/Scheve (Hrsg.)

Handbuch Datenmanagement

Qualität, Aggregation und Nutzbarmachung von Risikodaten in Banken und Sparkassen

2. Auflage

Pino-Sun Becker
Vice President Group Compliance
ACOLIN Europe AG
Konstanz

Mario Dütsch-Willmann
Datenqualitätsmanager
Hamburgische Investitions- und Förderbank

Dr. Karsten Foos
Leiter Anwendungsentwicklung Corporate Center
Helaba Landesbank Hessen-Thüringen

Andreas Freßmann
Prokurist, Leiter Revision
Volksbank Beckum-Lippstadt eG

Markus Frommlet
Fachberater DQM Kundenmanagement
FOCONIS AG
Hamburg

Heiko Hackbarth
Senior Referent | Data Governance Office
Berliner Sparkasse
Berlin

Lutz Hansen
Geschäftsführender Gesellschafter
HmcS Gruppe
Hannover

Dr. Manfred Hein (Hrsg.)
Leiter Projekte
FOCONIS AG
Hamburg

Carmen Heinemann
Dipl.-Informationsjuristin (FH) und IT-Compliance-Managerin (TÜV)
AE Data Warehouse/Business Intelligence
Helaba Landesbank Hessen-Thüringen

Sandra Holz
Chief Data Officer | Leitung Data Governance-Office
Berliner Sparkasse
Berlin

Hooshang Jafarpour
Methoden- und Produktmanager
parcIT GmbH

Kersten Kaufmann
Director Direct Sales
Deutsche Post Adress GmbH & Co. KG
Gütersloh

Jürgen Krug
IT-Revisor, stellv. Abteilungsleiter Zentralrevision
Frankfurter Sparkasse
Frankfurt am Main

Eva-Maria Scheiter
Head of GRC Consulting Cyber Security
NTT DATA Deutschland GmbH
Köln

Dr. Stefan Scheve (Hrsg.)
Sachgebietsleiter Laufende Aufsicht Sparkassen
Deutsche Bundesbank, Hauptverwaltung in Hannover

Dr. Joachim Selke
Head of BICC, Data Governance & Data Strategy
Volkswagen Bank

Finanz Colloquium Heidelberg, 2022

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACL	Access Control List
ADV	Allgemeine Datenverarbeitung
ALMM	Additional Liquidity Monitoring Metrics
AnaCredit	Analytic Credit Dataset
AUM	Assets under Management
AT	Allgemeiner Teil
BA	Bankenaufsicht
BAIT	Bankaufsichtlichen Anforderungen an die IT
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BI	Business Intelligence
BIA	Business-Impact-Analyse
BIZ	Bank für Internationale Zusammenarbeit
BL	Bereichsleitung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Besonderer Teil
BTO	Besonderer Teil (Organisation)
CSSF	Commission de Surveillance du Secteur Financier
CDO	Chief Data Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CNIL	Commission Nationale de l'Informatique et des Libertés
CMDB	Configuration Management Database
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COREP	Common Solvency Ratio Reporting
COVID-19	Coronavirus-Erkrankung
CPV	Credit Portfolio View

CRR	Capital Requirements Regulation
CSA	Cloud Security Alliance
CSV	Comma Separated Values
CVAR	Credit Value at Risk
DAMA	Data Management Association International
DDQ	Due Diligence Questionnaire
delVO	Delegierte Verordnung
DF	Datenfeld
DGO	Data Governance Office
DMZ	Demilitarisierte Zone
DQ	Datenqualität
DQM	Datenqualitätsmanagement
DSAnpUG	Datenschutz-Anpassungs- und -Umsetzungsgesetz
DSGVO	Datenschutzgrundverordnung
D-SIB	Domestic Systemically Important Banks
DV	Datenverarbeitung
DWH	Data Warehouse
EBA	European Banking Authority
EC	Economic Capital
EDV	Elektronische Datenverarbeitung
EIOPA	European Insurance and Occupational Pensions Authority
EL	Expected Loss
ESMA	European Securities and Markets Authority
EU AMLD	EU-Richtlinien zur Geldwäschebekämpfung
EZB	Europäische Zentralbank
FinaRisikoV	Finanz- und Risikotragfähigkeitsinformationenverordnung
FinaV	Finanzinformationsverordnung
FINREP	Financial Reporting
FISA	Foreign Intelligence Surveillance Act
FIU	Financial Intelligence Unit

GL	Guideline
GL	Geschäftsleitung
GoBD	Grundsätze ordnungsgemäßer Führung und Aufbewahrung von Büchern auch in elektronischer Form und zum Datenzugriff
G-SIB	Global Systemically Important Banks
HQ	Headquarter
ICI	Investment Company Institute
ICT	Information and Communications Technology
ID	Identifikator
IDV	Individuelle Datenverarbeitung
IFM	Investment Fund Manager
IFRS	International Financial Reporting Standards
IKS	Internes Kontrollsystem
ILM	Information Lifecycle Management
IQ	Informationsqualität
IQM	Informationsqualitätsmanagements
ISACA	Information Systems Audit and Control Association
ISM	Informationssicherheitsmanagement
ISO	International Organization for Standardization
IST	Implementing Technical Standard
KI	Künstliche Intelligenz
KPI	Key Performance Indicators
KRITIS	Kritische Infrastrukturen
KWG	Kreditwesengesetz
KYD	Know Your Distributor
LCR	Liquidity Coverage Ratio
LDAP	Lightweight Directory Access Protocol
LEI	Legal Entity Identifier
LGD	Loss Given Default
LiqV	Liquiditätsverordnung

LSI	Less Significant Institutions
MaRisk	Mindestanforderungen an das Risikomanagement
NACE	Statistische Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft
NIST	National Institute of Standards and Technology
NIV	Nettoinventarwert
NP	Natürliche Person
NSFR	Net Stable Funding Ratio
OpVAR	Operational Value at Risk
PbD	Privacy by Default
PD	Probability of Default
PIMS	Personal Information Management-Systeme
PKI	Public Key Infrastructure
PrüfbV	Prüfungsberichtsverordnung
RACF	Resource Access Control Facility
RPO	Recovery Point Objective
RTF	Risikotragfähigkeit
RTO	Recovery Time Objective
SDM	Standard-Datenschutzmodell
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SQL	Structured Query Language
SREP	Supervisory Review an Evaluation Process
SSM	Single Supervisory Mechanism
TXT	Text
Tz.	Textziffer
UBO	Ultimate Beneficial Owner

UCITS	Undertakings for Collective Investments in Transferable Securities
VPN	Virtual Private Network
ZAG	Zahlungsdiensteaufsichtsgesetz
ZVAdr	Zentrale Vorverarbeitung Adressenrisiko

Vorwort

Schon seit einiger Zeit und weiterhin zunehmend liegen Daten und deren Nutzung – nicht zuletzt aufgrund des Schlagworts Digitalisierung – im Fokus der Aufmerksamkeit. Digital vorliegende Daten bzw. Informationen bilden verstärkt die Grundlage für unsere (geschäftlichen) Entscheidungen. Dieses gilt insbesondere für die Risiken, die jedes Unternehmen für sich einschätzt und bewertet. Ein professioneller Umgang mit Daten in Banken und Sparkassen wird immer wichtiger bzw. ist zwingend notwendig – insbesondere in den Bereichen Risikocontrolling und -reporting, Meldewesen und Revision. Der verstärkte Fokus der Aufsicht richtet sich auf Datenqualität und IT-Risiken. Dies zeigen nicht nur die Vorgaben, die unter dem Stichwort BCBS 239 schon 2013 bekannt geworden sind, sondern auch die seit 2017 geltenden BAIT.

Das nunmehr in der zweiten Auflage vorliegende Buch widmet sich diesen Risikodaten im Hinblick auf Qualität, Verarbeitung und Prüfung. Die am 16.08.2021 von der BaFin veröffentlichte überarbeitete Version der BAIT wurde eingearbeitet. Die ebenfalls von der Aufsicht im August 2021 veröffentlichte sechste MaRisk-Novelle liegt nun der vorliegenden Auflage zu Grunde. Im Vergleich zur ersten Auflage erfolgte eine umfassende Überarbeitung. So wurden einige Kapitel aufgrund einer besseren thematischen Zuordnung in der Reihenfolge verschoben. Insbesondere enthält das Buch aber auch fünf neue Kapitel. Somit wird nun im Kapitel »Aufsichtsrechtliche Anforderungen an Bank-IT-Daten« die Erweiterung der BAIT auf nunmehr zwölf Kapitel erläutert. Im Bereich Datenmanagement wurde das Kapitel »Informations- und IT-Sicherheit als Grundlage für erfolgreiches Datenmanagement« hinzugefügt. Die »Selbstplausibilisierung von Kundenstammdaten« wird nun im Kapitel des Datenqualitätsmanagements beleuchtet. Der Bereich der Erfahrungsberichte wurde in der vorliegenden zweiten Auflage ausgebaut. Hier ist auf die neuen Kapitel »Datenmanagement im Immobiliengeschäft«, »KYD-Datenmanagement – Wo geht die Reise hin?« und »Relevanz von Kontaktdaten« hinzuweisen.

Das Buch richtet sich an Neueinsteiger sowie an erfahrene Spezialisten aus den Bereichen Risikomanagement/Risikocontrolling, Compliance, Revision, Organisation, Kredit und IT. Empfehlenswert ist dieses Handbuch auch für das Management von Banken und Sparkassen. Viele Beiträge lassen mit ihren konkreten Beispielen die Wichtigkeit begreifbar werden und zeigen auf, welche Fallstricke die Umsetzung einer Informations- bzw. Datenmanagementstrategie mühsam und aufwendig gestalten können. Das vorliegende Werk bietet umfangreiches Wissen, Empfehlungen und Erfahrungen auf vielen Ebenen zum

Umgang mit Daten im Allgemeinen und zum Umgang mit Risikodaten innerhalb von Kreditinstituten im Speziellen. Dabei werden Themen wie

- regulatorische Vorgaben
- Data Governance
- Datenmanagement
- IT-Sicherheit
- Datenqualitätsmanagement und
- Prüfung Datenqualität

beleuchtet.

Das Buch beginnt mit den aufsichtsrechtlichen Anforderungen ergänzt um Erfahrungen aus der Aufsichtspraxis und steigt dann in das Thema Data Governance und Datenmanagementstrategie ein. Mit dem nachfolgenden Thema Datenmanagement werden die Herausforderungen bei der Verarbeitung von Daten betrachtet. Hierbei erfahren die Bereiche Meldewesen und Risikomanagement eine besondere Aufmerksamkeit. Die Qualität der Daten steht nachfolgend im Mittelpunkt.

Direkt im Anschluss befinden sich die Beiträge mit Erfahrungs- und Praxisberichten sowie Beiträge zu Spezialthemen. Diese Beiträge sind in ihrer Reihenfolge von den Anforderungen über Strategie, Management, Datenqualität bis hin zur IT angeordnet.

Dieses Buch kann traditionell von vorne nach hinten gelesen werden. Der Leser erhält so einen umfangreichen Einblick in die verschiedenen Themenbereiche. Zusätzlich kann es genutzt werden, um zu einem der behandelten Themen schnell einen praxisrelevanten Überblick zu erhalten. Die Gliederung des Buches ermöglicht dazu einen schnellen Einstieg in das gewünschte Thema.

Abschließend möchten wir uns bei allen Autoren, die mit ihrem Engagement, ihrer Geduld und ihrer Bereitschaft, ihr Wissen und ihre Erfahrungen mit anderen zu teilen, dieses Handbuch ermöglicht haben, ganz herzlich bedanken.

Wir wünschen eine interessante Lektüre und viel Freude an den beim Lesen gewonnenen Gedanken.

Die Herausgeber

Dr. Stefan Scheve Dr. Manfred Hein

A.

Aufsichtsrechtliche Anforderungen an Bank-IT-Daten

A. Aufsichtsrechtliche Anforderungen an Bank-IT-Daten[1]

I. Zunehmende Bedeutung von Datenqualität und IT-Risiken

Sowohl Daten, die der Deutschen Bundesbank im Rahmen des Meldewesens aufgegeben werden, als auch Daten bzw. Datenbanken, die im internen Berichtswesen eines Kreditinstituts verwendet werden, sollten zuverlässig und frei von Fehlern sein. Leider ist dies nicht immer der Fall. Zahlen und Daten sind ggf. auf Grund von persönlichen Fehlern nicht korrekt erfasst worden. Diese Betrachtung ist aber nur eine Seite der Medaille. Eine schlechte bzw. geringe Datenqualität ist – neben Falscherfassungen – regelmäßig auf Probleme bei falschen Schnittstellen, fehlerhaften Programmadditionen oder fehlgeleiteten Daten zurückzuführen. Systematische Fehler sind grundsätzlich bedeutender als individuelle Einzelmängel, da sie wiederholt und ggf. regelmäßig auftreten. 1

Unzulänglichkeiten in der Datenverfügbarkeit und -sicherheit sind in den letzten Jahren in den Fokus der Aufsicht gerückt. Auch öffentlich gewordene Defizite – teilweise von Presse und Fernsehen ausführlich dargestellt – haben hierzu beigetragen. Die Abhängigkeit von EDV- bzw. IDV-Anwendungen hat stetig zugenommen. Somit sind Daten- bzw. IT-Risiken in den letzten Jahren weltweit stärker in den bankenaufsichtlichen Fokus gerückt. Unter dem Stichwort BCBS 239 hat der Basler Ausschuss für Bankenaufsicht (Banking Committee on Banking Supervision) der Bank für Internationalen Zahlungsausgleich (BIZ, Bank for International Settlement) schon im Jahr 2013 wegweisende Vorgaben gesetzt.[2] Im Jahre 2017 wurden wesentliche BCBS 239-Vorgaben durch die fünfte MaRisk-Novelle als zwingende Vorgaben für deutsche Banken und Sparkassen eingeführt. Weitere Vorgaben setzen die 2017 eingeführten und im Jahr 2021 umfassend überarbeiteten »Bankaufsichtlichen Anforderungen an die IT (BAIT)«. 2

1 Die nachfolgenden Interpretationen und Meinungen sind ausschließlich persönliche Auffassungen des Verfassers und stellen keine offizielle Meinungsäußerung der Deutschen Bundesbank dar.

2 Mittlerweile hat der Basler Ausschuss eine deutsche Übersetzung der Principles/Grundsätze des BCBS 239 veröffentlicht. Diese ist auf der BIZ-Website verfügbar: www.bis.org. Vgl. *Bank für Internationalen Zahlungsausgleich*: Basler Ausschuss für Bankenaufsicht: Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung, Januar 2013.

II. Vorgaben aus Basel zu Risk Data Aggregation und Risk Reporting (BCBS 239) und BSI- bzw. ISO-Standards

3 Am 09.01.2013 hat die BIZ mit dem Standard BCBS 239 Principles für Risikodatenaggregation und das entsprechende Berichtswesen veröffentlicht. Diese Principles/Vorgaben sind zwar im Adressantenkreis an große Institute (G-SIBs und D-SIBs) gerichtet, wirken sich aber indirekt auch auf alle Banken und Sparkassen in Deutschland aus.

4 Die BIZ hat 14 Prinzipien benannt, von denen 11 an die Kreditinstitute und die letzten 3 an die Bankenaufsicht gerichtet sind. In 4 Bereiche können die Prinzipien eingeteilt werden.

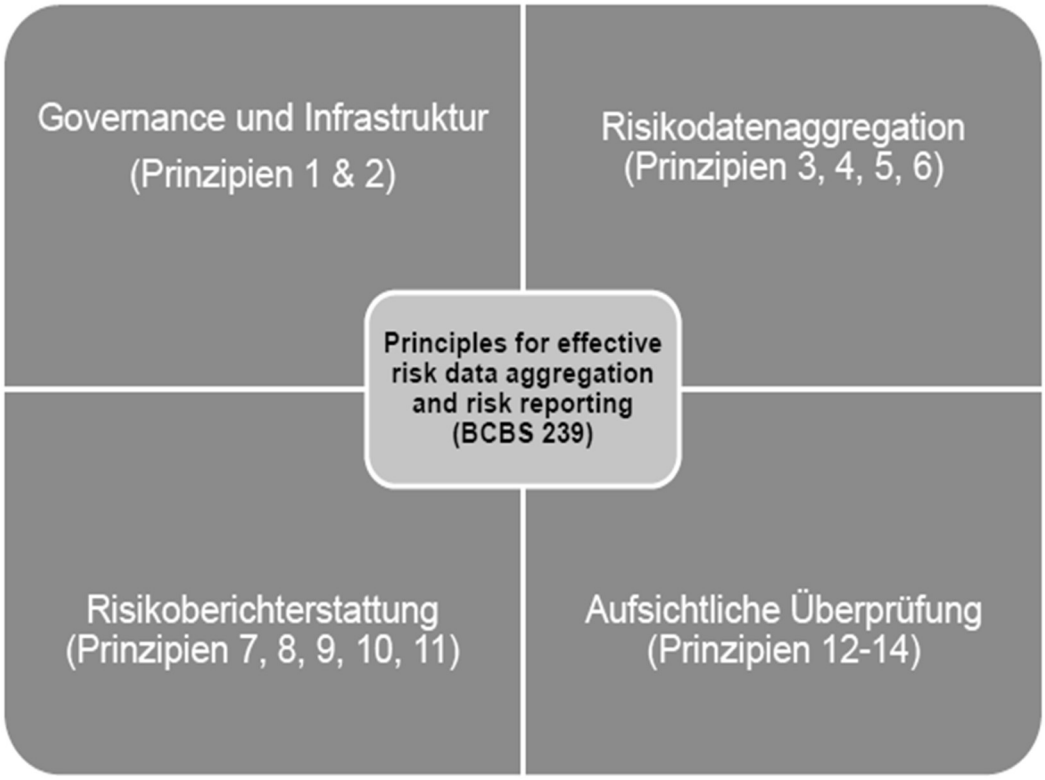

Abbildung: Prinzipien zu Data Aggregation & Risk Reporting laut BCBS 239 (Quelle: BIZ, Basler Ausschuss für Bankenaufsicht)

5 Unter dem Prinzip 1 (Governance) wird die Zuständigkeit des Topmanagements für die Vorgabe von klaren und konsistenten Regelungen für die Aggregation von Risikodaten und Risikoberichten betont. Die Verankerung in der IT-Strategie gehört ebenfalls hierzu.

Die Datenarchitektur und die IT-Infrastruktur müssen nach Prinzip 2 die Aggregation von Risikodaten und das Risikoreporting sowohl in normalen Zeiten als auch in Krisenzeiten gewährleisten. 6

Genauigkeit und Integrität werden mit Prinzip 3 angesprochen. Bei der Individuellen Datenverarbeitung (IDV) und bei manuellen Prozessen, die grundsätzlich zu reduzieren sind, müssen Kontrollen durchgeführt werden. Aggregationsprozesse sind grundsätzlich zu automatisieren. Somit ist eine passende Balance zwischen automatisierten und manuellen Prozessen zu finden. Genauigkeit und Integrität der Daten sind zu messen und zu überwachen. Abweichungstoleranzen sind festzulegen. 7

Gemäß Prinzip 4 müssen Daten vollständig sein. Es ist zwischen wesentlichen und unwesentlichen Risikodaten zu unterscheiden. 8

Prinzip 5 gibt vor, dass Daten aktuell sein müssen. Die Systeme müssen insbesondere in Stress- bzw. Krisenzeiten die Aktualität der Daten sicherstellen. 9

Die Anpassbarkeit der Daten wird mit Prinzip 6 gefordert. Die Datenhaltung muss so anpassungsfähig sein, dass auch ad-hoc-Anfragen schnell und flexibel erledigt werden können. 10

Für die Risikoberichterstattung gibt Prinzip 7 vor, dass die Risikoberichte genau sein müssen. Die Qualität der Berichte hat nicht schlechter zu sein als diejenige im Rechnungswesen. 11

Prinzip 8 spricht den Umfang der Riskoberichterstattung an. Risikoberichte sollen umfassend sein. Sie haben alle wesentlichen Inhalte abzubilden. Handlungsempfehlungen sollen aufgezeigt werden. Über den Stand der Umsetzung beschlossener Maßnahmen ist zu berichten. 12

Prinzip 9 fordert die Verständlichkeit. Die Inhalte der Risikoberichte müssen verständlich und klar formuliert sein. 13

Eine schnelle Verfügbarkeit von Daten auch in Krisenzeiten wird durch Prinzip 10 mit Vorgaben zur Frequenz gefordert. Die Häufigkeit der Berichtserstellung ist zu definieren. 14

Die Verteilung der Berichte hat zeitnah, vertraulich und adressatengerecht zu erfolgen. Somit werden mit Prinzip 11 Vorgaben zum Empfängerkreis gesetzt. 15

Die Prinzipien 12 bis 14 richten sich an die Aufsicht. Die Aufsichtsbehörden haben die Einhaltung der zuvor genannten Prinzipien regelmäßig zu überwachen und zu bewerten; auch unter Beachtung von Stressszenarien. Defizite sind 16

durch aufsichtliche Maßnahmen zügig zu beseitigen. Die Aufsichtsbehörden sollten zudem grenzüberschreitend kooperieren.

17 Die am 27.10.2017 veröffentlichte fünfte MaRisk-Novelle übertrug die Prinzipien der BCBS 239 proportional in deutsche Vorgaben. Somit wurden die Erwartungen der deutschen Aufsicht an Banken und Sparkassen in Deutschland für die Risikodatenaggregation und Risikoberichterstattung konkretisiert.

18 Ergänzend wird in diesem Kapitel auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) und auf die International Organisation for Standardization hingewiesen. Beide Institutionen geben wichtige Vorgaben, die sich in den MaRisk und den BAIT wiederfinden. So gibt das BSI das Grundschutzkompendium (IT-Grundschutzkataloge) heraus. Internationale Sicherheitsstandards (insbesondere ISO Standards 270xx) stammen von der International Organisation for Standardization. Die Kreditinstitute sind nach MaRisk und BAIT verpflichtet, bei der Ausgestaltung der IT-Systeme und der IT-Prozesse auf gängige Standards abzustellen.

III. Angepasste MaRisk-Vorgaben durch die fünfte und sechste Novelle der MaRisk (mit Bezug zu BCBS 239)

1. Grundsätze für das Datenmanagement, die Datenqualität und die Aggregation von Risikodaten mit Gültigkeit für große Institute

19 Mit der fünften MaRisk-Novelle[3] ist das neue Modul AT 4.3.4 »Datenmanagement, Datenqualität und Aggregation von Risikodaten« in die MaRisk aufgenommen worden. Dieses Modul gilt – auch nach der sechsten MaRisk-Novelle in 2021[4] – für systemrelevante Institute auf Gruppenebene als auch auf der Ebene der wesentlichen gruppenangehörigen Einzelinstitute. Der AT 4.3.4 enthält in 7 Textziffern (Tzn.) umfassende Vorgaben. So sind instituts- und gruppenweit geltende Grundsätze festzulegen, die von der Geschäftsleitung zu genehmigen und in Kraft zu setzen sind (Tz. 1). Auch nach der in 2021 veröffentlichen sechsten MaRisk-Novelle gelten diese Vorgaben weiterhin.

3 Vgl. *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)*: Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben 09/2017 (BA) vom 27.10.2017.

4 Vgl. *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)*: Mindestanforderungen an das Risikomanagement – MaRisk, Rundschreiben 10/2021 (BA) vom 16.08.2021.

Datenstruktur und -hierarchie müssen eine zweifelsfreie Identifikation, Zusammenführung, Auswertung und zeitnahe Zurverfügungstellung gewährleisten (Tz. 2). 20

Die Genauigkeit und Vollständigkeit der Daten müssen gewährleistet werden. Die Daten müssen nach unterschiedlichen Kategorien auswertbar und automatisiert aggregierbar sein. Manuelle Prozesse und Eingriffe müssen begründet, dokumentiert und auf das inhaltliche Maß beschränkt werden. Die Qualität und Vollständigkeit der Daten müssen anhand geeigneter Kriterien überwacht werden (Tz. 3). 21

Die Risikodaten müssen mit anderen Informationen (z. B. Daten aus dem Rechnungswesen und ggf. dem Meldewesen) – unter Einsatz von Verfahren zur Identifizierung von Datenfehlern und Schwachstellen – abgeglichen und plausibilisiert werden (Tz. 4). 22

Die Kapazitäten zur Datenaggregation müssen gewährleisten, dass aggregierte Daten sowohl unter normalen Umständen als auch in Stressphasen zeitnah zur Verfügung stehen. Ein zeitlicher Rahmen, innerhalb dessen die Daten vorliegen müssen, ist zu definieren. In Stressphasen müssen z. B. folgende Risikodaten vorliegen: 23

- Kreditrisiko auf Gesamtbankebene,
- aggregiertes Exposure gegenüber großen Schuldnern,
- Handelspositionen und -limite,
- Kontrahenten- und Marktpreisrisiken,
- Indikatoren für Liquiditäts- und operationelle Risiken (Tz. 5).

Zudem müssen die Datenaggregationskapazitäten ausreichend leistungsfähig und flexibel sein, um ad-hoc-Informationen nach unterschiedlichen Kriterien ausweisen und analysieren zu können (Tz. 6). 24

Für alle Prozessschritte sind Verantwortlichkeiten festzulegen und prozessabhängige Kontrollen einzurichten. Die Einhaltung der institutsinternen Regelungen, Verfahren, Methoden und Prozesse muss regelmäßig überprüft werden. Diese Überprüfung hat von einer von den operativen Einheiten unabhängigen Stelle (mit hinreichenden Kenntnissen) zu erfolgen (Tz. 7). 25