Hein/Scheve (Hrsg.)

Handbuch Datenmanagement

Qualität, Verarbeitung und Prüfung von (Risiko-)Daten in Banken & Sparkassen

Finanz Colloquium Heidelberg, 2019

Zitiervorschlag:

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

ISBN: 978-3-95725- 036-0

Im Bosseldorn 30, 69126 Heidelberg
www.FCH-Gruppe.de
info@FC-Heidelberg.de
Satz: MetaLexis, Niedernhausen
Druck: Strauss GmbH, Mörlenbach

Hein/Scheve (Hrsg.)

Handbuch Datenmanagement

Qualität, Verarbeitung und Prüfung von (Risiko-)Daten in Banken & Sparkassen

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

Andreas Freßmann
Stabstellenleiter
Volksbank Beckum-Lippstadt eG

Markus Frommlet
Fachberater DQM
emagixx GmbH
Hamburg

Heiko Hackbarth
Senior-Referent
Data Governance Office
Berliner Sparkasse
Berlin

Dr. Manfred Hein (Hrsg.)
Leiter Projekte
emagixx GmbH
Hamburg

Carmen Heinemann
Projektmanagerin und Coach ECM |
Agilität | IT-Compliance | Digitalisierung
Helaba Landesbank Hessen-Thüringen

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

Hooshang Jafarpour
Spezialist Modellrisiko & Validierung
Postbank – eine Niederlassung der DB Privat- und Firmenkundenbank AG
Bonn

Peter Kaminski
Specialist Cyber Security (CISSP, CEH, CISA, CRISC)
Abteilung Cyber Security
Santander Consumer Bank AG

Jürgen Krug
IT-Revisor, stellv. Abteilungsleiter Zentralrevision
Frankfurter Sparkasse
Frankfurt/M.

Dr. Stefan Scheve (Hrsg.)
Sachgebietsleiter Sparkassen Hauptverwaltung Hannover
Deutsche Bundesbank
Hannover

Dr. Joachim Selke
Leiter BICC & Risiko-Datenstrategie
Volkswagen Bank GmbH

Finanz Colloquium Heidelberg, 2019

Inhaltsübersicht

Abkürzungsverzeichnis **1**

A. Aufsichtsrechtliche Anforderungen an Bank-Daten **7**

B. Data Governance und Datenmanagementstrategien **29**

C. Datenmanagement **41**

D. Datenqualitätsmanagement **97**

E. Erfahrungsberichte und Praxisbeispiele **135**

Inhaltsverzeichnis

Abkürzungsverzeichnis **1**

Vorwort *(Hein/Scheve)* **5**

A. Aufsichtsrechtliche Anforderungen an Bank-Daten *(Scheve)* **7**

I. Zunehmende Bedeutung von Datenqualität und IT-Risiken 9

II. Vorgaben aus Basel zu Risk Data Aggregation und Risk Reporting (BCBS 239) 10

III. Neue bzw. angepasste MaRisk-Vorgaben durch die fünfte Novelle der MaRisk mit Bezug zu BCBS 239 12

1. Grundsätze für das Datenmanagement, die Datenqualität und die Aggregation von Risikodaten mit Gültigkeit für große Institute 12

2. Angepasste MaRisk-Vorgaben zu Datenqualität und IDV mit Gültigkeit für alle Institute 13

3. Vor und mit der fünften MaRisk-Novelle gültige Vorgaben zum Datenmanagement für alle Institute 14

IV. Bankaufsichtliche Anforderungen an die IT (BAIT) 15

1. IT-Strategie 16

2. IT-Governance 17

3. Informationsrisikomanagement 17

4. Informationssicherheitsmanagement 18

5. Benutzerberechtigungsmanagement 18

6. IT-Projekte, Anwendungsentwicklung (inklusive durch Endbenutzer in den Fachbereichen) 19

7. IT-Betrieb (inklusive Datensicherung) 20

8. Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen 21

V. EBA-Durchführungsstandards und EZB-Vorgaben für die Anzeigenverfahren bzw. das Meldewesen 21

VI. Erfahrungen aus der Aufsichtspraxis 24
1. Zunehmende qualitative/quantitative Meldeanforderungen 24
2. Häufige Defizite bei der Verwendung interner und externer Daten 24
3. Häufige Defizite bei Kernanforderungen an die IT und die verwendete EDV 25
4. Feststellungen im Rahmen von MaRisk-Prüfungen der Aufsicht zu IT & Datenqualität 25
a) Feststellungen zu Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit 25
b) Feststellung zur Schutzbedarfsanalyse 26
c) Feststellung zur Vertraulichkeit von Daten 26
VII. Datenqualität zunehmend im Fokus der Aufsicht 27
VIII. Literatur- bzw. Quellenverzeichnis 28

B. Data Governance und Datenmanagementstrategien 29

I. Data Governance *(Selke)* 31
II. Datenmanagement-Strategie *(Krug)* 35
1. Verstehen des Geschäftsmodells 36
2. Analyse der unterschiedlich strukturierten Datenbestände 37
3. Überprüfung und Anpassung der IT-Strategie 38
4. Harmonisierung 39
5. Bestimmung der von den Geschäftsfunktionen benötigten Daten 40

C. Datenmanagement 41

I. Überblick über das Datenmanagement *(Selke)* 43
1. Individuelle Voraussetzungen und Rahmenbedingungen im Institut 47
2. Zentrale Fragestellungen 48
3. Klares Zielbild 50

II. Zusammenhang von Datenmanagement und Prozessen *(Selke)* 51
1. Datenbeschreibung 53
2. Schlussbemerkung zum allgemeinen Datenmanagement 62
III. Datenmanagement im Kreditrisikomanagement *(Jafarpour)* 64
1. Verwendung geeigneter Daten 64
2. Datenhistorien 68
3. Daten aus externen Quellen 72
4. Einbeziehung der Daten-Risiken in die Risikosteuerungs- und -Controllingsprozesse 73
5. Fazit und Ausblick 81
IV. Datenmanagement im Meldewesen *(Freßmann)* 83
1. Sicherstellung eines aussagekräftigen Meldewesens: qualitativ hochwertige Melde-Daten in neuen Formaten 83
2. Verzahnung von Meldewesen und Funktionsbereichen mit (risiko-)relevanten Daten 84
3. Erweiterte Anforderungen für die Meldung von unterjährigen Plan-, Ertrags- und Risikodaten 84
4. Beurteilung des Datenmanagements und der Kontrollmaßnahmen im IKS hinsichtlich gemeldeter (Risiko-)Daten 85
5. Umsetzung neuer meldepflichtiger Finanzinformationen und Solvabilitäts-/Kapitaladäquanzmeldungen 88
a) Liquiditätskennziffern 88
b) Verschuldungsgrad 89
c) Einlagensicherung 90
6. Sicherstellung der Datenverfügbarkeit und Konsistenz der nach AnaCredit zu meldenden Daten 91
a) Effizientere Prozesse 92
b) Höherer Integrationsgrad 92
c) Besseres Datenqualitätsmanagement 93
7. Praxisbericht: (Daten)Fallstricke in der Meldewesenpraxis 93
8. Praxistipps zur (sinnvollen) Datenbereinigung von Meldewesen-Daten 95

D. Datenqualitätsmanagement **97**

I. Datenqualität *(Selke)* 99

II. Prüfung Datenqualität *(Krug)* 104

1. Prüfung der Qualität von (Risiko-)Daten zur Sicherstellung einer wirksamen Risikosteuerung 104
   a) Prüfungsplanung 105
   b) Prüfungsdurchführung 106
2. Projektbegleitung durch die Interne Revision 111

III. Datenqualitätsmanagement für operative Daten *(Frommlet/Hein)* 116

1. Einleitung und Überblick 116
2. Ursachen für schlechte operative Daten 118
   a) Probleme bei der Dateneingabe 119
   b) Zeitliche Einflüsse 120
   c) Systemänderungen 121
   d) Unzureichende Datenpflege 122
3. Datenqualitätsmanagement für operative Daten 123
   a) Definitionsprozess 124
   b) Bereinigungsprozess 126
4. Datenqualitätsmanagementsystem – Anforderungen an die Technik 128
5. Kurzfristige Maßnahmen zur Verbesserung der Datenqualität 131
6. Zusammenfassung und Fazit 132

E. Erfahrungsberichte und Praxisbeispiele **135**

I. Aufbau eines Data Governance Offices und Implementierung einer unabhängigen Validierungseinheit *(Hackbarth/Holz)* 137

1. Umfeld/Ausgangslage 137
2. Gesetzliche und aufsichtsrechtliche Anforderungen 139
3. Definition Data Governance 139
4. Organisation der Data Governance 140

a) Data Governance Strategie 140
b) Ziele 141
c) Organisatorische Zuordnung 141
d) Rollen mit Verantwortlichkeiten und Aufgaben 143

5. Etablierung 150

6. Wesentliche erste Schritte 152

II. Integrierter Datenhaushalt in einer internationalen Spezialbank und wesentliche Aspekte und Prinzipien von BCBS 239 *(Selke)* 153

1. Wesentliche Aspekte und Prinzipien von BCBS 239 153

2. Praxisbeispiel: Integrierter Datenhaushalt in einer internationalen Spezialbank 160

III. Herausforderungen bei Veränderung der IT-Prozesse und IT-Systemlandschaft *(Foos/Heinemann)* 165

1. Zusammenfassung der Anforderungen 165
a) Wesentliche Anforderungen aus der BCBS 239 166
b) Korrelation mit dem Datenschutz 166

2. Ableiten wesentlicher IT-Handlungsfelder 187
a) Konzernsicht 188
b) Taxonomie 189
c) Datenqualitätsmanagement 192
d) Datenaktualität 193
e) Adaptability 194

3. Lösungsansätze zur Umsetzung der Anforderungen 196
a) Datenbereitstellung und -haushalte 199
b) Business Intelligence 203
c) Entwickeln und Aufrechterhalten der Data Governance 206

4. Fazit 210

IV. Sicherheit beim Cloud Computing *(Kaminski)* 211

1. Cloud Computing 211

2. Risiken 212
a) Rechtliche Risiken und Datenschutz 212
b) Gemeinsame Nutzung von Cloud Ressourcen 213
c) Insider 213

d) Cyber Attacken 213
e) Standardisierung 213
f) Datensicherung 214
g) Verfügbarkeit und Leistung 214
3. Maßnahmen 214
a) Speicherung 214
b) Datenübertragung 215
c) Zugang 215
d) Backup 215
e) Archivierung 215
f) Datenlöschung 216
g) Cyberraum 216
4. Festlegen von Maßnahmen 216
5. Zusammenfassung 217
6. Weitere Literatur 217

Abkürzungsverzeichnis

ACL	Access Control List
ADV	Allgemeine Datenverarbeitung
ALMM	Additional Liquidity Monitoring Metrics
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
BGBI	Bundesgesetzblatt
BI	Business Intelligence
BIZ	Bank für Internationale Zusammenarbeit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Besonderer Teil
BTO	Besonderer Teil (Organisation)
CDO	Chief Data Officer
CIO	Chief Information Officer
COREP	Common Solvency Ratio Reporting
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
delVO	delegierte Verordnung
DF	Datenfeld
DGO	Data Governance Office
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
EL	Expected Loss
EZB	Europäische Zentralbank
FinaRisikoV	Finanz- und Risikotragfähigkeitsinformationenverordnung
FinaV	Finanzinformationsverordnung
FINREP	Financial Reporting
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
ID	Identifikator
IDV	Individuelle Datenverarbeitung
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
KWG	Kreditwesengesetz

LCR	Liquidity Coverage Ratio
LDAP	Lightweight Directory Access Protocol
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
NP	Natürliche Person
NSFR	Net Stable Funding Ratio
OpVAR	Operational Value at Risk
PbD	Privacy by Default
PD	Probability of Default
PKI	Public Key Infrastructure
PrüfbV	Prüfungsberichtsverordnung
RACF	Resource Access Control Facility
RPO	Recovery Point Objective
RTF	Risikotragfähigkeit
RTO	Recovery Time Objective
SLA	Service Level Agreement
SQL	Structured Query Language
SREP	Supervisory Review an Evaluation Process
SSM	Single Supervisory Mechanism
TXT	Text
Tz	Textziffer
ZVAdr	Zentrale Vorverarbeitung Adressenrisiko

Vorwort

Daten und deren Nutzung liegen nicht zuletzt aufgrund des Schlagworts Digitalisierung mehr und mehr 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 zunehmend wichtiger – 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 bekannt geworden sind, und die seit 2017 geltenden BAIT. Das vorliegende Buch widmet sich diesen Risikodaten im Hinblick auf Qualität, Verarbeitung und Prüfung.

Es 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
- gängige Prüfungspraxis
- Data Governance
- Datenmanagement
- Datenqualitätsmanagement

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 die 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 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

Juli 2019

A.

Aufsichtsrechtliche Anforderungen an Bank-Daten

A. Aufsichtsrechtliche Anforderungen an Bank-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 Sparkassen und Banken eingeführt. Weitere Vorgaben setzen die 2017 eingeführten »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)

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 Sparkassen und Banken 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 1: 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.

6 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.

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 durch aufsichtliche Maßnahmen zügig zu beseitigen. Die Aufsichtsbehörden sollten zudem grenzüberschreitend kooperieren. 16

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

III. Neue bzw. angepasste MaRisk-Vorgaben durch die fünfte 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

18 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 für systemrelevante Institute auf Gruppenebene als auch auf der Ebenen 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).

19 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 muss 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

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

vorliegen müssen, ist zu definieren. In Stressphasen müssen z. B. folgende Risikodaten vorliegen:

- 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). 23

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). 24

2. Angepasste MaRisk-Vorgaben zu Datenqualität und IDV mit Gültigkeit für alle Institute

Der neue BT 3 gilt für alle Institute und Institutsgruppen; unter Berücksichtigung des allgemeinen Proportionalitätsgrundsatzes. Innerhalb dieses neu gestalteten MaRisk-Abschnitts »Anforderungen an die Risikoberichterstattung« werden die Anforderungen an die Erstellung der Berichte gebündelt dargestellt und um relevante Anforderungen aus der Vorgabe BCBS 239 erweitert. 25

Auf vollständigen, genauen und aktuellen Daten müssen die Berichte beruhen. Die Daten müssen flexibel für die Erfordernisse des Risikomanagements aufbereitet und angepasst werden. 26

Für die Anforderungen an die Berichterstattung der Internen Revision gibt es spezielle Vorgaben. Die für die Interne Revision relevanten Berichtspflichten sind weiterhin im BT 2.4 geregelt. 27

Der AT 7.2 »Technisch-organisatorische Ausstattung« wurde mit der fünften MaRisk-Novelle erweitert. Zu den bisherigen und weiterhin gültigen Tzn 1, 2 und 3 kommen die geänderte Tz 4 und Tz 5 neu hinzu. 28

Laut Tz 5 sind die Anforderungen, die im AT 7.2 genannt werden, nunmehr auch beim Einsatz von durch die Fachbereiche selbst entwickelten Anwendungen (IDV) entsprechend zu beachten. Die Festlegung von Maßnahmen 29

zur Sicherstellung der Datensicherheit hat sich am Schutzbedarf der jeweiligen Daten zu orientieren.

30 Tz 4 fordert, dass für IT-Risiken angemessene Überwachungs- und Steuerungsprozesse einzurichten sind. Diese Prozesse haben insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und –minderung zu umfassen. Beim Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten.

3. Vor und mit der fünften MaRisk-Novelle gültige Vorgaben zum Datenmanagement für alle Institute

31 Unverändert haben sich nach Tz 1 des AT 7.2 Umfang und Qualität der technisch-organisatorischen Ausstattung an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten und der Risikosituation zu orientieren.

32 Tz 2, AT 7.2 schreibt vor, dass die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse die Integrität, die Verfügbarkeit, die Authentizität und die Vertraulichkeit der Daten sicherstellen müssen. Hier werden die vier Schutzziele angesprochen.

33 Unter Integrität ist die Sicherstellung der Unversehrtheit der Daten zu verstehen. Verfügbarkeit der Daten liegt vor, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. Authentizität heißt, dass ein Kommunikationspartner wirklich derjenige ist, der er vorgibt zu sein. Vertraulichkeit bedeutet Schutz vor unbefugter Preisgabe der Daten.

34 Gemäß Tz 2 ist weiterhin bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Es sind insbesondere Prozesse für eine angemessene Ist-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.

35 Tz 3 gibt vor, dass IT-Systeme vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen sind. Hierfür ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung

in die Produktionsprozesse zu etablieren. Produktions- und Testumgebung sind grundsätzlich voneinander zu trennen.

IV. Bankaufsichtliche Anforderungen an die IT (BAIT)

Am 03.11.2017 hat die BaFin die BAIT (=Bankaufsichtliche Anforderungen an die IT) als Rundschreiben 10/2017 (BA) veröffentlicht.[4] 36

Wie ist das Zusammenspiel MaRisk zu BAIT zu sehen? Natürlich bleiben die in den MaRisk enthaltenen Anforderungen unberührt. Sie werden – wie die BaFin betont – durch die BAIT IT-spezifisch konkretisiert. Somit verweisen die Leitsätze der BAIT auf die jeweiligen Textziffern der MaRisk. 37

Die Erwartungshaltung der Aufsicht an die Institute hinsichtlich der sicheren Ausgestaltung der IT-Systeme sowie der zugehörigen IT-Prozesse und die diesbezüglichen Anforderungen an die IT-Governance wird durch die BAIT transparent gemacht. Die BAIT enthalten grundsätzlich keine neuen Anforderungen an die Institute, sondern sind als Klarstellungen schon vorhandener Anforderungen zu sehen. 38

Die BAIT sind in acht Themenbereiche bzw. Kapitel unterteilt: 39

1. IT-Strategie
2. IT-Governance
3. Informationsrisikomanagement
4. Informationssicherheitsmanagement
5. Benutzerberechtigungsmanagement
6. IT-Projekte, Anwendungsentwicklung (inklusive durch Endbenutzer in den Fachbereichen)
7. IT-Betrieb (inklusive Datensicherung)
8. Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen

In den folgenden Kapiteln wird eine Zusammenfassung der Anforderungen der oben genannten Themenbereiche gegeben. 40

Ein wesentliches Ziel der BAIT ist die Stärkung des IT-Risikobewusstseins in den Banken und Sparkassen und insbesondere in den Führungsebenen. Die Notwendigkeit der Herstellung von Risikotransparenz und die Auseinander- 41

4 Die BAIT sind sowohl auf der homepage der BaFin als auch der Bundesbank einsehbar (www.bafin.de, www.bundesbank.de). Das Rundschreiben 10/2017 (BA) wird durch ein erläuterndes Anschreiben der BaFin ergänzt.

setzung mit dem IT-Risiko auf allen Ebenen eines Instituts sind zentraler Bestandteil der IT-Anforderungen und zieht sich somit durch alle acht Themenbereiche.[5] Die folgende Abbildung stellt dieses Erfordernis für die operative Umsetzung, den Steuerungsbereich und die Ebene der Geschäftsleitung bzw. der Governance dar.

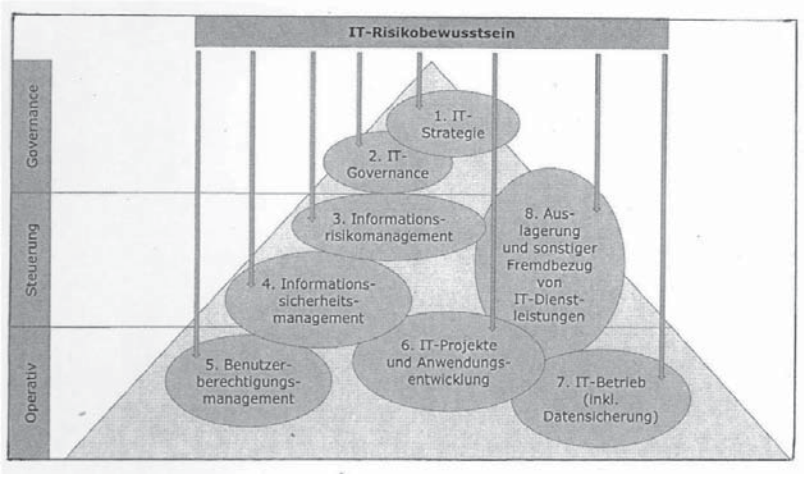

Abbildung 2: Schärfung des IT-Risikobewusstseins durch die BAIT (Quelle: BaFin Journal Januar 2018, S. 19.)

1. IT-Strategie

42 In diesem Themenbereich werden Mindestinhalte einer IT-Strategie genannt. Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente, nachhaltige IT-Strategie festzulegen, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden.

43 Als Mindestinhalte der IT-Strategie gelten:

- Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation sowie der Auslagerungen von IT-Dienstleistungen
- Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT
- Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation

[5] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): BaFin Journal: IT-Sicherheit: Aufsicht konkretisiert Anforderungen an die Kreditwirtschaft, Januar 2018, S. 18 f.

- Strategische Entwicklung der IT-Architektur
- Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange
- Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten)

2. IT-Governance

Für die Umsetzung der Regelungen zur IT-Governance ist die Geschäftsleitung verantwortlich. Das Institut hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb sowie die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Personal auszustatten. Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden. Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative und qualitative Kriterien festzulegen. Deren Einhaltung ist zu überwachen. 44

3. Informationsrisikomanagement

Die Informationsverarbeitung und -weitergabe in Geschäfts- und Serviceprozessen wird durch datenverarbeitende IT-Systeme und zugehörige IT-Prozesse unterstützt. 45

Im Themenbereich Informationsrisikomanagement wird ein stets aktueller Überblick über die Bestandteile des festgelegten Informationsverbundes sowie deren Abhängigkeiten und Schnittstellen gefordert. Ferner werden Vorgaben an die Methodik zur Ermittlung des Schutzbedarfs beschrieben. 46

Ein Sollmaßnahmenkatalog ist zu erstellen. Im Rahmen der Erstellung dieses Katalogs sind die Anforderungen des Instituts zur Umsetzung der Schutzziele in den Schutzbedarfskategorien festzulegen und in geeigneter Form zu dokumentieren. 47

Die Ergebnisse der Risikoanalyse sind in den Prozess des Managements der operationellen Risiken zu überführen. Die Geschäftsleitung muss regelmäßig, mindestens vierteljährlich, darüber und über Veränderungen an der Risikosituation informiert werden. 48

4. Informationssicherheitsmanagement

49 Zunächst hat die Geschäftsleitung eine Informationssicherheitsleitlinie zu beschließen und im Institut zu kommunizieren.

50 Auf Basis der von der Geschäftsleitung beschlossenen Informationssicherheitsleitlinie sind dann konkretisierende und den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse hinsichtlich der Dimensionen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.

51 Jedes Institut hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien des Instituts niedergelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung überprüft und überwacht werden.

52 Um mögliche Interessenkonflikte zu vermeiden, ist die Funktion des Informationssicherheitsbeauftragten organisatorisch und prozessual unabhängig auszugestalten. Zudem ist die Funktion grundsätzlich im eigenen Haus vorzuhalten. Regional tätige (insbesondere verbundangehörige) Institute sowie kleine (insbesondere gruppenangehörige) Institute ohne wesentliche eigenbetriebene IT mit einem gleichgerichteten Geschäftsmodell und gemeinsamen IT-Dienstleistern können einen gemeinsamen Informationssicherheitsbeauftragten bestellen. Allerdings ist dann in jedem Institut eine zuständige Ansprechperson für den Informationssicherheitsbeauftragten zu benennen.

53 Der Informationssicherheitsbeauftragte hat der Geschäftsleitung regelmäßig, mindestens vierteljährlich, über den Status der Informationssicherheit sowie anlassbezogen zu berichten. Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informationssicherheit zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen.

5. Benutzerberechtigungsmanagement

54 Die Nutzungsbedingungen und der Umfang von IT-Berechtigungen für die IT-Systeme sind konsistent zum ermittelten Schutzbedarf in einem Berechtigungskonzept festzulegen. Die Berechtigungskonzepte haben die Vergabe von Berechtigungen nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip