Data Governance als Werkzeug zur Erfüllung aufsichtsrechtlicher Vorgaben im Bankbereich

Peter Gluchowski, Christoph Kreiterling

Data Governance als Werkzeug zur Erfüllung aufsichtsrechtlicher Vorgaben im Bankbereich

Peter Gluchowski / Christoph Kreiterling

I. Einführung und Motivation

Die globale Finanzkrise 2007/2008 hat die Finanzwelt durch massive ökonomische Auswirkungen erschüttert. Zahlreiche Finanzinstitute waren zum damaligen Zeitpunkt auf die globalen Verwerfungen nicht ausreichend vorbereitet, weil es ihnen nicht gelang, relevante Risikodaten in angemessener Zeit zu aggregieren und zu analysieren. Der Erfolg von Unternehmen und vor allem denen in der Finanzindustrie hängt entscheidend von der Beherrschung der Risiken ab, die in vielfältiger Form und unterschiedlicher Stärke unerwartet auftreten und die Geschäftsprozesse stören und negativ beeinflussen können. Nicht zuletzt vor diesem Hintergrund sind die vielfältigen regulatorischen Vorgaben zu verstehen, denen sich Finanzinstitute heute ausgesetzt sehen und die sich durch ihre internationale, europäische und nationale Tragweite auszeichnen.

Die Steuerung der Risiken erfordert die Einbeziehung einer großen Vielfalt an umfangreichem Datenvolumen und erfolgt daher heute fast durchweg durch die Nutzung der zugehörigen IT-Systeme. Für die Gestaltung und den Einsatz der Systeme sind verbindliche Vorgaben im Sinne einer IT-Governance zu erstellen, die einen Ordnungsrahmen für das anforderungsgerechte und regelkonforme

Management der IT vorgeben. [1] Wichtige Gestaltungsbereiche der IT-Governance finden sich in der Lieferfähigkeit, der Produktivität und dem Risikomanagement sowie vor allem in den Bereichen IT-Kosten und IT-Sicherheit. Inhaltlich richtet sich die IT-Governance an den Vorgaben der Corporate Governance aus und versucht, eine möglichst wirtschaftliche Gestaltung von IT-Systemen und der damit verbundenen organisatorischen Strukturen und Prozessen zu erreichen.[2]

Zunehmend setzt sich heute in den Unternehmen das Bewusstsein durch, dass die verfügbaren Daten ein wichtiges Wirtschaftsgut darstellen und zur Erlangung von Wettbewerbsvorteilen beitragen. [3] Die steigende Bedeutung der Daten für den Unternehmenserfolg führt zu einem sorgfältigen und abgestimmten Umgang mit diesem wertvollen Gut und letztlich zur Etablierung einer eigenständigen Data Governance in den Unternehmen. In Abgrenzung zur IT-Governance, in deren Verantwortungsbereich sowohl die IT-Systemlandschaft als auch die Programme fallen, widmet sich die DG den (digitalen) Daten und Informationen. [4]

Der vorliegende Beitrag widmet sich der Data Governance als Werkzeug zur Erfüllung aufsichtsrechtlicher Vorgaben im Bankenbereich. Dazu werden im folgenden zweiten Abschnitt zunächst die relevanten aufsichtsrechtlichen Bestimmungen dargestellt. Der nachfolgende dritte Abschnitt widmet sich der Data Governance vor diesem Hintergrund und zeigt die zentralen Nutzenpotenziale auf, bevor eine kurze Zusammenfassung im vierten Abschnitt erfolgt.

II. Aufsichtsrechtliche Vorgaben im Bankenbereich

Die Adressat/innen aufsichtsrechtlicher Vorgaben im Bankenbereich sind die Inhaber/innen einer ‚Banklizenz', also einer Erlaubnis nach § 32 Kreditwesengesetz (KWG). Diese wird benötigt, wenn die abschließend in § 1 Absatz 1 KWG aufgeführten Bankgeschäfte in Deutschland geschäftsmäßig betrieben werden, also etwa das Einlagen-, das Kredit- oder das Depotgeschäft. Inhaber/innen der Erlaubnis müssen dann die aufsichtsrechtlichen Vorgaben erfüllen, wozu beispielsweise ein ausreichendes Anfangskapital in Höhe von mindestens fünf Millionen Euro gehört.[5]

---

[1] *Weill, P., & Ross, J. W.* (2004) IT Governance – How Top Performers Manage IT Decision Rights for Superior Results. In Harvard Business Review Press, Brighton.

[2] *Asprion, P. M., & Knolmayer, G.* (2016) IT-Governance. In Enzyklopädie der Wirtschaftsinformatik, http://www.enzyklopaedie-der-wirtschaftsinformatik.de/ lexikon/ daten-wissen/ Grundlagen-derInformationsversorgung/IT-Governance, Abruf am 03.10.2020.

[3] *Schulze, K.-D., Dittmar, C., & Ballerstedt, D.* (2016) Auf dem Weg zur Data Driven Company – Wie die fortschreitende Digitalisierung die klassische BI verändert, Vortrag auf der TDWI-Jahreskonferenz, München, 21.06.2016.

[4] *Khatri, V., & Brown, C. V.* (2010). Designing Data Governance. In Communications of the ACM, 53 (1), 148-152.

[5] *BaFin* (2016). Zulassung von Banken und Finanzdienstleistern sowie von Zahlungs- und E-Geldinstituten. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/7846482

Die aufsichtsrechtlichen Anforderungen an Banken, Sparkassen und andere Kreditinstitute (nachfolgend zusammenfassend als Banken bezeichnet) sind vielfältig, umfangreich, teils komplex und unterliegen laufenden aufsichtsrechtlichen Änderungen und Ergänzungen.[6] Wegen des begrenzten Umfangs dieses Artikels kann daher nachfolgend nur eine exemplarische Auswahl an aufsichtsrechtlichen Anforderungen vorgestellt werden, die weder den Anspruch hat, vollständig noch repräsentativ zu sein. Gleichwohl wird durch die Auswahl deutlich, welche Anknüpfungspunkte für Data Governance bestehen, um einen Beitrag zu leisten, damit die aufsichtsrechtlichen Anforderungen erfüllt werden können.

Bei der Auswahl werden international relevante, europäische und nationale Regularien berücksichtigt, die für einen Großteil der Banken in Deutschland bedeutsam sind. Dazu werden als internationale Richtlinien eingangs die Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung des Basler Ausschusses (BCBS 239) adressiert, da sie eine weitreichende Bedeutung für Banken und aufsichtsrechtliche Anforderungen haben.[7] Daran anknüpfend folgt die europäische Perspektive, wobei sich hier zunächst der zweiten europäischen Finanzmarktrichtlinie (Markets in Financial Instruments Directive, MiFID II) gewidmet wird. Die MiFID II war eine zentrale Komponente im Aktionsplan der Europäischen Kommission für Finanzdienstleistungen und hat Auswirkungen auf alle Banken, die Wertpapierdienstleistungen anbieten.[8] Danach folgt die Darstellung der zweiten Zahlungsdiensterichtlinie (Payment Service Directive 2, PSD2) und der ihr inhärenten Meldepflicht bei Zahlungssicherheitsvorfällen, da nahezu alle Banken in Deutschland hiervon betroffen sind.[9] Die europäische Perspektive wird abschließend im Rahmen der Kreditdatenstatistik (AnaCredit) behandelt, da alle europäischen Banken seit September 2018 detaillierte Daten zu allen Krediten ab 25 000 Euro, die an nichtnatürliche Personen vergeben werden, an die jeweilige Zentralbank melden müssen.[10] Anschließend folgen die nationalen regulatorischen Anforderungen, wobei das KWG dafür den Ausgangspunkt bietet. Hierbei wird insbesondere die Forderung nach einer ordnungsgemäßen Geschäftsorganisation adressiert. [11] Letztere wird in den Mindestanforderungen an das

[6] *Sironi, A.* (2018). The evolution of banking regulation since the financial crisis: A critical assessment. Baffi Carefin Centre Research Paper, (2018-103).

[7] *Cree, M.* (2015). BCBS 239–Principles for effective risk data aggregation and reporting.

[8] *Gillet, R., Ligot, S., & Firouzi, H. O.* (2017). The challenges and implications of the Markets in Financial Instruments Directive (MiFID) and of its revision (MiFID II, MiFIR) on the efficiency of financial markets. In Financial Regulation in the EU (pp. 151-198). Palgrave Macmillan, Cham.

[9] *Göbel, C. A.* (2017). Chancen und Herausforderungen durch die PSD2 und Instant Payment. In Mobile Payment (pp. 167-178). Springer Gabler, Wiesbaden.

[10] *Brananova, O. C., & Watfe, G.* (2017). Use of AnaCredit granular data for macroprudential analysis. IFC Bulletins Chapters, 46.

[11] *Lütgerath, N.* (2016). Die Vorgaben zur ordnungsgemäßen Geschäftsorganisation im Bankaufsichtsrecht.

Risikomanagement (MaRisk) und in den Bankaufsichtlichen Anforderungen an die IT (BAIT) konkretisiert.[12]

1. BCBS 239

Die Finanzkrise, die im Jahr 2007 begann, hat die Schaffung eines neuen gesetzlichen und regulatorischen Rahmens beschleunigt. [13] Diese Krise, die zum Teil durch die übermäßige Risikobereitschaft von Banken ausgelöst wurde, hatte weltweite Auswirkungen auf die aufsichtlichen Anforderungen.[14] Es folgte mit der Veröffentlichung der „Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung" (BCBS 239) des Baseler Ausschusses für Bankenaufsicht (BCBS) ein Standard, der eine Wiederholung dieser Ereignisse verhindern soll.[15] Übergeordnetes Ziel der BCBS 239 ist es, die Fähigkeiten der Banken zur Aggregation von Risikodaten und die interne Risikoberichterstattungspraxis zu stärken, was wiederum das Risikomanagement und die Entscheidungsfindungsprozesse verbessern soll.[16]

Auch wenn die BCBS 239 nicht unmittelbar und für alle Banken gilt, so haben sie doch weitreichende Auswirkungen auf die weltweite Entwicklung von aufsichtlichen Anforderungen an Banken. Nahezu alle Aspekte der BCBS 239 finden sich in ähnlicher oder abgewandelter Form als aufsichtliche Anforderungen an Banken wieder. Die BCBS 239 waren damit eines der weitreichendsten aufsichtlichen Mandate nach der 2007 beginnenden Finanzkrise.[17]

Die BCBS 239 bestehen im Kern aus 14 Grundsätzen, von denen die ersten elf an Banken gerichtet sind. Nachfolgend werden deren wesentliche Inhalte vorgestellt.[18]

So sollen als eines der Hauptziele die Fähigkeit einer Bank zur Aggregation von Risikodaten und die Praxis der Risikoberichterstattung strengen Governance-Regeln unterliegen. Hieran können bereits Data-Governance-Konzepte anknüpfen. Daneben sollen Banken eine Datenarchitektur und eine IT-

[12] *Maksimovic, T., & Biernat, H.* (2019). MaRisk und BAIT im Detail. In Bankaufsichtliche Anforderungen an die IT (BAIT) (pp. 17-54). Springer Gabler, Wiesbaden.

[13] *Claessens, S., & Van Horen, N.* (2015). The impact of the global financial crisis on banking globalization. IMF Economic Review, 63(4), 868-918.

[14] *Claessens, S., Laeven, M. L., Igan, D., & Dell'Ariccia, M. G.* (2010). Lessons and policy implications from the global financial crisis (No. 10-44). International Monetary Fund.

[15] *Grody, A. D.* (2018). Rebuilding financial industry infrastructure. Journal of Risk Management in Financial Institutions, 11(1), 34-46.

[16] *Orgeldinger, J.* (2018). The Implementation of Basel Committee BCBS 239: Short analysis of the new rules for Data Management. Journal of Central Banking Theory and Practice, 7(3), 57-72.

[17] *Arboleda, P., Bagheri, S., & Khakzad, F.* (2016). Model risk. In the context of the regulatory climate change. Working Paper.

[18] *BCBS* (2013). Principles for effective risk data aggregation and risk reporting. Aufgerufen 2020-09-14 unter https://www.bis.org/publ/bcbs239.pdf

Infrastruktur entwerfen, aufbauen und unterhalten, die die Fähigkeit zur Aggregation von Risikodaten und das Verfahren zur Risikoberichterstattung nicht nur in normalen, sondern auch in Stress- oder Krisenzeiten unterstützt. Zusätzlich soll eine Bank in der Lage sein, genaue und verlässliche Risikodaten zu generieren, um die Genauigkeitsanforderungen für normale und Stress- bzw. Krisenberichte zu erfüllen. Die Daten sollen auf einer weitgehend automatisierten Basis aggregiert werden, um die Wahrscheinlichkeit von Fehlern zu minimieren.

Ferner sollen Banken in der Lage sein, alle wesentlichen Risikodaten zu erfassen und zu aggregieren. Die Daten sollen nach für das jeweilige Risiko relevanten Gruppierungen geordnet werden können, um die Identifizierung und Meldung von Risikopositionen, Konzentrationen und neu auftretenden Risiken zu ermöglichen. Außerdem sollen Banken in der Lage sein, aggregierte und aktuelle Risikodaten zeitnah zu generieren und gleichzeitig die Grundsätze bezüglich Genauigkeit, Integrität, Vollständigkeit und Anpassungsfähigkeit zu erfüllen, wobei dies insbesondere von der Art und der potentiellen Volatilität des gemessenen Risikos und seiner Bedeutung für das Gesamtrisikoprofil der Bank abhängt. Allerdings können bankspezifische Anforderungen an die Frequenz der Berichterstattung individuell berücksichtigt werden.

Ebenfalls sollen Banken in der Lage sein, aggregierte Risikodaten zu generieren, um ein breites Spektrum an Ad-hoc-Risikomanagement-Berichtsanforderungen auf Abruf zu erfüllen, einschließlich Anforderungen in Stress- bzw. Krisensituationen, Anforderungen aufgrund sich ändernder interner Bedürfnisse und Anforderungen zur Erfüllung aufsichtsrechtlicher Anfragen. Überdies sollen mithilfe der Risikomanagementberichte aggregierte Risikodaten genau und präzise vermittelt und das Risiko exakt wiedergegeben werden. Dazu sollen die Risikomanagementberichte der Banken alle wesentlichen Risikobereiche abdecken. Die Tiefe und der Umfang dieser Berichte sollen der Größe und Komplexität der Geschäftstätigkeit und dem Risikoprofil der Bank sowie den Anforderungen der Empfänger/innen entsprechen.

Gleichzeitig sollen die Risikomanagementberichte der Banken Informationen in klarer und prägnanter Weise vermitteln. Berichte sollten leicht verständlich und dennoch umfassend genug sein, um eine informierte Entscheidungsfindung zu erleichtern. Sie sollen ein angemessenes Gleichgewicht zwischen Risikodaten, Analyse und Interpretation sowie qualitativen Erläuterungen enthalten. Berichte sollen zudem aussagekräftige Informationen umfassen, die auf die Bedürfnisse der Empfänger/innen zugeschnitten sind. Daneben soll die Geschäftsleitung festlegen, wie häufig die Risikomanagementberichte erstellt werden und wie sie verteilt werden.

Die Anforderungen an die Häufigkeit sollen die Bedürfnisse der Empfänger/innen, die Art des gemeldeten Risikos und die Geschwindigkeit, mit der sich das Risiko ändern kann, sowie die Bedeutung der Berichte als Beitrag zu einem soliden Risikomanagement und einer effektiven bzw. effizienten

Entscheidungsfindung in der gesamten Bank widerspiegeln. Die Häufigkeit der Berichte sollte in Stress- bzw. Krisenzeiten erhöht werden. Letztlich sollen die Risikomanagementberichte auch unter Wahrung der Vertraulichkeit an die relevanten Empfänger/innen übermittelt werden.

In Anbetracht der Anforderungen an Banken, die in BCBS 239 festgehalten werden und sich inhaltlich vergleichbar in einer Vielzahl anderer aufsichtlichen Anforderungen an Banken wiederfinden, lassen sich viele Anknüpfungspunkte für Data Governance als Hilfsmittel zur Erfüllung der aufsichtlichen Vorgaben erkennen.

2. MiFID II

Die MiFID (Markets in Financial Instruments Directive) II, die zweite europäische Finanzmarktrichtlinie, ist seit Januar 2018 anzuwenden. Sie wird ergänzt durch die Finanzmarktverordnung (Markets in Financial Instruments Regulation, MiFIR).[19] Gegenstand ist der Handel mit Wertpapieren und Finanzinstrumenten. Neben der Harmonisierung des europäischen Wertpapierrechts ist eines der Hauptziele von MiFID II von MiFIR, Investor/innen mehr Transparenz und Schutz bei Wertpapieranlagen zu verschaffen. Daneben wurde das Produktinterventionsrecht der Aufsichtsbehörden neugestaltet. Die MiFID II hat Auswirkungen auf eine Vielzahl an Bankaktivitäten und den damit verbundenen Informationssystemen.[20]

Mit der MiFID II wird die Wertpapieraufsicht in den Ländern der Europäischen Union (EU) harmonisiert und dadurch der Anwendungsbereich der Vorschriften erweitert. Insbesondere werden in der Richtlinie mehr Meldepflichten und Tests vorgeschrieben, um die Transparenz zu erhöhen und die Verwendung von Dark Pools (private Finanzbörsen, die es Anlegern ermöglichen, ohne Offenlegung ihrer Identität zu handeln) sowie den außerbörslichen Handel (Over the counter, OTC) zu reduzieren. Nach den neuen Regeln ist das Handelsvolumen einer Aktie in einem Dark Pool begrenzt. Die Vorschriften zielen auch auf den Hochfrequenzhandel ab. Algorithmen, die für den automatisierten Handel verwendet werden, müssen registriert und getestet werden und über einen Not-Schutzschalter verfügen.[21]

Mit der MiFID II wird der Geltungsbereich der Anforderungen auf weitere Finanzinstrumente wie Aktien, Rohstoffe, Schuldtitel, Futures und Optionen, börsengehandelte Fonds sowie Währungen ausgeweitet. Wenn ein Produkt in einem Land der EU erhältlich ist, fällt es unter MiFID II – auch, wenn beispielsweise

[19] *European Securities and Markets Authority* (2017). MIFID II. Aufgerufen 2020-09-14 unter https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

[20] *Busch, D.* (2017). MiFID II and MiFIR: stricter rules for the EU financial markets. Law and Financial Markets Review, 11(2-3), 126-142.

[21] *Gillet, R., Ligot, S., & Firouzi, H. O.* (2017). The challenges and implications of the Markets in Financial Instruments Directive (MiFID) and of its revision (MiFID II, MiFIR) on the efficiency of financial markets. In Financial Regulation in the EU (pp. 151-198). Palgrave Macmillan, Cham.

die Händler/innen, die es kaufen möchten, außerhalb der EU ansässig sind. Dabei deckt die MiFID II nicht nur praktisch alle Aspekte der Finanzanlagen und des Finanzhandels ab, sondern auch alle mit Wertpapiertransaktionen betrauten Intermediäre innerhalb der EU wie etwa Banken, die die Bestimmungen der MiFID II einhalten müssen.[22]

Zusätzlich sind in der MiFID II Beschränkungen für Anreize vorgesehen, die an Wertpapierfirmen oder Finanzberater/innen von Dritten im Zusammenhang mit Dienstleistungen für Kunden gezahlt werden. Zusätzlich müssen Makler/innen wie Banken detaillierte Berichte über ihre Geschäfte anfertigen, die Daten wie Preis- und Volumeninformationen enthalten. Dazu müssen alle Mitteilungen, einschließlich Aufzeichnungen von Telefongesprächen, gespeichert werden. Letztlich wird dadurch der elektronische Handel gestärkt, da er sich mit einer geringeren Anzahl an Medienbrüchen aufzeichnen und nachverfolgen lässt.[23]

Die Umsetzung der Anforderungen aus der MiFID II ist für Banken mit Aufwänden verbunden insbesondere im Hinblick auf Meldepflichten, Auszeichnungspflichten und Anforderungen an die Informationssysteme. Auch hier kann durch Data-Governance-Konzepte ein Beitrag geleistet werden.

3. PSD2-Zahlungssicherheitsvorfälle

Die 2015 vom Europäischen Parlament verabschiedete zweite Zahlungsdiensterichtlinie PSD2 (Payment Services Directive2) wurde im Januar 2018 mit dem geänderten Zahlungsdiensteaufsichtsgesetz in deutsches Recht umgesetzt.[24] Mit dem Gesetz werden Zahlungsdienstleister adressiert, worunter auch alle Banken in Deutschland sowie weitere Unternehmen fallen. Ein Bestandteil dieses Gesetzes ist dabei die Pflicht der Zahlungsdienstleister/innen, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) unverzüglich über schwerwiegende Betriebs- und Sicherheitsvorfälle zu unterrichten. Diese PSD2Zahlungssicherheitsvorfälle sollen über das Meldeportal der BaFin an die Aufsicht übermittelt werden.[25]

[22] *Papaconstantinou, G. A.* (2016). Investment bankers in conflict: the regime of inducements in MiFID II and the member states' struggle for fairness. European review of contract law, 12(4), 356-390.

[23] *Pfisterer, P.* (2015). Die neuen Regelungen der MiFID II zum Anlegerschutz: Analyse und Vergleich zur bestehenden Rechtslage. Springer-Verlag.

[24] *BaFin* (2019). Zahlungsdienste und PSD2. Aufgerufen am 2020-09-14 unter https://www.bafin.de/dok/12672828

[25] *BaFin* (2017). PSD2-Zahlungssicherheitsvorfälle. Meldungen nach § 54 Absatz 1 Satz 1 ZAG. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10241070

Unter einem PSD2-Zahlungssicherheitsvorfall, also einem Betriebs- oder Sicherheitsvorfall, wird verstanden ein einzelnes Ereignis oder eine Reihe miteinander verbundener, von den Zahlungsdienstleister/innen nicht geplante Ereignisse, die sich nachteilig auf die Integrität,

Verfügbarkeit, Vertraulichkeit, Authentizität und/oder Kontinuität der zahlungsbezogenen Dienste auswirken oder wahrscheinlich auswirken werden.[26] Dazu existieren spezifische Kriterien für die Einstufung eines Betriebs- oder Sicherheitsvorfalls als schwerer Vorfall. Von den Anbieter/innen von Zahlungsdiensten wird erwartet, dass sie innerhalb von vier Stunden nach Feststellung des Vorfalls Berichte über einen schweren Vorfall vorlegen, unabhängig davon, ob der Vorfall während der Abwesenheitszeiten festgestellt wird.[27]

- **Erstbericht:** Die Zahlungsdienstleister/innen müssen einen Erstbericht innerhalb von vier Stunden nach Feststellung des Betriebs- oder Sicherheitsvorfalls übermitteln. In diesem Rahmen wird verlangt, grundlegende Informationen sowie eine allgemeine Beschreibung des Vorfalls zu liefern. Die Zahlungsdienstleister/innen sollen den Erstbericht nach bestem Wissen ausfüllen.[28]
- **Zwischenbericht:** Zahlungsdienstleister/innen sind verpflichtet, innerhalb von 72 Stunden nach dem Erstbericht sowie bei Kenntnisnahme wesentlicher Änderungen oder neuer Informationen, die für den Vorfall relevant sind, einen Zwischenbericht zu übermitteln. Dieser Bericht sollte detaillierte Informationen über die Art und die Auswirkungen des Vorfalls enthalten. Zahlungsdienstleister/innen sollten weiterhin Zwischenberichte senden, bis die ‚Business-as-usual-Aktivitäten' wieder aufgenommen werden.
- **Abschlussbericht:** Zahlungsdienstleister/innen müssen ihren Abschlussbericht innerhalb von zwei Wochen nach Abschluss des schweren Vorfalls einreichen. Der Abschlussbericht sollte detaillierte Angaben über die Vorfallursache, die ergriffenen Maßnahmen und alle anderen relevanten Informationen enthalten.

Auch bei der Meldung der PSD2-Zahlungssicherheitsvorfall-Berichte an die BaFin über deren Meldeportal zeigen sich Anknüpfungspunkte für Data Governance, um hier für Banken einen zweckmäßigen Beitrag leisten zu können.

---

[26] *European Banking Authority* (2019). EBA/GL/2019/04 - Guidelines on ICT and security risk management. Aufgerufen 2020-09-14 unter https://eba.europa.eu/regulation-and-policy/internal-governance/guidelineson-ict-and-security-risk-management

[27] *BaFin* (2017). Informationen zum Meldeverfahren für schwerwiegende Betriebs- und Sicherheitsvorfälle bei Zahlungsdienstleistern. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10020844

[28] *BaFin* (2018). Rundschreiben 08/2018 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10941432

4. Kreditdatenstatistik (AnaCredit)

Mit Beschluss vom Mai 2016 hat die Europäische Zentralbank (EZB) das Analytical Credit Dataset (AnaCredit) als Kreditmeldesystem der EZB etabliert.[29] Mit AnaCredit wird die harmonisierte Erhebung detaillierter Informationen über einzelne Bankkredite in der Eurozone ermöglicht. Ziel des Systems sind die Überwachung der Finanzstabilität, die Durchführung geldpolitischer Analysen und die Steuerung des Risikomanagements.[30]

Nur Kredite ab 25 000 Euro, die nicht an natürliche Personen gewährt werden, müssen gemeldet werden. Dazu müssen alle Banken in Deutschland seit September 2018 die Daten regelmäßig an die Deutsche Bundesbank melden. Die Meldungen müssen meist monatlich oder vereinzelt auch quartalsweise über das Meldeportal der Deutschen Bundesbank im XMLDatenformat erfolgen. Auch Banken außerhalb der Euro-Zone mit einer Niederlassung in Deutschland müssen in diesem Kontext an die Deutsche Bundesbank melden. Letztere übermittelt ihrerseits die Daten an die EZB, die dadurch einen aggregierten Blick auf die Gesamtkreditvergabe im Euroraum hat.[31]

Durch AnaCredit kann die EZB Informationen über den Zugang von Unternehmen zu Bankkrediten identifizieren. Die Daten können auch verwendet werden, um die Unternehmensverschuldung und deren Tragfähigkeit zu beurteilen.

Auch im Rahmen des AnaCredit-Systems und den Meldungen bieten sich mehrere Anknüpfungspunkte für Data Governence, um einen sachdienlichen Beitrag zu leisten.

5. KWG, MaRisk und BAIT

Wie eingangs bereits skizziert, wird für das gewerbsmäßige Erbringen von Bankdienstleistungen gemäß § 1 Absatz 1 des KWG eine Lizenz nach § 32 KWG benötigt. Dazu müssen mehrere Anforderungen schon beim Erlaubnisantrag erfüllt sein. Dazu gehören etwa die zuvor erwähnten 5 Millionen Euro

[29] *EZB* (2016). Decision (EU) 2016/868 of the European Central Bank of 18 May 2016 amending Decision ECB/2014/6 on the organisation of preparatory measures for the collection of granular credit data by the European System of Central Banks (ECB/2016/14). Aufgerufen 2020-09-14 unter http://data.europa.eu/eli/dec/2016/868/oj

[30] *EZB* (2019). What is AnaCredit? Aufgerufen 2020-09-14 unter https://www.ecb.europa.eu/explainers/tellme-more/html/anacredit.en.html

[31] *Deutsche Bundesbank* (2020). Kreditdatenstatistik (AnaCredit). Aufgerufen 2020-09-14 unter https://www.bundesbank.de/de/service/meldewesen/bankenstatistik/kreditdatenstatistik-anacredit--611424

Anfangskapital. Eine detaillierte Auflistung aller Anforderungen findet sich im Merkblatt über die Erteilung einer Erlaubnis zum Erbringen von Finanzdienstleistungen gemäß § 32 Absatz 1 KWG.[32]

Im Hinblick auf Data Governance als Werkzeug zur Erfüllung aufsichtsrechtlicher Vorgaben im Bankenbereich sind hierbei insbesondere die Anforderungen des § 25a KWG zu nennen. Hier wird von Banken eine ordnungsgemäße Geschäftsorganisation verlangt, mit der die Einhaltung der von der Bank zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet wird (vgl. § 25a Absatz 1 Satz 1 KWG). Dabei ist das Risikomanagement von zentraler Bedeutung, da damit die Basis für die Risikotragfähigkeit laufend sichergestellt wird.[33]

Um das gesetzlich geforderte Risikomanagement weiter zu konkretisieren, hat die BaFin das

Rundschreiben zu den Mindestanforderungen an das Risikomanagement (MaRisk) veröffentlicht.[34]. Hierin finden sich etwa detaillierte Vorgaben zur Risikoberichterstattung (vgl. Allgemeiner Teil (AT) 1, MaRisk), Berichtspflichten zur Compliance (vgl. AT 4.4.2, MaRisk), Berichtspflichten der internen Revision (vgl. AT 4.4.3, MaRisk) sowie Anforderungen an die technisch-organisatorische Ausstattung der Banken (vgl. AT 7.2, MaRisk).

Eine weitere Konkretisierung findet sich im ebenfalls von der BaFin veröffentlichten Rundschreiben zu den Bankaufsichtlichen Anforderungen an die IT (BAIT).[35] Hier werden etwa Berichtspflichten des Informationsrisikomanagements (vgl. Nr. 3, BAIT), des Informationssicherheitsmanagement (vgl. Nr. 4, BAIT) und zu IT-Projekten und IT-Projektrisiken (vgl. Nr. 6, BAIT) gefordert.

Auch mit den Anforderungen aus dem KWG, der MaRisk und den BAIT und den mit ihnen verbundenen Berichtspflichten bieten sich mehrere Anknüpfungspunkte für Data Governance, um einen zweckmäßigen Beitrag zu leisten, die aufsichtlichen Vorgaben zu erfüllen.

III. Data Governance

Ansätze zur Organisation, Steuerung und Kontrolle der wachsenden Menge und Vielfalt an Daten in strategischer Hinsicht werden derzeit unter dem Oberbergriff Data Governance (DG) diskutiert. Dem liegt die Sichtweise zugrunde, dass Daten und selbstverständlich gerade auch solche von

[32] *BaFin* (2018). Merkblatt über die Erteilung einer Erlaubnis zum Erbringen von Finanzdienstleistungen gemäß § 32 Absatz 1 KWG. Aufgerufen am 2020-09-14 unter https://www.bafin.de/dok/7851544

[33] *Fiedler, S.* (2018). Analyse der Risikotragfähigkeit. In Basel III und Risikotragfähigkeit (pp. 33-63). Springer Gabler, Wiesbaden.

[34] *BaFin* (2017). Rundschreiben 09/2017 (BA) - Mindestanforderungen an das Risikomanagement – MaRisk. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10149454

[35] *BaFin* (2018). Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018 - Bankaufsichtliche Anforderungen an die IT (BAIT). Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10171052

Finanzinstituten als Vermögenswerte betrachtet werden sollten[36]. Zur Erreichung dieses Ziels müssen u. a. Prozesse, Standards, Regelungen und Verantwortlichkeiten bestimmt werden.[37]

Zur Annäherung an die Kernideen der Data Governance folgen einige Grundlagen insbesondere hinsichtlich der Einordnung und Abgrenzung zu verwandten Begrifflichkeiten. Daran schließt sich eine Vorstellung ausgewählter Nutzenpotenziale an, bevor die unterschiedlichen Handlungsfelder im Rahmen der Data Governance aufgezeigt werden.

1. Einordnung und Grundlagen der Data Governance

Die steigende Bedeutung der Daten für den Unternehmenserfolg führt zu einem sorgfältigen und abgestimmten Umgang mit diesem wertvollen Gut und letztlich zur Etablierung einer eigenständigen Data Governance in den Unternehmen. Data Governance umfasst dann alle Führungsaufgaben, die den risikofreien Zugang zu korrekten Daten gewährleisten und sich in Standards und Verantwortlichkeiten widerspiegeln.[38] Als wesentliches Charakteristikum kann herausgestellt werden, dass Data Governance keine einmalige Aktivität mit begrenztem zeitlichen Rahmen darstellt, sondern eine fortwährende Managementaufgabe. Dabei gilt es, Daten als betriebliche Vermögenswerte zu verstehen und zu behandeln.

Im Ergebnis führt Data Governance dann zu einer Sammlung von Richtlinien, Prozessen, Strukturen, Rollen, Zuständigkeiten und Technologien, durch die Verpflichtungen, Entscheidungsrechte und Zurechenbarkeiten für das effektive Management von Daten umrissen und eingefordert werden.[39] In diesem Sinne beinhaltet Data Governance die Ausübung von Entscheidungshoheit über die Art und Weise, wie die Aufgaben des Datenmanagements ausgeführt werden,[40] mit dem Ziel, den Nutzen zu maximieren, der sich aus der Verwendung von Daten erreichen lässt.

---

[36] *Khatri, V., & Brown, C. V.* (2010). Designing Data Governance. Communications of the ACM, 53 (1), 148; Ladley, J. (2012). Data governance. How to design deploy and sustain an effec-tive data governance program. O. O.: Morgan Kaufmann, 11–13.

[37] *Mosley, M., Brackett, M. H., Earley, S., & Henderson, D*. (2009). The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Bradley Beach, N.J.: Technics Publications LLC, 37.

[38] *Ladley, J.* (2012). Data governance. How to design deploy and sustain an effec-tive data governance program. O. O.: Morgan Kaufmann.

[39] *Villar, M.; Kushner, T., & Wells D.* (2018). Data Governance Fundamentals, www.elearningcurve.com, Abruf am 09.10.2020.

[40] *Finger, R. (2013).* Data Governance und Business Intelligence – Eine Einordnung. In: BI-Spektrum, 022013, 6.

2. Data-Governance-Nutzenpotenziale

Die Nutzenpotenziale einer umfassenden Data Governance sind vielschichtig und spannen breites Spektrum auf. Sie reichen von zusätzlicher Datentransparenz, -qualität und -integrität über Datenschutz, -compliance und -verfügbarkeit bis hin zu gesteigerter Datensicherheit. In einigen Fällen ergibt sich zusätzlich die Option zur Monetarisierung von Teilen des Datenbestandes. Die folgende Tabelle 1 führt einige Nutzenpotenziale auf, die durch Data Governance gehoben werden können, einschließlich der zugehörigen Verbesserung in der Wertschöpfung.

Data-Governance-Nutzenpotenziale	**Beispiel für die Wertschöpfung**
Datentransparenz	- Reduzierung der Suchkosten / Entwicklungszeiten - Erschließung neuer Potenziale / Geschäftsfelder - Reduzierung von Beschaffungskosten externer Daten - Reduzierung von Daten- und Systemredundanzen
Datenqualität / -integrität	- Steigerung der Prozesseffizienz - Grundlage für Automatisierung - Mehr Umsatz, Zufriedenheit und Servicequalität durch 360° Sicht auf Kunden - Weniger Beschaffungs- / Produktionskosten durch Rundumsicht auf Produkte
Datenverfügbarkeit	- Reduzierung der Entwicklungszeiten in der Informationsversorgung und Digitalisierung - Steigerung der Mitarbeiterzufriedenheit und Produktivität - Ermöglichung neuer Geschäftsmodelle - Betrugserkennung - Erkennung von Ineffizienzen
Datenschutz und Datencompliance	- Vermeidung von Bußgeldern - Stärkung der Kundenbindung durch Steigerung des Vertrauens - Stärkung Unternehmensimage

	- Erhalt des Geschäftsmodells / der Lizenzen
Datensicherheit	- Vermeidung von finanziellen Schäden - Vermeidung von Imageschäden - Schutz vor Wirtschaftsspionage - Sicherung des eigenen Wettbewerbsvorteils
Datenmonetarisierung	- Zusätzliches Geschäftsfeld - Zusätzlicher Umsatz durch Data Services für Externe - Neue Kunden / Partner / Fähigkeiten

Tab. 4: Relevanz der Data Governance für die Wertschöpfung[41]

3. Data-Governance-Handlungsfelder

Die Handlungsfelder beim Aufbau einer tragfähigen Data Governance erstrecken sich auf fünf Bereiche, die in den folgenden Ausführungen näher beleuchtet werden sollen:

- Richtlinien und Standards,
- Rollen und Verantwortlichkeiten,
- Prozesse und Verfahren,
- Monitoring und
- Technik.[42]

a) Richtlinien und Standards

Als verbindliche Vorgaben legen Richtlinien (im englischen Sprachraum auch als „policies" bezeichnet) allgemein und auf hoher Abstraktionsebene fest, welche Entscheidungen in Bezug auf den Umgang mit Daten zu treffen sind.[43] Sie beinhalten unter anderem verbindliche Reglungen zu den Bereichen

[41] *Dittmar, C., & Fürber, C.* (2020). Data Governance als Wegbereiter der Digitalisierung. In Gluchowski, P. (Hrsg.). Data Governance. Grundlagen, Konzepte und Anwendungen. dpunkt, Heidelberg.

[42] *Gluchowski, P.* (2020). Data Governance – Einführung und Überblick. In Gluchowski, P. (Hrsg.). Data Governance. Grundlagen, Konzepte und Anwendungen. dpunkt, Heidelberg.

[43] *Soares, S.* (2014). The Chief Data Officer Handbook for Data Governance, MC Press. Boise, 35.

Datenqualität, Datensicherheit, Datenmodellierung oder interner sowie externer Datenaustausch.[4445] So kann beispielsweise festgelegt werden, dass eine angemessenen Qualität der Daten unternehmensweit zu gewährleisten ist und dass eine Modellierung von Daten flächendeckend anhand gleicher Standards zu erfolgen hat.

Standards dienen der Konkretisierung und Implementierung von Richtlinien, erweisen sich folglich als detaillierter und sind für alle Datenmanagementfunktionen festzulegen, wie z.B.

Stammdaten-, Datensicherheits- oder Datenqualitätsmanagement. [46] Somit sollten beispielsweise Standards zur Datenstrukturierung und für die Datenspeicherung erarbeitet, kommuniziert sowie deren Einhaltung überprüft und deren Angemessenheit im Zeitablauf evaluiert werden. Als Beispiel lässt sich hier die Verwendung der Data-Vault-Modellierung bei der Gestaltung eines Core Data Warehouses anführen.

Als eng damit verknüpft erweisen sich Regeln, die es zu definieren gilt und die zunächst aus einer fachlichen Perspektive beispielsweise einzuhaltende Grenzwerte im Bereich der Datenqualität festschreiben oder definierten, wann welche Daten zu archivieren sind.

b) Rollen und Verantwortlichkeiten

Zur Umsetzung der Ziele, die mit einer Data-Governance-Initiative verbunden sind, bedarf es der Zuweisung von Entscheidungsbefugnissen und Zuständigkeiten an Rollen., wobei unter einer Rolle eine Funktion zu verstehen ist, die der Rolleninhaber für das Unternehmen ausübt.[47]

Das Verständnis und die Abgrenzung von Rollen erweist sich zwar als uneinheitlich, häufig wird auf die Rollen Data Owner, Data Steward und teilweise auch auf Data Custodian (technischer Data Steward) verwiesen.[48]

Data Ownership beruht auf dem Gedanken, dass für ein effektives Datenmanagement Verantwortlichkeiten festgelegt werden müssen. Aus diesem Grund werden Dateneigentümer (Data

[44] *Mosley, M., Brackett, M. H., Earley, S., & Henderson, D.* (2009). The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Brad-ley Beach, N.J.: Technics Publications LLC,

[45] ff.

[46] *Soares, S.* (2014). The Chief Data Officer Handbook for Data Governance, MC Press. Boise.

[47] Unter einer Rolle ist eine Funktion zu verstehen ist, die der Rolleninhaber für das Unternehmen ausübt. Eine Funktion umfasst dabei entweder ein bestimmtes Aufgabengebiet bzw. einen definierten Verantwortungsbereich oder ein konkretes Tätigkeitsspektrum. Vgl. *Tsolkas, A., Schmidt, K.* (2017). Rollen und Berechtigungskonzepte. Identity- und Access-Management im Unternehmen, 2. Aufl., Springer, Wiesbaden.

[48] *DGI* (2014). The DGI Data Governance Framework, The Data Governance Institute. Verfügbar unter http:// www.datagovernance.com/ wp-content/ uploads/ 2014 /11/ dgi_framework.pdf, Abruf am 15.09.2018, 17. Gansor, T., & Totok, A. (2015). Von der Strategie zum Business Intelligence Competence Center (BICC), 2. Aufl., Heidelberg.

Owner) bestimmt, die für einen gewissen Teil der Unternehmensdaten und dabei für die Einhaltung von datenbezogenen Regeln und Standards die Verantwortung tragen.[49] Meist handelt es sich hierbei um einen Senior Manager aus dem Fachbereich mit ausgeprägten Kenntnissen der Datensemantik und der fachlichen Datenanforderungen, welcher weitreichende datenbezogene Entscheidungskompetenzen besitzt und zugehörige Richtlinien definiert.

Aufgrund der Komplexität der Dateninhalte, -strukturen und -ströme können sich die Aufgaben eines Data Owners als vielschichtig und aufwendig erweisen. Zur Unterstützung lassen sich Data Stewards einsetzen,[50] die eine effektive Steuerung und Nutzung von Datenbeständen sicherstellen sollen. Meist handelt es sich hierbei um Mitarbeiter aus den Fachbereichen mit ausgeprägtem Daten- und IT-Verständnis und unternehmensweiter Sichtweise auf die

Datenverwendung, die Empfehlungen bezüglich der Datenzugriffe, Datenverteilung, Datensicherheit und Datenaufbewahrung aussprechen. So kann beispielsweise dem Bereich Data Security Management die Zuständigkeit für die Lösung datenbezogener Sicherheitsprobleme zugeordnet sein.[51]

Die Entscheidung über die Zuordnung von Ownership oder Stewardship lässt sich nach unterschiedlichen Kriterien vornehmen, wie etwa nach Datenarten. (z. B. Stamm-, Meta-, Transaktionsdaten) oder Speicherformen (z. B. Dokumente, Datensätze, Sensordaten).

Eine weitere Rolle füllt der Data Custodian (oder Technischer Data Steward) aus, der als Datenspezialist (Architekt, Modellierer, Administrator) aus der IT mit sowohl technischen als auch datenbezogenen Kenntnissen und Kompetenzen in Bezug auf die Datenverwaltung, archivierung, -sicherung und -wiederherstellung aufwartet und dabei u. a. die Vermeidung von Datenverlusten oder -verfälschungen gewährleistet.

Als institutionalisierte (Stabs-)Stelle in der Aufbauorganisation lässt sich ein Data Governance Office verstehen, das eine Unterstützungsfunktion ausübt und weniger als physischer Ort zu verstehen ist, sondern eher als Person oder Personenkreis mit der Zuständigkeit für die Koordination der anfallenden Data-Governance- Aktivitäten.[52] In kleineren Unternehmen kann das DGO mit dem Project Management Office verglichen werden und dient als Ansprechpartner für alle datenbezogenen Projekte. In größeren Organisationen gestaltet sich das Tätigkeitsfeld umfassender und beinhaltet z. B. die Informationsversorgung aller identifizierten Stakeholder. Hier findet sich dann auch die explizite Rolle

[49] *Thomas, G.* (2013a). Assigning Data Ownership. Verfügbar unter http://www.datagovernance.com/assigning-data-ownership, Abruf am 15.09.2018.

[50] *Khatri, V., & Brown, C. V.* (2010). Designing Data Governance. Communications of the ACM, 53 (1), 150.

[51] *Thomas, G.* (2013c). Working with Data Stewards. Approaches to Assigning Data Ownership and Stewardship. Verfügbar unter http://www.datagovernance.com/working-with-data-stewards, Abruf am 15.09.2018.

[52] *Mosley, M., Brackett, M. H., Earley, S., & Henderson, D.* (2009). The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Bradley Beach, N.J.: Technics Publications LLC.

eines Data Governance Managers, dem bisweilen auch der Titel Chief Data Officer (CDO) zugeordnet wird. Die für die Koordinationsfunktion der DG-Aktivitäten zuständigen Personen müssen nicht unbedingt (alle) Experten im Bereich Daten sein, allerdings über ein fundiertes Grundwissen verfügen und insbesondere mit allen Interessengruppen kommunizieren, deren Anliegen verstehen und Aufgaben zuweisen können.[53]

Zu den Aufgaben des DG-Office gehören die Koordination der Entscheidungsfindung sowie Unterstützung in den Bereichen Kommunikation und Dokumentation. Weiterhin lassen sich auch Risiko und Projektmanagement, Qualifizierungsmaßnahmen für Mitarbeiter und die

Festlegung von Metriken zur Messung der Zielerreichung anführen.[54]

c) Prozesse und Verfahren,

Als weiteres Handlungsfeld im Bereich Data Governance sind die Prozesse und Verfahren zu verstehen, die im Sinne einer verbindlichen Ablauforganisation Vorgehensweisen für datenbezogene Aktivitäten festlegen.

Im Einzelnen handelt es sich hierbei um spezifizierte Ablauffolgen für die DG-Kernprozesse Metadaten, Datenqualität, Stammdaten, Datenarchitektur, Datensicherheit etc.[55] Beispielsweise kann es sich hierbei um die Aufnahme neuer, externer Datenbestände, um die Erweiterung von Datenmodellen oder um die Zuweisung von Berechtigungen zu Rollen oder Personen handeln. Die exakte Benennung von einzelnen Schritten bzw. Vorgängen mit der zugehörigen zeitlichen Abfolge erweist sich hier als unabdingbar.

Offensichtlich ist die enge Verknüpfung zum Handlungsfeld Rollen und Verantwortlichkeiten, da im Idealfall alle einzelnen Vorgänge konkreten Rollen zugeordnet werden.

d) Monitoring

Die Einhaltung von erstellten Vorgaben wie Regeln oder Standards ist zu kontrollieren, denn erst durch regelmäßige Messungen und Auswertungen zuvor definierter quantitativer Messgrößen lassen sich Abweichungen und Auffälligkeiten identifizieren, um gegebenenfalls entgegensteuernd einzuwirken.

---

[53] *Thomas, G.* (2013b). Establishing a Data Governance Office. Verfügbar unter http://www.datagovernance.com/establishing-a-data-governance-office Abruf am 15.09.2018.

[54] *Plotkin, D.* (2014). Data Stewardship: An Actionable Guide to Effective Data Management and Data Governance. Waltham, MA: Morgan Kaufmann, 17–19.

[55] *Dittmar, C., & Fürber, C.* (2020). Data Governance als Wegbereiter der Digitalisierung. In Gluchowski, P. (Hrsg.). Data Governance. Grundlagen, Konzepte und Anwendungen. dpunkt, Heidelberg.

Eine Abbildung der Ergebnisse kann dann z. B. in einem DGDashboard erfolgen, das Kennzahlen aus den verschiedenen Themenfeldern zusammenhängend darstellt.

e) Technik

Für die bislang dargestellten Handlungsfelder bedarf es einer angemessenen technischen Unterstützung, um die vielfältigen Aufgaben wirksam zu unterstützen. Den Ausgangspunkt bildet hierbei die gewählte technische Architektur, deren Aufbau den Umgang mit den einzelnen Aktivitätenbündeln maßgeblich bestimmt. Zu integrieren sind geeignete Tools für die Themenbereiche Datenqualität, Stammdatenmanagement sowie Datenschutz, Datensicherheit und vor allem Metadatenmanagement.

IV. Zusammenfassung

Banken müssen umfangreichen aufsichtlichen Anforderungen, die dabei laufenden Änderungen und Anpassungen unterliegen, gerecht werden. So haben internationale Standardsetter wie der BCBS ebenso einen Einfluss wie europäische Vorgaben und nationale Mindestanforderungen. Sofern etwa Berichtspflichten erfüllt werden müssen, sind teils unterschiedliche Behörden wie etwa die Deutsche Bundesbank und die BaFin die Adressaten.

Data Governance repräsentiert einen Ansatz, mit dem sich ein Rahmen für das professionelle Management von Daten schaffen lässt. Die aufgezeigten Nutzenpotenziale verdeutlichen, dass sich hierdurch Transparenz und Nachvollziehbarkeit in Bezug auf Daten erheblich verbessern lassen. Aus diesem Grund trägt Data Governance in erheblichem Ausmaß zur leichteren und besseren Erfüllbarkeit der gesetzlichen Vorgaben bei.

Literaturen

Arboleda, P., Bagheri, S., & Khakzad, F. (2016). Model risk. In the context of the regulatory climate change. Working Paper.

Asprion, P. M., & Knolmayer, G. (2016). IT-Governance. In Enzyklopädie der Wirtschaftsinformatik, http://www.enzyklopaedie-der-wirtschaftsinformatik.de/ lexikon/ daten-wissen/ Grundlagen-derInformationsversorgung/ IT-Governance, Abruf am 03.10.2020.

BaFin (2016). Zulassung von Banken und Finanzdienstleistern sowie von Zahlungs- und E-Geldinstituten. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/7846482

BaFin (2017). Informationen zum Meldeverfahren für schwerwiegende Betriebs- und Sicherheitsvorfälle bei Zahlungsdienstleistern. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10020844

BaFin (2017). PSD2-Zahlungssicherheitsvorfälle. Meldungen nach § 54 Absatz 1 Satz 1 ZAG. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10241070

BaFin (2017). Rundschreiben 09/2017 (BA) - Mindestanforderungen an das Risikomanagement – MaRisk. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/ 10149454

BaFin (2018). Merkblatt über die Erteilung einer Erlaubnis zum Erbringen von Finanzdienstleistungen gemäß § 32 Absatz 1 KWG. Aufgerufen am 2020-09-14 unter https://www.bafin.de/dok/7851544

BaFin (2018). Rundschreiben 08/2018 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle. Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/ 10941432

BaFin (2018). Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018 - Bankaufsichtliche Anforderungen an die IT (BAIT). Aufgerufen 2020-09-14 unter https://www.bafin.de/dok/10171052

BaFin (2019). Zahlungsdienste und PSD2. Aufgerufen am 2020-09-14 unter https://www.bafin.de/dok/12672828

BCBS (2013). Principles for effective risk data aggregation and risk reporting. Aufgerufen 2020-09-14 unter https://www.bis.org/ publ/ bcbs239.pdf

Brananova, O. C., & Watfe, G. (2017). Use of AnaCredit granular data for macroprudential analysis. IFC Bulletins Chapters, 46.

Busch, D. (2017). MiFID II and MiFIR: stricter rules for the EU financial markets. Law and Financial Markets Review, 11(2-3), 126-142.

Claessens, S., & Van Horen, N. (2015). The impact of the global financial crisis on banking globalization. IMF Economic Review, 63(4), 868-918.

Claessens, S., Laeven, M. L., Igan, D., & Dell'Ariccia, M. G. (2010). Lessons and policy implications from the global financial crisis (No. 10-44). International Monetary Fund.

Cree, M. (2015). BCBS 239–Principles for effective risk data aggregation and reporting. Risk.

Deutsche Bundesbank (2020). Kreditdatenstatistik (AnaCredit). Aufgerufen 2020-09-14 unter https://www.bundesbank.de/de/service/ meldewesen/bankenstatistik/kreditdatenstatistik-anacredit-611424

DGI (2014). The DGI Data Governance Framework, The Data Governance Institute. Verfügbar unter http:// www.datagovernance.com/ wp-content/ uploads/ 2014 /11/ dgi_framework.pdf, Abruf am 15.09.2018.

Dittmar, C., & Fürber, C. (2020). Data Governance als Wegbereiter der Digitalisierung. In Gluchowski, P. (Hrsg.). Data Governance. Grundlagen, Konzepte und Anwendungen. (pp. 13-31). dpunkt, Heidelberg, 13-31.

European Banking Authority (2019). EBA/GL/2019/04 - Guidelines on ICT and security risk management. Aufgerufen 2020-09-14 unter https://eba.europa.eu/regulation-and-policy/internalgovernance/guidelines-on-ict-and-security-risk-management

European Securities and Markets Authority (2017). MIFID II. Aufgerfen 2020-09-14 unter https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

EZB (2016). Decision (EU) 2016/868 of the European Central Bank of 18 May 2016 amending Decision ECB/2014/6 on the organisation of preparatory measures for the collection of granular credit data by the European System of Central Banks (ECB/2016/14). Aufgerufen 2020-09-14 unter http://data.europa.eu/eli/dec/2016 /868/oj

EZB (2019). What is AnaCredit? Aufgerufen 2020-09-14 unter https://www.ecb.europa.eu/explainers/tell-memore/html/anacredit.en.html

Fiedler, S. (2018). Analyse der Risikotragfähigkeit. In Basel III und Risikotragfähigkeit (pp. 33-63). Springer Gabler, Wiesbaden.

Finger, R. (2013). Data Governance und Business Intelligence – Eine Einordnung. In BI-Spektrum, 02-2013.

Gansor, T., & Totok, A. (2015). Von der Strategie zum Business Intelligence Competence Center (BICC), 2. Aufl., Heidelberg 2015.

Gillet, R., Ligot, S., & Firouzi, H. O. (2017). The challenges and implications of the Markets in Financial Instruments Directive (MiFID) and of its revision (MiFID II, MiFIR) on the efficiency of financial markets. In Financial Regulation in the EU (pp. 151-198). Palgrave Macmillan, Cham.

Gillet, R., Ligot, S., & Firouzi, H. O. (2017). The challenges and implications of the Markets in Financial Instruments Directive (MiFID) and of its revision (MiFID II, MiFIR) on the efficiency of financial markets. In Financial Regulation in the EU (pp. 151-198). Palgrave Macmillan, Cham.

Gluchowski, P. (2020). Data Governance – Einführung und Überblick. In Gluchowski, P. (Hrsg.). Data Governance. Grundlagen, Konzepte und Anwendungen. (pp. 3-12). dpunkt, Heidelberg.

Göbel, C. A. (2017). Chancen und Herausforderungen durch die PSD2 und Instant Payment. In Mobile Payment (pp. 167-178). Springer Gabler, Wiesbaden.

Grody, A. D. (2018). Rebuilding financial industry infrastructure. Journal of Risk Management in Financial Institutions, 11(1), 34-46.

Khatri, V., & Brown, C. V. (2010). Designing Data Governance. Communications of the ACM, 53 (1), 148-152.

Ladley, J. (2012). Data governance. How to design deploy and sustain an effective data governance program. O. O. Morgan Kaufmann.

Lütgerath, N. (2016). Die Vorgaben zur ordnungsgemäßen Geschäftsorganisation im Bankaufsichtsrecht.

Maksimovic, T., & Biernat, H. (2019). MaRisk und BAIT im Detail. In Bankaufsichtliche Anforderungen an die IT (BAIT) (pp. 17-54). Springer Gabler, Wiesbaden.

Mosley, M., Brackett, M. H., Earley, S. & Henderson, D. (2009). The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Bradley Beach, N.J. Technics Publications LLC.

Orgeldinger, J. (2018). The Implementation of Basel Committee BCBS 239: Short analysis of the new rules for Data Management. Journal of Central Banking Theory and Practice, 7(3), 57-72.

Papaconstantinou, G. A. (2016). Investment bankers in conflict: the regime of inducements in MiFID II and the member states' struggle for fairness. European review of contract law, 12(4), 356-390.

Pfisterer, P. (2015). Die neuen Regelungen der MiFID II zum Anlegerschutz: Analyse und Vergleich zur bestehenden Rechtslage. Springer-Verlag.

Plotkin, D. (2014). Data Stewardship: An Actionable Guide to Effective Data Management and Data Governance. Waltham, MA. Morgan Kaufmann.

Schulze, K.-D., Dittmar, C., & Ballerstedt, D. (2016). Auf dem Weg zur Data Driven Company – Wie die fortschreitende Digitalisierung die klassische BI verändert. Vortrag auf der TDWI-Jahreskonferenz, München, 21.06.2016.

Sironi, A. (2018). The evolution of banking regulation since the financial crisis: A critical assessment. Baffi Carefin Centre Research Paper, (2018-103).

Thomas, G. (2013a). Assigning Data Ownership. Verfügbar unter http://www.datagovernance.com/assigningdata-ownership, Abruf am 15.09.2018.

Thomas, G. (2013b). Establishing a Data Governance Office. Verfügbar unter http://www.datagovernance.com/establishing-a-data-governance-office, Abruf am 15.09.2018.

Thomas, G. (2013c). Working with Data Stewards. Approaches to Assigning Data Ownership and Stewardship. Verfügbar unter http://www.datagovernance.com/working-with-data-stewards, Abruf am 15.09.2018.

Tsolkas, A., & Schmidt, K. (2017). Rollen und Berechtigungskonzepte. Identity- und Access-Management im Unternehmen, 2. Aufl., Springer, Wiesbaden.

Villar, M.; Kushner, T., & Wells D. (2018). Data Governance Fundamentals, www.elearningcurve.com, Abruf am 09.10.2020.