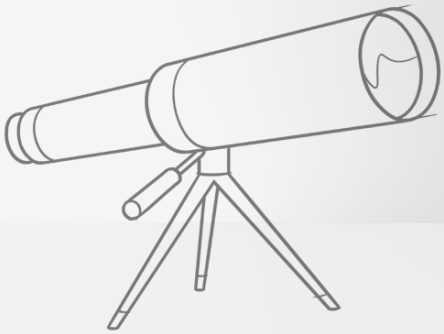
» REGULATORY TRENDS IN BANKING



Seit der Finanzmarktkrise, die ihren Höhepunkt in 2008 hatte, sind nun 10 Jahre vergangen. In dieser Zeit haben die Regulatoren bereits eine Vielzahl an neuen Regelungen für Banken veröffentlicht und Gesetze wie das CRD-IV-Paket verabschiedet.

Noch immer werden laufend Anpassungen am bestehenden Regelwerk vorgenommen, um neue Erkenntnisse einfließen zu lassen – die Regulierungsflut bricht folglich auch nach einer Dekade intensiver Nachjustierungen und Neuregulierungen nicht ab.

In diesem Paper schauen wir nun auf die nächsten 10 Jahre und haben für Sie die aktuellen Trends und Entwicklungen in den Bereichen Bankenregulierung und Aufsichtspraxis zusammengestellt.

Auf der einen Seite geht es dabei mit der „Finalisierung von Basel III" (BCBS 424) verstärkt in Richtung **Abkehr** bis hin Verbot von **internen Modellen** (TREND 1); auf der anderen Seite rücken **neue Risiken** wie das Cyberrisiko (TREND 2) in den Fokus der Aufsicht. Weiterhin kristallisiert sich die Tendenz zur **Meldung einzelner Data Cubes** anstelle von aggregierten Reports (TREND 3) heraus – ein Grund dafür, dass viele Banken nun vermehrt auf die **Standardisierung und Konsolidierung ihrer IT-Anwendungen** auf Konzernebene (TREND 4) setzen. Insgesamt wird die Erfüllung regulatorischer Anforderungen zunehmend komplexer und herausfordernder; eine vorausschauende Planung wird unabdingbar.

» TREND 1
ABKEHR VON INTERNEN MODELLEN

AUSGANGSLAGE

Interne Modelle nehmen aktuell eine bedeutende Rolle bei der Bestimmung der **regulatorischen Eigenmittel** sowie bei der internen **Risikobewertung** ein. Verglichen mit Standardansätzen ermöglichen sie eine risikosensitivere Ermittlung der RWAs und können durch diese präzisere Betrachtung zu einer Reduktion der erforderlichen Eigenkapitalunterlegung führen.

Im Rahmen des aufsichtsrechtlichen Überprüfungsprozesses (SREP) zeigte sich jedoch, dass die Verwendung interner Modelle bei Banken mit ähnlichen Risikoportfolien zu einer **heterogenen** Risikobewertung und somit zu **nicht vergleichbaren** Eigenmittelanforderungen führt.

Die Aufsicht reagierte mit der Einführung des Total Review of Internal Models (TRIM)[1], einer Überprüfung der internen Modelle bei systemrelevanten Banken. Hierdurch sollten die Angemessenheit zugelassener Säule-1-Modelle bestätigt, die Sicherstellung der Einhaltung regulatorischer Standards gewährleistet und eine Harmonisierung der Aufsichtspraktiken im Single Supervisory Mechanism (SSM) erreicht werden.

Neben der Überarbeitung des Modellabnahme-Prozesses rückt vermehrt die Diskussion in den Fokus, ob und inwiefern interne Modelle überhaupt für die Ermittlung der Eigenmittelanforderungen zugelassen und angewendet werden sollten.

TREND

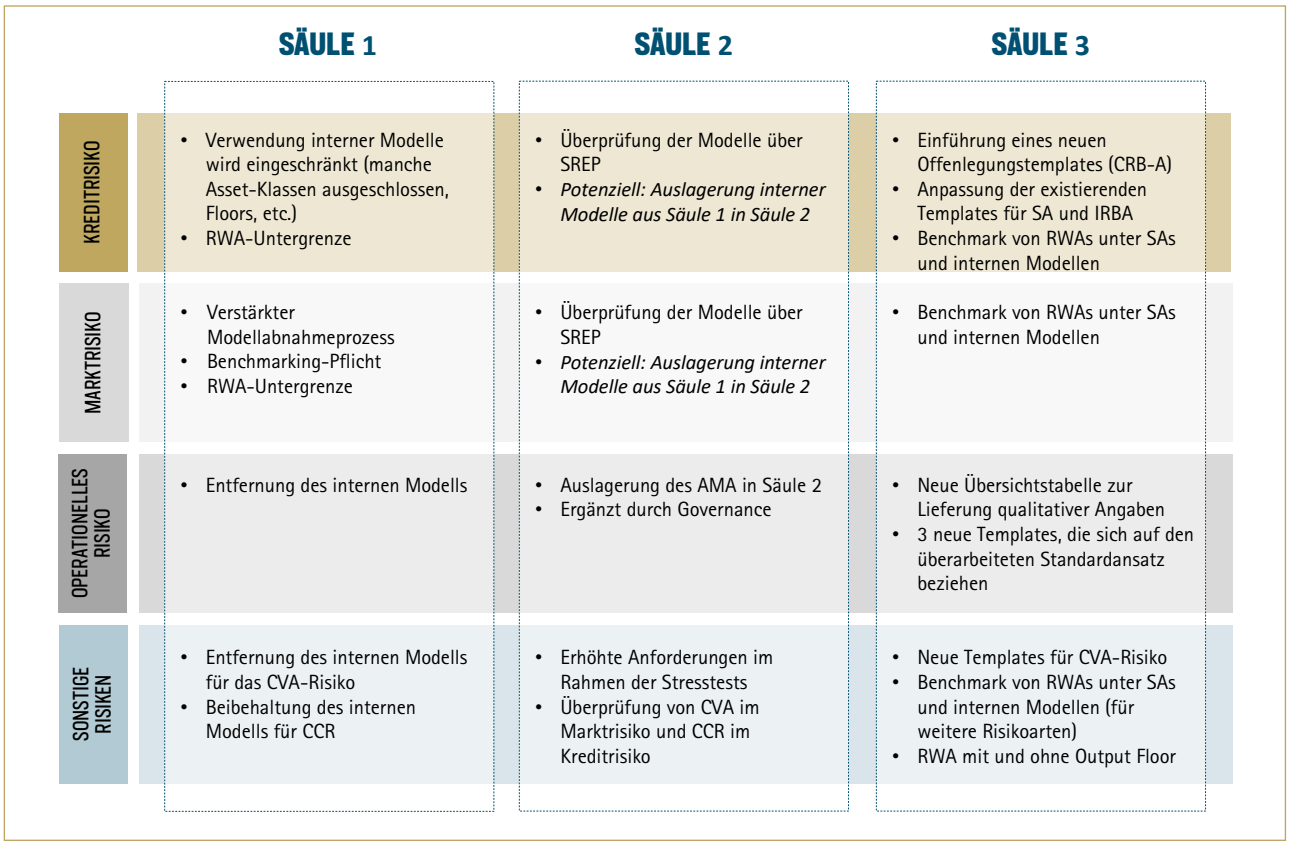
Aufsicht und Regulatoren wenden sich vermehrt von bankinternen Modellen zur Bestimmung der Risiken und Eigenmittelanforderungen von Banken ab. Stattdessen nehmen sie einfache, risikosensitive und standardisierte Methoden ins Visier, deren Nachvollziehbarkeit und Vergleichbarkeit die Überwachung der Finanzstabilität erleichtern sollen. Auch tendiert die Aufsicht zur Verwendung von Standardansätzen, um größeren und komplexeren Banken keinen Vorteil durch überlegene Ressourcen zu verschaffen.

Diese Bestrebungen spiegeln sich besonders in der im Dezember 2017 veröffentlichten Basel-III-Reform wider. Mit der **Finalisierung des Basel-III-Paketes**[2] werden Standardansätze mit erhöhter Risikosensitivität für das Kreditrisiko, das Kreditbewertungsrisiko (CVA Risk) und das operationelle Risiko (OpRisk) eingeführt. Für das Kreditrisiko bedeutet dies, dass unter anderem neue Forderungsklassen (wie z. B. nachrangige Verbindlichkeiten und Pfandbriefe) eingeführt, die vorgeschriebenen Risikogewichte angepasst sowie die Pflicht zur Durchführung von Due-Diligence-Prüfungen eingeführt werden. Der überarbeitete Standardansatz für das OpRisk ist neu kalibriert, statt des Bruttoertrags wird der volumenorientierte „Business Indicator" als Referenzgröße verwendet. Weiterhin wird eine historische Verlustkomponente eingeführt, d.h. bei großen Instituten müssen eigene Verlustdaten einbezogen werden. Jedoch dürfen Ereignisse mit einem Schadenwert kleiner als 20.000 Euro außer Acht gelassen werden.

Zusätzlich werden die internen Modelle für CVA Risk und OpRisk aus Säule 1 ausgeschlossen und für das Kreditrisiko eingeschränkt. So wird die Nutzung des fortgeschrittenen IRB-Ansatzes für Risiken gegenüber Groß- und mittelständischen Unternehmen sowie gegenüber Banken und Finanzinstituten zukünftig nicht mehr zulässig sein, da für diese Forderungsklassen keine robuste und zurückhaltende Modellierung des Kreditrisikos möglich sei. Außerdem wird der fortgeschrittene IRB-Ansatz für Risiken gegenüber Einrichtungen, die typischerweise nur einen kleinen Anteil am Kreditrisiko haben, gestrichen. Dies bedeutet, dass sich die Aufsicht in einem ersten Schritt der Abkehr von internen Modellen widmet.

[1] Siehe auch: https://www.bankingsupervision.europa.eu/about/ssmexplained/html/trim.en.html

[2] Standard BCBS 424 (Basel III: Finalising Post-Crisis Reform)



Quelle: ifb group

Bei der Beaufsichtigung der Institute, denen die Nutzung des IRB-Ansatzes genehmigt wurde, liegt der Fokus im zweiten Schritt darauf, eine **unverhältnismäßige Reduktion der Eigenmittelanforderungen** durch die Anwendung des internen Modells zu **verhindern**. Zum Beispiel wird durch die Anwendung fester Werte für die Höhe des Verlustes, den Loss Given Default (LGD), im Basis-IRB-Ansatz die RWA-Variabilität behoben. Zusätzlich werden sowohl im Basis- als auch im fortgeschrittenen IRB-Ansatz Untergrenzen, sogenannte Input Floors, für die Ausfallwahrscheinlichkeit, die Probability of Default (PD), sowie für LGD und Exposure at Default (EAD) (nur im fortgeschrittenen IRB-Ansatz) eingeführt. Auch werden Haircuts, die für Sicherheiten angewendet werden, erhöht und LGD-Parameter reduziert.

Die grundlegendste Änderung ist jedoch die **Einführung einer Gesamt-RWA-Untergrenze** in Form eines *Output Floors*: durch die Nutzung des IRB-Ansatzes darf der Wert für die Gesamt-RWAs höchstens bei 72,5% des Wertes, der sich bei der Verwendung der jeweiligen Standardansätze ergeben würde, angesetzt werden.

Um diesen Änderungen des Basel-III-Frameworks auch im Rahmen der **Offenlegung** gerecht zu werden, wurde im Februar 2018 ein Konsultationsentwurf zur Überarbeitung der Säule-3-Anforderungen[3] veröffentlicht. Neben der Anpassung der bestehenden Offenlegungspflichten für Kreditrisiko, OpRisk und CVA Risk sieht das Baseler Komitee auch die Einführung einer ganz neuen Offenlegungspflicht vor: ein **Benchmarking von RWAs** nach internen Modellen gegen RWAs nach Standardansatz. Konkret bedeutet dies, dass die RWAs, die sich bei der Anwendung interner Modelle ergeben, mit den RWAs gemäß Standardansatz auch pro Risikoart verglichen werden können. So sollen Transparenz erhöht und Vergleichbarkeit zwischen Banken verbessert werden.

[3] Standard BCBS 400 (Pillar 3 disclosure requirements – consolidated and enhanced framework, Consultative Version)

WIRKUNG

KURZFRISTIG sind mit den neuen regulatorischen Vorgaben für die Banken Kosten verbunden, denn sie müssen ihre IT-Systeme, Berechnungsmethodiken und Reportingprozesse anpassen und sich auf möglicherweise höhere Eigenmittelanforderungen vorbereiten. Denn sowohl die Einführung des Output Floors als auch die Verwendungspflicht der Standardansätze für CVA Risk und OpRisk können mittelfristig zu erhöhten RWA-Werten und damit auch höheren Kapitalanforderungen führen. Die Beschaffung von Eigenmitteln könnte also kostspieliger werden und Institute könnten – in Extremfällen – gezwungen sein, geringere Ausschüttungen vorzunehmen.

LANGFRISTIG ergeben sich durch die Standardisierung der Risikomodelle jedoch auch Chancen. Für Stakeholder sollte es leichter werden, verschiedene Institute in Bezug auf die eingegangenen Risiken und die vorgehaltenen Kapitalpuffer zu vergleichen. Aber auch Banken könnten profitieren. Denn interne Modelle sind komplex, teuer umzusetzen, benötigen eine große Datenhistorie und weisen einen langwierigen Abnahmeprozess auf. Mit ihrer Entfernung aus Säule 1 geht folglich eine Möglichkeit zur Kostenreduzierung einher. Anderweitig muss die Modell-Governance schlanker und günstiger werden, zum Beispiel durch standardisierte „off-the-shelf" Risikomodelle, die von Drittanbietern verkauft, betrieben und somit ausgelagert werden könnten. Derartige Auslagerungen wären unter anderem für die Risikomessung von Kredit- oder Marktrisiko für regulatorische, eventuell sogar für ökonomische Zwecke denkbar.

ZUSAMMENGEFASST

Aktuell wendet sich die Aufsicht verstärkt von internen Modellen ab, was sich einerseits in der weitreichenden Einschränkung dieser in Säule 1, andererseits in erhöhten Anforderungen an die Modellabnahme zeigt. Banken sollten folglich ihren Fokus auf interne Modelle reduzieren, um Kosten zu sparen; gleichzeitig müssen sie sich frühzeitig auf potenziell höhere Eigenmittelanforderungen einstellen.

» TREND 2

ZUKUNFT DER SÄULE 2 – NEUE RISIKEN & GOVERNANCE

AUSGANGSLAGE

Die **klassischen Risikoarten** Kredit-, Markt- und Liquiditätsrisiko haben sowohl in der Regulierung als auch in der Ökonomie einen **hohen Reifegrad** erreicht – Berechnung und Steuerung sind inzwischen größtenteils durch regulatorische Vorgaben in Säule 1 standardisiert und in internen Bankprozessen sowie in Säule 2 verankert.

Inzwischen rücken **neue Risikoarten** in den Fokus der Aufsicht, darunter unter anderem **Cyber- und Modellrisiko**, welche aufsichtsrechtlich dem operationellen Risiko (OpRisk) zuzurechnen sind.

Der Standardansatz in Säule 1 für das OpRisk ist allerdings ein eher grober Indikator, der lediglich zu einer vergleichbaren Ermittlung der Eigenmittelunterlegung dient und einzelne Risikounterarten nicht explizit betrachtet – der Regulator verschiebt die Berücksichtigung dieser stattdessen bis auf weiteres in **Säule 2**.

TREND

Das Baseler Komitee (BCBS) hat erst kürzlich einen neuen Standardansatz für die Berücksichtigung des operationellen Risikos in **Säule 1** erarbeitet (Standardised Measurement Approach, **SMA**). Da die Idee eines internen Modells (Advanced Measurement Approach, AMA) bis auf weiteres fehlgeschlagen ist, wird der Standardansatz um eine **historische Verlustkomponente** ergänzt, der die idiosynkratische Natur operationeller Risiken widerspiegeln soll.

In der **Säule 2** erfolgt die aufsichtsrechtliche Steuerung operationeller Risiken nun vermehrt über **explizite Governance-Vorgaben**, u.a. im Rahmen des SREP. Dabei werden auch „neue", bisher nicht oder kaum explizit regulierte **Risikoarten** berücksichtigt.

Für besonders wichtig im Jahr 2018 halten Risikomanager operationelle Risiken, die schwer quantifizierbar sind und – sollten sie schlagend werden – enorme Verluste mit sich bringen.[4] Dazu zählen unter anderem das Cyberrisiko, das Modellrisiko und das geopolitische Risiko. Diese Risikoarten wurden bisher aufgrund der geringen Eintrittswahrscheinlichkeit kaum beobachtet, geschweige denn gesteuert; durch globale Entwicklungen steigt ihre Eintrittswahrscheinlichkeit jedoch stetig an. Daher werden gerade die neuen bzw. erst in den letzten Jahren relevant gewordenen Risikoarten aufsichtsrechtlich über Governance-Vorgaben gesteuert.

In ihrer **„Pillar 2 Roadmap"**[5] (veröffentlicht im April 2017) bestätigt die EBA diesen Fokus und nennt Internal Governance als einen der Bereiche innerhalb der SREP Guidelines, die sie zu aktualisieren und auch zukünftig verstärkt zu berücksichtigen beabsichtigt.

In ihrem Ende 2017 veröffentlichten Konsultationsentwurf für die Überarbeitung des SREP[6] ergänzt sie dementsprechend die Vorgabe, dass nationale Aufsichtsbehörden den bankindividuellen Risiko-Score nicht mehr einzig und allein durch die Einschätzung inhärenter Risiken bestimmen, sondern zusätzlich Überlegungen zu Risikomanagement und Kontrollen miteinbeziehen sollen.

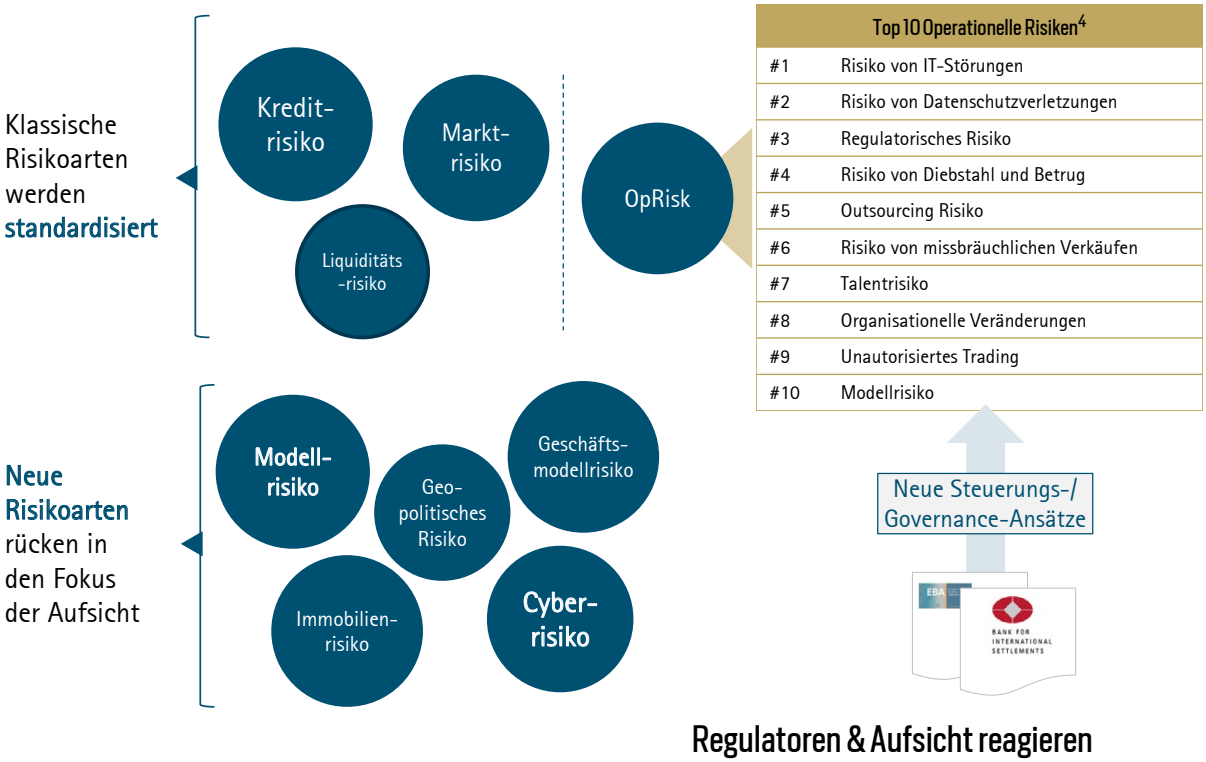
Trotz allem sind die regulatorischen Vorgaben zu neueren Risikoarten wie Modell- oder Cyberrisiko bisher **eher allgemein gefasst** und wenig ausgereift. Leitfäden zu Messmethoden, wie zum Beispiel zu Stresstests oder Szenarioanalysen, sucht man derzeit noch vergeblich.

[4] Siehe auch: https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018

[5] Siehe auch: https://www.eba.europa.eu/-/eba-outlines-roadmap-of-its-plan-to-update-2017-2018-srep

[6] EBA/CP/2017/18: Consultation Paper on Draft Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing

Die Verankerung der neuen Risikoarten in der öffentlichen und aufsichtsrechtlichen Diskussion lässt aber vermuten, dass sich dies zukünftig ändern könnte. Eine frühzeitige Auseinandersetzung mit der Thematik ist aus Perspektive der Banken also maßgeblich, auch da das Risikocontrolling bezüglich der neuen Risiken schon im Zuge des SREP 2018 vermehrt überprüft werden soll.



Quelle: ifb group

FÜR DIE FOLGENDEN RISIKOARTEN LÄSST SICH DIE RICHTUNG DER AUFSICHT BEREITS ABSCHÄTZEN:

CYBERRISIKO

In einem Report zum G20 Gipfel 2017 in Hamburg[7] nannte das Financial Stability Board (FSB) den Umgang mit Cyberrisiken als eine der drei großen Prioritäten für die internationale Zusammenarbeit im aufsichtsrechtlichen und regulatorischen Bereich.

Auch die Bank for International Settlements (BIS) hat sich bereits ausführlich mit Cyberrisiken auseinandergesetzt. Einem Paper[8] über aktuelle regulatorische Ansätze zum Umgang mit Cyberrisiken zufolge existieren im internationalen Vergleich derzeit **zwei gegensätzliche Ansichten**:

[7] Siehe auch: www.fsb.org/2017/06/fsb-issues-a-report-on-the-financial-stability-implications-from-fintech/

[8] Crisanto, J. C., & Prenio, J. (2017). Regulatory approaches to enhance banks' cyber-security frameworks. *FSI Insights on policy implementation No 2.*

1. Der Großteil aller Bankaufsichtsbehörden ist bisher der Auffassung, das Cyberrisiko müsse im Aufsichtsrecht nicht als eigenständige Risikoart berücksichtigt werden, sondern könne als **Teil des Op-/TechRisk** im Rahmen der derzeitigen Regulierungen abgedeckt werden.
2. Einige wenige Jurisdiktionen (darunter Hongkong, Singapur, Großbritannien und die USA) teilen diese Auffassung jedoch nicht mehr; ihrer Ansicht nach ist eine **explizite Regulierung des Cyberrisikos** erforderlich. Dabei greifen manche auf einen prinzipienbasierten Ansatz zurück, während andere die Anwendung spezifischer Vorschriften bevorzugen.

Die wenigen derzeit bestehenden Regulierungsvorschriften zu Cyberrisiken könnten zukünftig auch von weiteren Jurisdiktionen in Erwägung gezogen werden – sollte sich der ausdrückliche Einbezug des Cyberrisikos in die regulatorische Landschaft international durchsetzen.

Seit dem 1. Januar 2018 gilt auch für europäische Aufsichtsbehörden eine spezifische Richtlinie zur Berücksichtigung von Cyberrisiken – oder genauer des „**Information and Communication Technology, ICT-Risikos**" – als Komponente des OpRisk im Rahmen des SREP. In der im Mai 2017 veröffentlichten Richtlinie[9] definiert die EBA neben dem Aufkommen (neuer) Cyberrisiken im Sinne von Angriffen auf die IT-Landschaft auch die erhöhte Abhängigkeit von ausgelagerten ICT-Dienstleistungen und Drittanbieter-Produkten als Teile des Cyberrisikos. Bei der Überprüfung der Banken sollen die nationalen Aufsichtbehörden explizit auf die Abdeckung des Cyberrisikos im Rahmen der Internal Governance sowie auf die hinreichende Berücksichtigung in der internen Risikoabbildung eingehen.

Die Entwicklung der regulatorischen Betrachtung des Cyberrisikos bleibt abzuwarten. Es ist jedoch absehbar, dass Regulatoren zunehmend auf qualitative Vorgaben wie Governance setzen, um Banken zu einem bewussten Risikomanagement zu bewegen.

MODELLRISIKO

Schon 2011 hat das Federal Reserve Board, als eine der drei amerikanischen Bankenaufsichtsbehörden, mit der Richtlinie SR-11-7[10] einen prinzipienbasierten Ansatz für die Überwachung und Einschätzung des **aggregierten Modellrisikos** auf den Weg gebracht.

In Europa ist das Modellrisiko bereits im SREP als **Teil des OpRisk** zu berücksichtigen. Neben dem Risiko, die Eigenmittelanforderungen durch die Anwendung interner Modelle zu unterschätzen, sind hierunter auch Verluste aus der Entwicklung, der Implementierung oder dem unangemessenen Einsatz interner Modelle gefasst. Die Überprüfung bezieht sich auf Governance-Fragestellungen und das Risikobewusstsein des Instituts – quantitative Anforderungen sind bisher nicht gesetzlich verankert.

Das heißt: Europäische Regulatoren folgen verstärkt dem amerikanischen Vorbild und setzen auf **Modell-Governance**. Dabei haben sie bisher vor allem das erste Teilrisiko, die mögliche Unterschätzung der Eigenmittelanforderungen, im Blick. So sollen z. B. durch Mindest-PDs/-LGDs und Output Floors starke Abweichungen zwischen den Ergebnissen aus Standardansätzen und internen Modellen verhindert werden, während mit TRIM (Targeted Review of Internal Models) eine jährliche Modellüberprüfung eingeführt wurde.

In 2018 könnte das zweite Teilrisiko, Verluste aufgrund des Einsatzes interner Modelle, an Relevanz gewinnen – insbesondere, da spezifische Vorgaben zur Messung und Steuerung des Modellrisikos noch fehlen. Verstärkt wird die Relevanz zusätzlich dadurch, dass Banken vermehrt neue Methoden wie z. B. **Machine learning** für die Modellselektion und -validierung nutzen.

Dies ist nicht zwangsläufig im Sinne von Regulatoren und Aufsicht, wie eine Stellungnahme der Federal Reserve zeigt: Ihrer Meinung nach führe die Nutzung von Machine learning für die Modellvalidierung zu systemischem Modellrisiko, außerdem fehle Transparenz.

[9] EBA/GL/2017/05: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)
[10] Siehe auch: https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf

Der Umgang mit Machine learning und weiteren fortschrittlichen Validierungsmethoden stellt eine große Herausforderung für die Regulatoren dar: Die Überwachung derartiger „Black-Box-Modelle" ist schwierig bis hin unmöglich und komplexe Methoden, die risikoartenübergreifend das Modellrisiko schätzen sollen, stellen in sich ein neues Modellrisiko dar. Von diesem Standpunkt aus erscheint der steigende Fokus auf standardisierte Modelle nachvollziehbar.

Trotz der zunehmenden Abkehr von internen Modellen ist festzuhalten: Das Modellrisiko gewinnt in der Wahrnehmung der Aufsicht an Bedeutung und wird verstärkt im Rahmen der Säule 2 überwacht.

WIRKUNG

KURZFRISTIG müssen Banken mit erhöhtem Dokumentationsaufwand und steigenden Kosten für Internal Governance und Compliance mit Säule-2-Vorgaben rechnen.

LANGFRISTIG könnte die Abkehr von internen Modellen die Quantifizierung des Modellrisikos erleichtern und die Bedeutung dieser Risikoart reduzieren. Cyberrisiken hingegen werden in Bedeutung und Größe weiter steigen und müssen mit adäquaten Ansätzen und Strategien gesteuert werden.

INSGESAMT GILT

Der Einbezug neuer Risikoarten ins Aufsichtsrecht und ein verstärkter Fokus auf die Internal Governance von Banken zeichnet sich deutlich im aktuellen Geschehen ab. Insbesondere Cyber- und Modellrisiken werden intensiv diskutiert und könnten im kommenden Jahr Bestandteil neuer Veröffentlichungen der Aufsicht sein.

Um effektiv und informiert auf solch neue Regulierungen reagieren zu können, ist eine frühzeitige Auseinandersetzung mit den relevanten Sachverhalten kritisch. Ansätze anderer Regulatoren wie z. B. der Federal Reserve können hierbei als Hilfestellung dienen.

» TREND 3
VON AGGREGIERTEN REPORTS ZU EINZELNEN DATA CUBES

AUSGANGSLAGE

Seit der Finanzkrise sind die regulatorischen Anforderungen an Banken stetig gestiegen. Um künftig systemische Krisen besser verhindern zu können, setzen die Aufsichtsbehörden und Zentralbanken vermehrt auf intern durchgeführte Analysen, wie z. B. Stress Tests oder Simulationen, und auf Ad-Hoc Reporting. Dafür werden zunehmend **Daten in granularer Form** benötigt.

Die derzeit gültigen Meldevorschriften sind **heterogen**: Sie fordern zum einen von den Banken, eine Vielzahl vorgefertigter Formulare mit aggregierten Daten an die Zentralbanken und/oder Aufsichtsbehörden zu übermitteln; zum anderen sehen erste Meldungen (z. B. Statistics on Holdings of Securities, SHS) explizit die Abgabe granularer Daten vor.

Zudem sind die Meldepflichten **auf unterschiedlichen Ebenen** geregelt:

Diese Entwicklung hat zur Folge, dass Kreditinstitute mit zahlreichen Meldeformularen konfrontiert sind, die unterschiedliche **Aggregationsebenen** und Meldefrequenzen vorsehen. Das Resultat ist ein zunehmend komplexes System, das für Außenstehende nur noch schwer durchschaubar ist.

Dadurch kommt es zum Teil zur Erhebung und Übermittlung redundanter Informationen, da ähnliche Daten in unterschiedlichen Zusammensetzungen gemeldet werden müssen. Zusätzlich stehen Banken vor der Herausforderung, die Inhalte der einzelnen Meldungen zu validieren und Datenkonsistenz zwischen diesen sicherzustellen. Dies führt zu einer wesentlichen Erhöhung der mit dem Meldewesen verbundenen **Kosten**.

TREND

Im Rahmen eines längerfristigen strategischen Projekts plant das Europäische System der Zentralbanken (ESZB), das Meldewesen im großen Stil europaweit zu harmonisieren und zu vereinfachen.

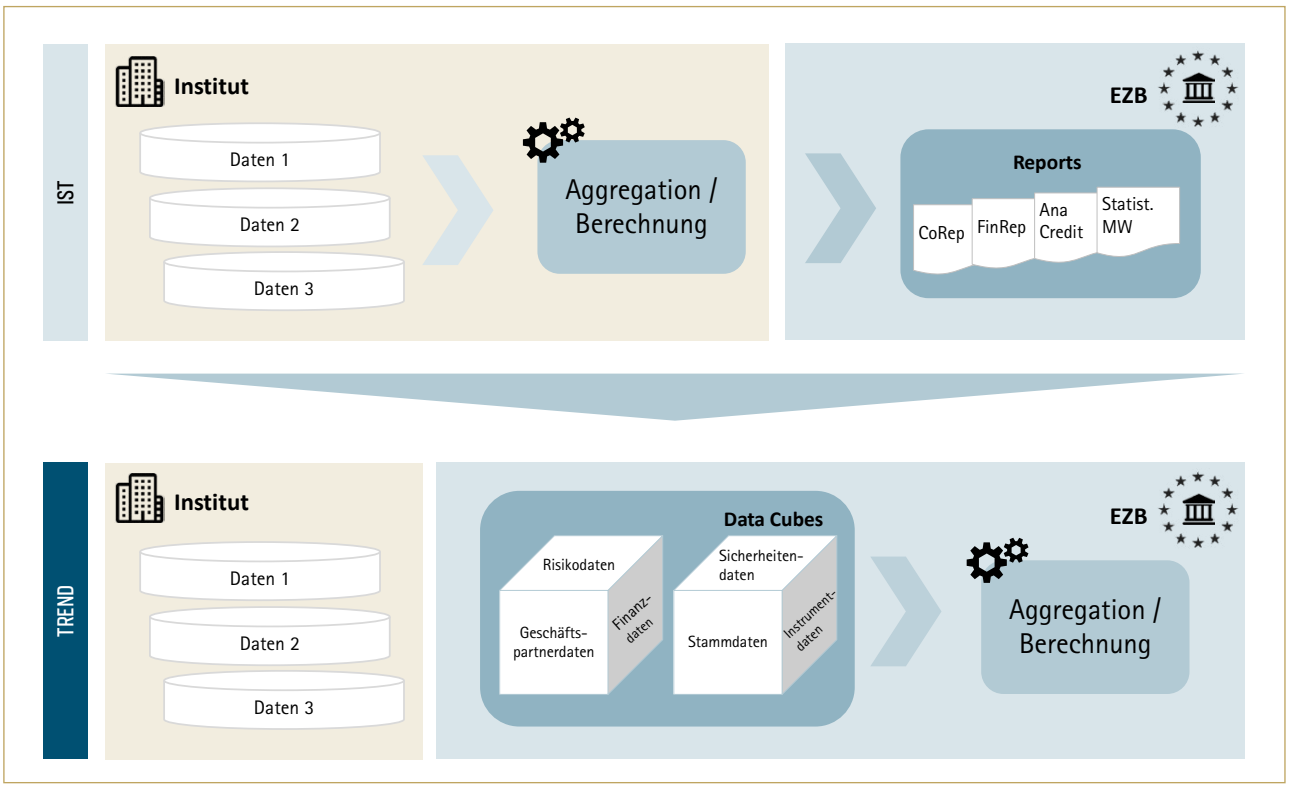
Um dieses Ziel zu erreichen, setzen die Regulatoren verstärkt auf den Ausbau des „**European Reporting Frameworks**" (ERF) (auch „Primary Reporting" oder „Output Layer")[11]. Innerhalb dieses Berichtsrahmens soll die Datenerhebung in einem ersten Schritt für statistische Zwecke und in einem zweiten Schritt zur Erfüllung aufsichtsrechtlicher Anforderungen europaweit zusammengeführt werden. Der Fokus wird dabei auf Einzeldatenübermittlung und die generelle Verringerung des Aggregationsniveaus gelegt. Auf diese Weise sollen inhaltliche Überschneidungen in bisher zu erstellenden Meldungen verringert werden.

[11] European Reporting Framework (ERF): Key facts and information

Als Vorbild für das ERF gilt das bereits seit 2013 etablierte österreichische Berichterstattungssystem, welches wie folgt funktioniert: Die Österreichische Nationalbank (OeNB) definiert ein standardisiertes, vollständiges Datenmodell auf granularer Ebene, auch **Basic Cubes** genannt, in welchem die Banken Mikrodaten zu Einzelgeschäften anliefern. Durch Aggregation und Transformation werden aus diesen Basic Cubes dann sogenannte **Smart Cubes** erstellt, die an die OeNB weitergegeben und von ihr ausgewertet werden. Für die IT-seitige Umsetzung der Strecke zwischen Basic Cubes und Smart Cubes wurde u.a. die Meldewesenplattform „AuRep – Austrian Reporting Services GmbH" [12] gegründet. Sie fungiert als eine Art Zwischenspeicher, wo Daten der österreichischen Banken bei Bedarf (ad hoc bzw. regulär) abgerufen und der Aufsicht bereitgestellt werden können; Service und regulatorische Wartung sind dabei zentralisiert.

Als erste neue Regulierung beinhaltet **AnaCredit**[13] (Analytical Credit Datasets), die im September 2018 in Kraft tretende Meldeanforderung zum Aufbau eines europäischen Kreditregisters, wesentliche Charakteristika des österreichischen Modells und ist damit der erste Schritt in die Richtung eines einheitlichen Meldewesens.

Um die Vereinheitlichung des Meldewesens und die Anwendung von Data Cubes zu vereinfachen, hat die Aufsicht zudem die Initiative **„BIRD – Bank's Integrated Reporting Dictionary"** [14] ins Leben gerufen. Diese beinhaltet ein europaweit harmonisiertes Datenmodell sowie spezifische Transformationsregeln für die Erstellung geltender Meldeanforderungen und wird den Banken kostenfrei als „öffentliches Gut" zur Verfügung gestellt. Die Verwendung der BIRD-Spezifikationen ist allerdings bisher freiwillig.



Quelle: ifb group

[12] Die AuRep ist ein Joint Venture, das auf Anregung der OeNB durch acht Bankengruppen gegründet wurde.

[13] Finale AnaCredit-Verordnung: EZB-VO (EU) 2016/867

[14] Siehe auch: www.banks-integrated-reporting-dictionary.eu/

WIRKUNG

KURZFRISTIG müssen Finanzinstitute mit hohen Kosten und gestiegenem Aufwand zur Umsetzung der neuen Meldeanforderungen, insbesondere zum Aufbau der Data Cubes, rechnen. Über eine längere Übergangsphase werden Daten weiterhin redundant erhoben, sodass sich die Anzahl der Meldungen zunächst erhöht. Zudem sind Investitionen in neue Hard- und Software notwendig, und neues Know-How bzgl. der sich stetig ändernden Meldeanforderungen, aber auch bzgl. Datenhaushalt und IT, muss erworben werden.

LANGFRISTIG gesehen kommt ein europaweit einheitliches Meldewesen sowohl der Aufsicht als auch den Kreditinstituten zu Gute. Die Aufsicht optimiert mithilfe des neuen Systems die Überwachung der Finanzstabilität: Einerseits können Banken besser miteinander verglichen und dementsprechend effizienter überwacht werden, andererseits sollen Risiken innerhalb des europäischen Finanzsystems früher erkannt werden. Auf Seiten der Institute sollte sich der Aufwand für Reportingaufgaben verringern: Durch optimierte Meldeprozesse werden zukünftig relevante Daten auf feingranularer Ebene nur einmal an die Aufsicht geliefert; die weitere Verarbeitung der Daten übernehmen die Aufsichtsbehörden bzw. die EZB. So kann die Fertigungstiefe im Meldewesen auf Seiten der Banken – und damit einhergehend Kosten und Aufwand – langfristig gesenkt werden. Zudem müssen Banken durch die neuen Vorgaben die Automatisierung vorantreiben, die wiederum den steigenden Kosten für IT und Datenbereitstellung entgegenwirkt.

ES BLEIBT FESTZUHALTEN

Ein einheitliches und granulares Meldewesensystem in Europa birgt langfristig Kosteneinsparungspotenziale für Banken und verspricht eine Steigerung der Effizienz. Inwieweit sich diese positiven Vorhersagen bewahrheiten, bleibt allerdings abzuwarten. Kritisch für eine erfolgreiche Vereinheitlichung des Meldewesens ist die verstärkte Automatisierung von Meldeprozessen und damit einhergehend auch die Sicherstellung ausreichender Datenqualität. Zunächst steuern die Banken folglich auf einen „Berg voller Arbeit" und signifikante Investitionen zu.

» TREND 4

STANDARDISIERUNG UND KONSOLIDIERUNG DER IT-ANWENDUNGEN AUF KONZERNEBENE

AUSGANGSLAGE

Banken sind einerseits durch den Niedrigzins, einer schwachen Ertragslage und erhöhten Kapitalkosten **steigendem Margendruck** ausgesetzt. Andererseits steigt die Anzahl **regulatorischer Anforderungen** wie BCBS 239, AnaCredit und IFRS 9, die erfüllt werden müssen.

Um diesem Umfeld gerecht zu werden, müssen Banken tiefgreifende Veränderungen vornehmen. Insbesondere im Bereich der IT-System- und -Prozesslandschaft herrscht teils enormer Nachholbedarf und großes Optimierungspotenzial.

Grund dafür ist, dass Institute oftmals über historisch gewachsene, silo-artige Strukturen in ihrer IT-Systemlandschaft verfügen – nicht nur Tochtergesellschaften und Mutterkonzern, sondern teils sogar bankinterne Fachbereiche arbeiten mit verschiedenen Software-Applikationen oder greifen auf unterschiedliche Datenhaushalte zu. Dies kann zu **Inkonsistenzen** und **Mehraufwand** durch Abstimmung führen. Grundlegende IT-Projekte werden aber häufig vom Vorstand gescheut, da sie sehr kostenintensiv sind und keine unmittelbar sichtbaren Auswirkungen auf die Ertragslage mit sich bringen.

Neue regulatorische Anforderungen wie BCBS 239 zielen darauf ab, die IT-Systemlandschaft der Banken in Bezug auf Finanz- und Risikodaten zu integrieren. Unabhängig davon, ob BCBS 239 anzuwenden ist, sollten sich alle Banken zusätzlich Gedanken machen, inwieweit sie ihre IT-System- und -Prozesslandschaft optimieren können, um auch zukünftig zu bestehen.

TREND

Derzeitige Entwicklungen im Bankensektor zeigen, dass Banken immer mehr den Fokus auf die **Standardisierung und Konsolidierung der IT-Anwendungen** auf Einzelinstituts- sowie Konzernebene legen.

Dies beinhaltet u. a. die Einführung eines konzernübergreifenden IT-Zielbildes, die Nutzung eines einheitlichen Kernbankensystems und weiterer Anwendungen (Bestandssysteme, Meldewesentools, BI-Lösungen) sowie die Schaffung eines integrierten Datenhaushalts in Kombination mit einem konzernweit einheitlichen Datenmodell.

Damit die Vorteile eines integrierten Datenhaushalts vollumfänglich genutzt werden können, wird der Aufbau eines umfangreichenden Data-Governance-Rahmenwerks sowie die Durchführung eines effektiven Datenqualitätsmanagements immer wichtiger.

Zudem kommt dem Zusammenspiel zwischen Mutter- und Tochterunternehmen immer mehr eine tragende Rolle zu, um die Standardisierung und Konsolidierung der IT-Anwendungen zu bewerkstelligen.

INTEGRIERTER DATENHAUSHALT (ID)

Die Definition eines gut durchdachten **Integrierten Datenhaushalts (IDs)** ist unabdingbar. Dieser dient als „golden Source" für das Risikomanagement sowie für jegliche finanzielle-, aufsichtsrechtliche-, und steuerungsrelevante Berichterstattung. Grundvoraussetzung für den Aufbau eines solchen IDs ist das erfolgreiche Zusammenspiel dreier Faktoren:

- Organisation (in Bezug auf Zielvorgaben und Change Management)
- Fachabteilungen (in Bezug auf Fachprozesse und Datenanforderung)
- IT (in Bezug auf IT-Systeme und -Architektur)

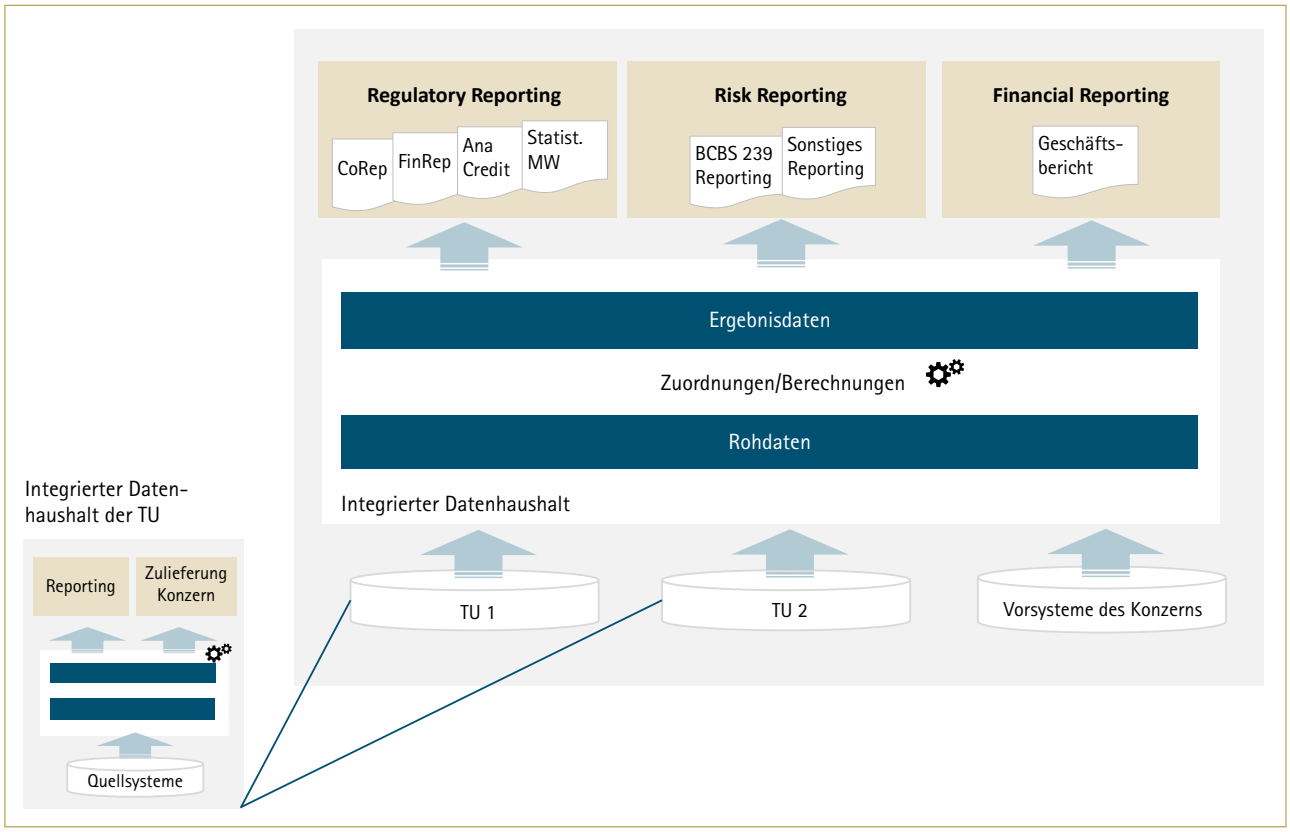
Beim Aufbau des IDs sollte wie folgt vorgegangen werden: Zunächst muss innerhalb der Organisation ein **einheitliches Zielbild** für die erwünschte Systemlandschaft beschlossen und vorangetrieben werden. Dies beinhaltet zum einen, einen hohen Abstimmungsgrad in Bezug auf die „Bedürfnisse" der unterschiedlichen Abteilungen innerhalb des Institutes zu erreichen; zum anderen ist die Bereitstellung adäquater finanzieller und personeller Ressourcen sicherzustellen.

Als nächstes gilt es, ein vollumfängliches **fachliches Datenmodell** zu entwickeln, welches die Datenanforderungen einzelner Berichte und Meldungen widerspiegelt. Das Datenmodell muss zusätzlich um Metadatendefinitionen und Taxonomien erweitert werden, damit konzernweit ein einheitliches Verständnis der erforderlichen Kennzahlen und Merkmale herrscht. Diese sind in einem Glossar zu dokumentieren, sodass Transparenz und Konsistenz innerhalb des Konzerns herrschen. In großen Konzernen ist ein **Top-Down-Ansatz** empfehlenswert, d.h. ausgehend von den Berichten und Kennzahlen wird definiert, welche Daten aus den Quellsystemen und von einzelnen Tochterunternehmen (TU) benötigt werden. Das daraus resultierende Datenmodell wird dann auf die einzelnen TU übertragen, sodass diese ihre Daten, die zur Befüllung der Risikoberichte und aufsichtsrechtlichen Meldungen benötigt werden, angemessen zuliefern können. Sobald das initiale Datenmodell umgesetzt ist, kann es **sukzessive**, um zusätzliche Datenanforderungen wie Profit Center **erweitert** werden.

Die Befüllung des konzernweiten IDs erfolgt mit **granularen Daten** (d.h. auf Einzelgeschäftsebene) aus den bestehenden operativen Systemen sowie aus den einzelnen IDs der TU. Dies erfordert die Anbindung sämtlicher Bestandssysteme an den ID – also auch die Anbindung von Systemen, welche innerhalb der Fachbereiche zur Datenverarbeitung und Erstellung einzelner Berichte genutzt werden. Zudem ist die **Überführung der wesentlichen individuellen Datenverarbeitungen** (IDVs) in **operative Datenverarbeitungen** (ODVs) sowie deren Anbindung an den ID der Muttergesellschaft/der einzelnen TU anzustreben. Hierdurch könnte der manuelle Aufwand der Datenbereitstellung reduziert und die Frequenz der Datenanlieferung erhöht werden.

SPEZIFISCHE ANFORDERUNGEN AN DIE TOCHTERUNTERNEHMEN

Um eine Konsolidierung zu erleichtern und eine Standardisierung herbeizuführen, sollte sich die Daten- und IT-Architektur der Tochterunternehmen in das Zielbild des Konzerns einfügen.
Konkret heißt das: Um eine Überführbarkeit der Daten sicherzustellen, sollte das fachliche Datenmodell des Konzerns sowie die Ermittlungsweise der wesentlichen Risikokennzahlen (sofern relevant) von den TUs übernommen werden. Die Systemlandschaft der einzelnen TU sollte sich daher an der Systemlandschaft des Konzerns orientieren. Bestenfalls werden schon auf TU-Ebene – basierend auf den fachlichen Vorgaben des Konzerns – einzelne, eigenständige IDs erstellt. Diese werden an den konzernweiten ID angebunden und versorgen ihn mit den Daten der TU.



Quelle: ifb group

KONZERNWEITE DATA GOVERNANCE

Das Bestehen eines integrierten Datenhaushalts setzt zudem voraus, dass Vorgaben zum Datenmanagement und einheitliche Qualitätsansprüche existieren. Das heißt, Data Governance muss konzernweit erfolgen. Erleichtert wird dies z. B. durch **Data Lineage**. Darunter versteht man die Möglichkeit, für aggregierte Kennzahlen die Herkunft sowie Abhängigkeiten zwischen den Datenattributen zu bestimmen. Die durch Data Lineage erhöhte Transparenz des Datenstroms ist eine Grundvoraussetzung für ein konzernweites Data-Governance-Rahmenwerk.

Außerdem sollte die Umsetzung eines konzernweiten Datenmodells durch die Einführung eines ganzheitlichen, mehrstufigen **Data Quality (DQ) Regelwerks** begleitet werden. Neben der Definition von Datenqualitätsanforderungen sollte ein derartiges Werk auch den Anstoß von Korrekturprozessen vorsehen. Zuletzt muss sichergestellt werden, dass **Datenkorrekturen** ausschließlich in den operativen Systemen (in Ausnahmefällen auch im ID) erfolgen.

WIRKUNG

KURZFRISTIG gilt sich nichts vorzumachen: Auch wenn Vorreiterinstitute durch eine frühzeitige Umsetzung genannter Maßnahmen einen Wettbewerbsvorteil generieren können, sind zunächst hohe Kosten und Mehraufwand durch die zu tätigenden IT-Investitionen zu erwarten. Die Erhöhung der Datengranularität zur Erfüllung regulatorischer Anforderungen ist notwendig und wird durch die Standardisierung und Konsolidierung der IT-Systemlandschaft unterstützt.

LANGFRISTIG hingegen sind die Auswirkungen der Standardisierung und Konsolidierung vielversprechend: Durch weniger Doppelarbeiten und eine engere Zusammenarbeit zwischen Mutter- und Tochterunternehmen kann die Effizienz (z. B. in Bezug auf den Testaufwand) gesteigert werden. Redundanzen (wie z. B. überflüssige Schnittstellen) können vermieden und Kosten durch geringeren Abstimmungsaufwand gesenkt werden. Außerdem sollte Konsistenz leichter herzustellen sein, sodass Vergleichbarkeit und Abstimmbarkeit von Risiko-, Accounting- sowie Meldewesendaten verbessert werden. Dies impliziert eine schnellere, transparente und flexible Berichterstattung. Zudem sollte sich die Datenqualität erheblich verbessern – durch das einheitliche fachliche Datenmodell und DQ-Regelwerk werden die technische und fachliche Vollständigkeit und Richtigkeit der Daten erreicht.

ES GILT ALSO

Die derzeitigen Herausforderungen und Änderungen im Bankenumfeld bieten den Banken die einmalige Chance, Optimierung und Überholung der teilweise stark fragmentierten IT-Landschaft anzugehen. So können wichtige Effizienzverbesserungen und Kostensenkungen langfristig gesehen realisiert werden. Dafür ist auf kurze Sicht allerdings ein hoher Investitionsaufwand notwendig. Nichtsdestotrotz sollten Banken hier strategisch vorgehen und ein ganzheitliches, auf die nachhaltige Ertragsentwicklung fokussiertes Konzept entwickeln – sogenanntes „Stückwerk" ist wenig hilfreich.

Ihre Ansprechpartnerin:

Juliana Müller
Director
M: +49 178 2448636
juliana.mueller@ifb-group.com

Autoren:

Philipp Enzinger
Senior Consultant

Marcel Knodt
Senior Consultant

Juliana Müller
Director

ifb AG
Schloßstraße 23
82031 Grünwald
Tel. +49 89 69989437-0
info@ifb-group.com