



cutting through complexity

Basel Committee on Banking Supervision: „Principles for effective risk data aggregation and risk reporting“ (BCBS 239)

Neue Anforderungen an IT-Architektur
und Data-Governance im Risikobereich
von Banken

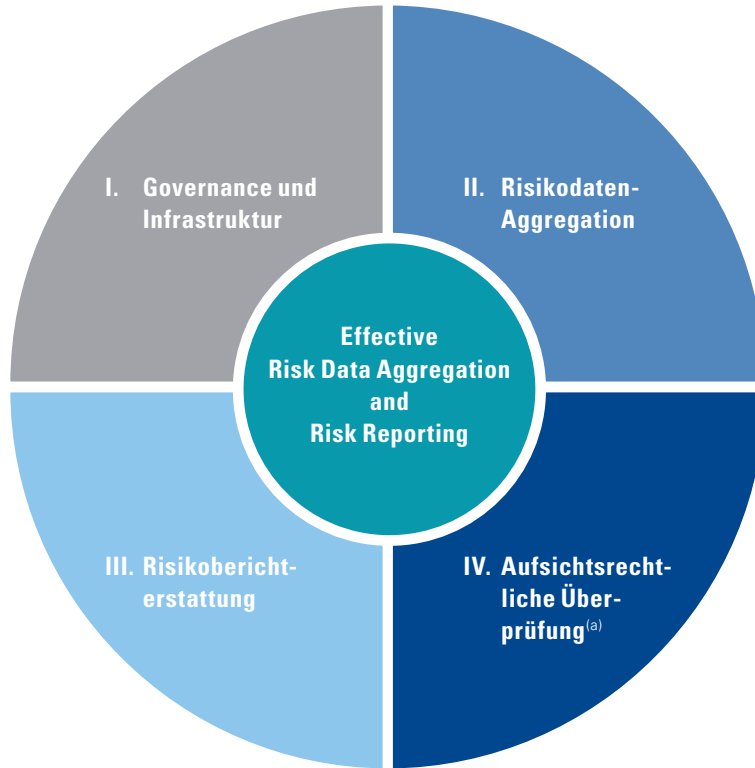


Konkrete Vorgaben für IT-Systeme und Data-Governance von Kreditinstituten

Im Januar 2013 hat das Basel Committee on Banking Supervision die „Principles for effective risk data aggregation and risk reporting“ (BCBS 239) veröffentlicht. Das prinzipienbasierte Papier soll national in eine Aktualisierung der MaRisk münden und entsprechend der Größe und dem Geschäftsmodell einer Bank ausgelegt werden. Damit möchte der Regulator die Fähigkeiten von Banken weiter absichern, ihre gruppenweiten Risiken zu identifizieren und zu managen. Die vollständige Anwendung der Grundsätze wird für global und national systemrelevante Banken ab 1. Januar 2016 verpflichtend; die neuen Regelungen müssen bis zu diesem Termin umgesetzt sein. Die Anwendung auf weitere Kreditinstitute obliegt den nationalen Aufsehern und ist derzeit im Standard noch nicht näher spezifiziert – die Bundesbank verweist auf eine proportionale Anwendung der Anforderungen.

Der Regulator verfolgt das Ziel, die Datenhaltung sowie die Reportingsysteme – als wesentliche Voraussetzungen für ein funktionierendes Risikomanagement – zu verbessern. Damit liegen erstmals konkrete regulatorische Anforderungen an die IT-Architektur und das Datenmanagement in Banken vor, die eine übergreifende Sicht über die Daten und Prozesse gewährleisten sollen. Neben den umfangreichen IT-Implikationen wird die neue Regelung auch wesentliche Auswirkungen auf die Aufbau- und Ablauforganisation der gesamten Risikofunktion in Banken haben. Das bedeutet: Banken müssen deutlich höhere Standards hinsichtlich der Qualität und Konsistenz ihrer Risikodaten sowie bezüglich der Geschwindigkeit und Flexibilität ihres Reportings setzen. Darüber hinaus sollte die Verantwortung für die Einhaltung aller Standards auf Vorstandsebene angesiedelt sein.

Die Themenbereiche der Regelung BCBS 239 im Überblick



(a) Der Themenbereich IV „Aufsichtsrechtliche Überprüfung“ beinhaltet im Unterschied zu den drei anderen Themenbereichen keine Anforderungen an Banken, sondern Empfehlungen an die nationalen Aufseher.

© 2013 KPMG, Deutschland



Anforderungen an die Kreditinstitute:

- Datenqualität liegt in der Verantwortung von Vorstand und Senior Management, denen die Grenzen des Risikoreportings vollständig bewusst sind
- Ziel sind korrekte Risikodaten unabhängig von organisatorischen Grenzen (Geschäftseinheiten, Jurisdiktionen und Ähnliches)
- Sicherstellung der effektiven IT-Unterstützung der Risikodaten-Aggregation und des Reportings – auch in Krisen- und Stresszeiten



Anforderungen an die Kreditinstitute:

- Zeitnahe Erstellung und Verteilung validierter Risikoberichte
- Integration aller materiellen Risikofelder
- Verständlichkeit des Risikoreportings für Adressaten
- Transparente Darstellung der Schwachstellen und Grenzen des Risikoreportings, sodass diese bei Entscheidungen mitberücksichtigt werden können



Anforderungen an die Kreditinstitute:

- Fähigkeit zur Generierung von korrekten und vollständigen Risikodaten
- Weitgehend automatisierte Generierung der Risikodaten zur Fehlerreduktion
- Sicherstellung einer zeitnahen Risikodaten-Aggregation
- Flexibilität und Skalierbarkeit der Risikodaten-Aggregation im Hinblick auf Ad-hoc-Reporting und aufsichtsrechtliche Anforderungen (insbesondere in Krisenszenarien)



Empfehlungen an die nationale Aufsicht:

- Überprüfung und Überwachung der Einhaltung der Grundsätze durch die nationale Aufsicht
- Empfehlungen zum Einsatz geeigneter Werkzeuge für die Reviews und zu Sanktionsmaßnahmen der Aufsicht (beispielsweise die Möglichkeit, im Fall von Bedenken das Größenwachstum zu beschränken)
- Grenzüberschreitende Zusammenarbeit der Aufseher

Die neuen Regelungen des BCBS 239 „Principles for effective risk data aggregation and risk reporting“ stellen an Kreditinstitute in vier unterschiedlichen Handlungsfeldern vielfältige Anforderungen.

IT-Architektur

- Konzernweite Überführbarkeit der Risikodatenmodelle mit vereinheitlichten Namenskonventionen
- Konzernweit einheitlicher Detaillierungsgrad der Daten, um ein flexibles Reporting zu ermöglichen
- Abstimmbarkeit von Risiko- und Accountingdaten
- Konzernweit hohe Automatisierung in der Risikodaten-Aggregation, manuelle Prozesse nur als Ausnahme
- Anstreben einer „Single Source“ für Risikodaten je Risikoart

Data Quality Framework

- Leistungsfähiges Datenqualitätsmanagement mit automatischen Messverfahren und Eskalationsprozeduren
- Umfassende Data-Governance für Risikodaten mit Data-Ownern in Business und IT

- Dokumentation von Reporting- und Abstimmungsprozessen
- Integration maschineller und manueller Qualitätskontrollen in den Berichtsprozess

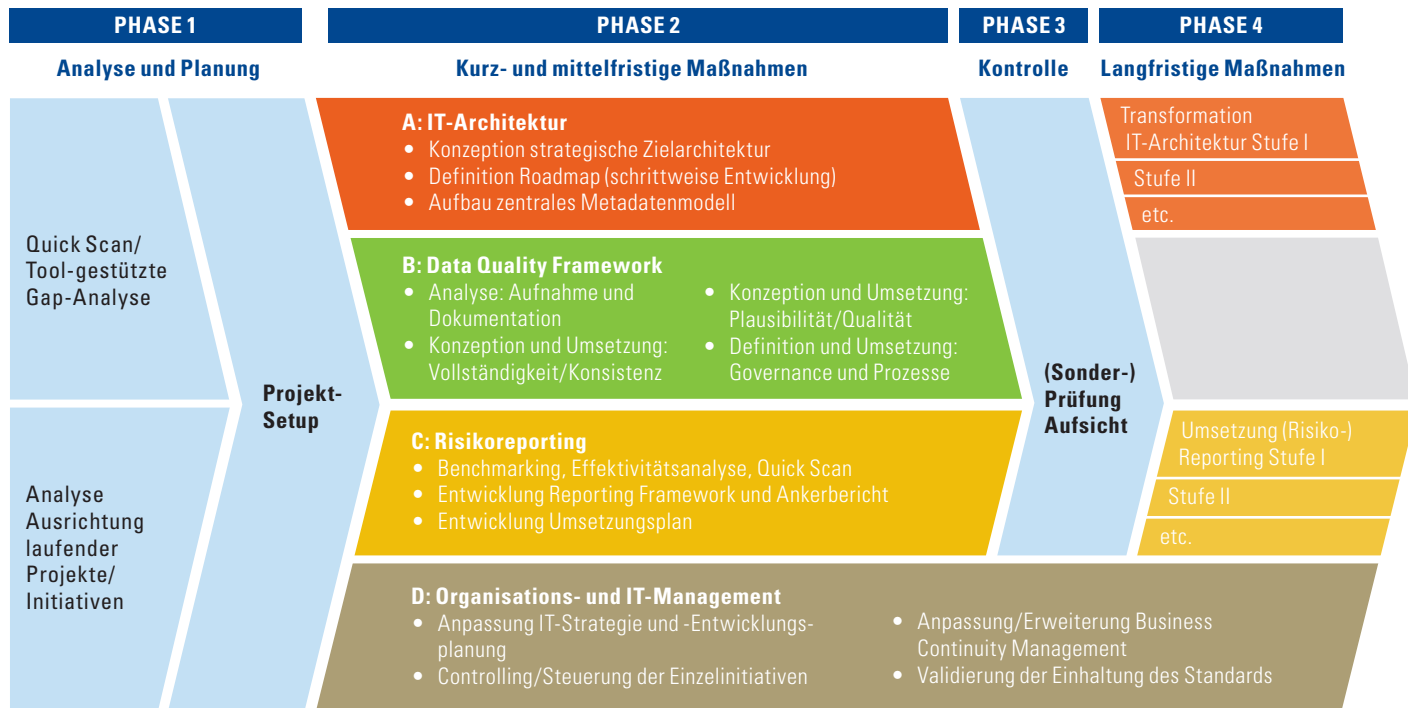
Risikoreporting

- Simulations- und Frühwarnmechanismen sowie zeitnahe und flexible Reporting- und Analysemöglichkeiten
- Inhaltlich vollumfängliches und qualitativ geeignetes Risikoreporting

Organisations- und IT-Management

- Klare Abbildung in der IT-Strategie und Entwicklungsplanung
- Unabhängige Validierung der Einhaltung des Standards
- Verankerung im Business Continuity Management

Modulares Vorgehensmodell zur Erfüllung der Anforderungen gemäß BCBS 239



Aufgrund der unterschiedlichen Ausgangssituation der einzelnen Kreditinstitute empfehlen wir auf Basis unserer Praxiserfahrungen einen modularen Projektansatz mit folgenden kurz- und mittelfristigen Maßnahmen für die einzelnen Handlungsfelder.

IT-Architektur

- Konzeption der strategischen Zielarchitektur
- Definition einer Roadmap
- Aufbau eines zentralen Metadatenmodells

Data Quality Framework

- Analyse, Konzeption und Umsetzung eines automatisierten Messverfahrens
- Definition und Umsetzung eines Governance-Modells mit klaren Rollenverantwortlichkeiten und Prozessen

Risikoreporting

- Benchmarking, Effektivitätsanalyse und Quick Scan
- Entwicklung eines Reporting Frameworks und Ankerberichts

Organisations- und IT-Management

- Anpassung von IT-Strategie und Entwicklungsplanung
- Aufsetzen der unabhängigen Validierung
- Einbettung in das Business Continuity Management
- Controlling und Steuerung der Projekte zur Erfüllung der Standardkonformität

Dabei bieten wir als ersten Schritt die Identifikation und Strukturierung aller relevanten Handlungsfelder im Rahmen eines Quick Scans.

Sprechen Sie uns an!

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Dr. Peter Stork

Partner, Information Technology
T +49 69 9587-3130
pstork@kpmg.com

Marco Lenhardt

Partner, Regulatory & Compliance
T +49 69 9587-3403
mlenhardt@kpmg.com

www.kpmg.de

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2013 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Germany. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.