BCG

The Boston Consulting Group

Risikosteuerung in Zeiten von BCBS 239

Der richtige Weg zur zeitgerechten IT-Umsetzung aller regulatorischen und marktgetriebenen Fachanforderungen

Ein praxisnaher Vorschlag

Walter Bohmayr, Björn Brings, Jörg Erlebach und Ulrik Lackschewitz

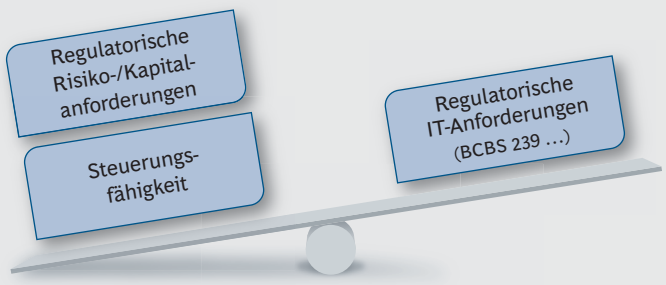
Mai 2014

ZUSAMMENFASSUNG

Banken stehen aufgrund der ungewöhnlich hohen Marktvolatilität und der im Zuge der Finanzmarktkrise wachsenden Anzahl neuer regulatorischer Anforderungen und Ad-hoc-Anfragen verschiedener Stakeholder[1] vor einer enormen Herausforderung: Zur Sicherstellung zeitgerechter Reaktionsfähigkeit und der Konsistenz der vorhandenen Daten müssen sie eine zentrale IT-Architektur schaffen. Diese muss zum einen flexibel und leistungsfähig genug sein, um den enormen Änderungsgeschwindigkeiten Rechnung zu tragen; zum anderen muss sie alle Anforderungen erfüllen, die einen sicheren Betrieb auch während der laufenden Weiterentwicklung gewährleisten. In der Folge stehen Banken zunehmend vor dem Zielkonflikt, die erforderlichen Anpassungen und Sonderauswertungen entweder innerhalb der bestehenden prozessbewährten IT-Infrastruktur oder auf anderen, flexibleren Wegen mittels Workarounds durchzuführen. Ein wesentliches Entscheidungskriterium ist dabei die "Time-to-Market", d. h. die zur Umsetzung benötigte Zeit.

Ein Plädoyer zum Primat der Steuerungsfähigkeit und der Liefertreue gegenüber den Stakeholdern vor der ubiquitären Einhaltung aller IT-Richtlinien.

Abbildung 1 | Abwägung verschiedener Anforderungen an die Risikosteuerung



Quelle: BCG-Analyse

Aktuelle IT-Umsetzung in den Banken häufig sehr zeitaufwändig

Die IT-Umsetzung neuer regulatorischer Anforderungen erfolgt in den meisten deutschen Banken nach dem Wasserfallprinzip[2], d. h. in einer prozessual klar definierten Aufgabentrennung zwischen den Fachbereichen und dem IT-Bereich. Neben dem Ziel der organisatorischen Trennung sind oft fehlende IT-Kompetenz in den Fachbereichen sowie mangelnde Fachexpertise in der IT zu berücksichtigen. Gerade im Risikobereich mit seiner analytischen Zugangsweise werden zunehmend aber auch Fachkollegen eingesetzt, die ausgeprägte IT-Expertise aufweisen müssen.

Gemäß dieser "traditionellen" Aufgabentrennung zwischen den Fachbereichen und IT werden zuerst die neuen regulatorischen Anforderungen von dem jeweiligen Fachbereich zu einem institutsspezifischen Anforderungsdokument aufbereitet. Im nächsten Schritt wird dieses mit dem IT-Bereich besprochen und in ein ausführliches Fachkonzept überführt. Dies ist die Basis für das durch die IT erstellte IT-Konzept, welches wiederum durch den Fachbereich geprüft wird. Nach Abschluss der technischen Konzeption wird das IT-Konzept durch die IT umgesetzt. Der Fachbereich entwickelt währenddessen Testfälle und führt diese nach Fertigstellung der IT-Anwendung in einer Testumgebung aus. Nach erfolgreicher Prüfung werden die Änderungen schließlich vom Fachbereich freigegeben. Gleichzeitig dokumentieren Fach- und IT-Bereich jeweils die einzelnen Prozessschritte bzw. deren Umsetzung.

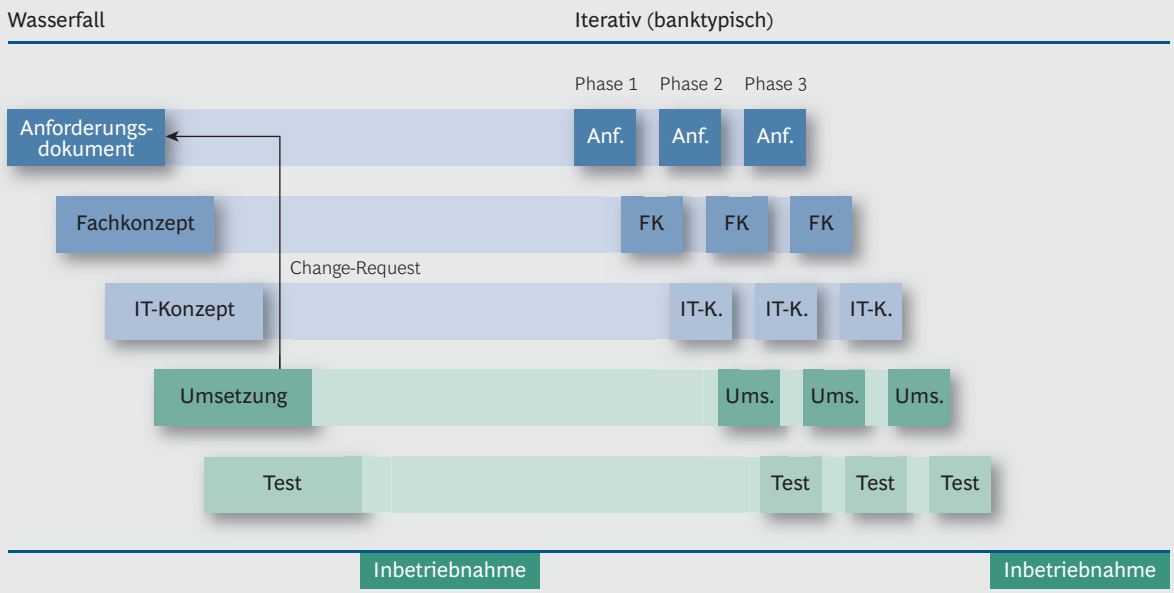
Die Realität zeigt, dass beim Test durch die Fachbereiche häufig fehlende oder nicht korrekt spezifizierte Funktionalitäten auffallen. Als Resultat erfolgt ein sogenannter "Change-Request", infolge dessen der Prozess nochmals, wenn auch in kürzerer Form, durchgeführt werden muss. Der gesamte Prozess erstreckt sich in der Praxis auf Zeiträume von sechs bis zwölf Monaten.

"Agilere" Vorgehensmodelle adressieren diese Unzulänglichkeiten dahingehend, dass die Schritte von der Fachkonzeption bis zur Umsetzung nicht auf einmal mit einer großen Änderung vollzogen werden, sondern iterativ in mehreren kleinen Änderungen stattfinden und somit den Softwareentwicklungsprozess flexibler und schlanker gestalten (eine solche Vorgehensweise wird durch verschiedene Modelle, wie z. B. Scrum[3], unterstützt). Diese iterative Herangehensweise hat jedoch den Nachteil, dass sie regelmäßige technische Inbetriebnahmen ("Deployments") erfordert. Da es in großen Organisationen meist nur wenige feste Deployment-Termine, etwa zur Anpassung von Schnittstellen oder Softwareupdates, gibt, werden solche Konzepte oft wieder "ausgebremst", sodass der effektive Zeitgewinn nur 10 bis 20 % beträgt. Die erhöhte Erfolgswahrscheinlichkeit für Projekte schlägt jedoch bei stringenter Anwendung des agilen Ansatzes positiv zu Buche.

Steigende Anzahl regulatorischer und marktgetriebener Anforderungen

Die Innovationszyklen der Regulatoren haben sich in der Banken- und Finanzmarktbranche infolge schwieriger und volatiler Marktsituationen in den letzten Jahren deutlich verkürzt. Während es 2009 pro Arbeitstag weltweit "nur" ca. 40 regulatorische Änderungen gab, sind es heute rund 100. Zwischen 2009 und 2013 hat sich also die Anzahl regulatorischer Anforderungen mehr als verdoppelt.

Abbildung 2 | Vergleich von Wasserfall und iterativer Umsetzung



Quelle: BCG-Analyse

Außerdem kämpfen viele Banken mit der parallelen Lösung diverser "Findings" zu bereits umgesetzten regulatorischen Anforderungen. Dafür steht häufig nur ein Umsetzungszeitraum von einem Jahr zur Verfügung. Neue regulatorische Maßnahmen müssen aufgrund absehbar knapper Deadlines und der notwendigen Umsetzungsdauer häufig zu einem Zeitpunkt spezifiziert werden, zu dem die umzusetzenden Regularien noch gar nicht endgültig feststehen. Ein größerer nachträglicher Änderungsaufwand ist daher bereits vorherzusehen.

Hohe Reaktionsgeschwindigkeit durch Vielzahl an Marktänderungen erforderlich

Eine wesentliche Ursache für die steigenden regulatorischen Änderungen ist eine im Vergleich mit den Jahren, aus denen die hierfür vorgesehenen bankinternen Prozesse und Strukturen stammen, ungeahnte und deutlich gestiegene Marktvolatilität, deren Steuerung die Institute vor erhebliche Herausforderungen gestellt hat und weiter stellen wird. Dabei wurden viele bisher unterstellte Paradigmen in der Markt- und Risikoanalyse widerlegt. Beispielsweise zeigen der Zahlungsausfall bei griechischen Staatsanleihen, die Pleite von Lehman Brothers oder die Auswirkungen der Fukushima-Katastrophe, dass kurzfristig verfügbare Analysen für die Steuerung jedes Instituts unabdingbar sind. Für Institute, die kein entsprechendes Instrumentarium zur Verfügung hatten und somit auf die Steuerung ihrer Risiken nicht adäquat vorbereitet waren, hatten diese "Stressfälle" erhebliche, manchmal existenzvernichtende Auswirkungen.

Deutlich gestiegene Marktvolatilität stellt Institute vor erhebliche Herausforderungen.

Verschärfung regulatorischer Anforderungen an die Umsetzung

Zusätzlich verschärft werden die Umsetzung regulatorischer Maßnahmen und die notwendige Anpassung der Steuerung durch das im Januar 2013 veröffentlichte BCBS-Paper 239 "Principles for Effective Risk Data Aggregation and Risk Reporting" des Basel Committee on Banking Supervision. Dieses definiert über das bisherige Maß hinausgehende regulatorische Anforderungen an die Datenverarbeitung und das Reporting innerhalb des Risikomanagements. Gefordert werden flexible Analysen (Principle 2 und 6) auf Basis automatisierter verarbeiteter Daten aus einer einzigen Datenquelle ("Single Point of Truth", Principle 3), welche vollständig und in ausreichender Granularität (Principle 4) innerhalb kürzester Zeit (Principle 5) vorliegen müssen.

Aktuelle Umsetzung erfolgt oft auch auf Basis von IDV-Systemen[4] im Fachbereich

Nahezu alle Banken sind von dem in BCBS 239 formulierten Zielbild noch weit entfernt, denn um den fachlichen Ansprüchen und Marktgegebenheiten gerecht zu werden, haben sich in den meisten Banken die Fachbereiche mittels IDV eine "Schatten-IT" aufgebaut. Es existieren also oftmals größere IDV-Systeme auf Basis von Excel oder Access, die sich aus verschiedenen bestandsführenden oder weiterverarbeitenden Systemen speisen. Die Verwaltung dieser Schatten-IT obliegt zumeist demjenigen Fachbereich, der sie entwickelt hat, und existiert neben den von der IT verwalteten Systemen. Dadurch entsteht ein hohes operationelles Risiko, da diese IDV-Systeme meist nicht ausreichend abgegrenzt und dokumentiert sind sowie nur schwer zentral erfasst und geprüft werden können. Häufig liegen die IDV-Systeme ohne adäquate Absicherung und Backups auf lokalen Rechnern in der Hoheit einzelner Mitarbeiter, nicht selten nur einer einzigen Person, die sie auch als Einzige wirklich warten kann. Da Ergebnisse dieser Systeme oftmals direkt über offizielle Reports oder indirekt durch Weiterverarbeitung in die Steuerung und

Banken brauchen IDV-Systeme, um fachliche Herausforderungen zu bewältigen.

Risikomessung eingehen, kann es im schlimmsten Fall zu einer inkonsistenten oder fehlerhaften Information verschiedener Stakeholder kommen.

IDV-Fortbestand nicht mit BCBS 239 vereinbar.

Der Fortbestand solcher IDV-"Notlösungen" ist mit BCBS 239 nicht vereinbar. Eine Abschaffung dieser IDV-Systeme bzw. ihre vollständig IT-konforme Implementierung in die zentrale Standardsoftware, sofern diese überhaupt in der benötigten Form am Markt existiert, ist aber aufgrund des Umfangs für Banken kaum bis zum Inkrafttreten zu bewältigen. Insbesondere die Flexibilität von IDV-Systemen, die es erlauben, auf Marktanforderungen schnell und somit rechtzeitig reagieren zu können, ist mit der aktuell in Banken vorhandenen Standardsoftware nicht erreichbar. Weiterhin würde während der Umstellung das Frühwarnsystem für Marktveränderungen verloren gehen, da die IDV-Systeme in dieser Phase nur schwer gewartet oder angepasst werden könnten. Nicht zuletzt würde die Umstellung viele IT-Ressourcen binden, sodass andere regulatorische Umsetzungen ausgesetzt werden müssten oder sich stark verzögern würden.

Zielkonflikt zwischen Umsetzungsgeschwindigkeit und Einhaltung von Richtlinien

Die Banken stehen daher vor dem Zielkonflikt, entweder nur

1. die Sicherstellung einer marktgerechten Steuerung und einer zeitgerechten Umsetzung aller regulatorischen Fachanforderungen, gegebenenfalls auch unter Verletzung der Prinzipien aus BCBS 239 und anderer IT-Richtlinien,

   oder

2. die Umsetzung der Anforderungen gemäß den IT-Richtlinien und die Umstellung aller IDV-Systeme gemäß den Prinzipien aus BCBS 239 unter Verlust der Reaktionsgeschwindigkeit im Stressfall und unter Verletzung der vom Regulator auferlegten Zeitfristen

zu erreichen.

Auflösung des Zielkonflikts durch ein "Risk-Labor"

Eine mögliche Lösung für diesen Zielkonflikt ist ein mehrstufiges Vorgehen im Umgang mit diesem Dilemma:

Mögliche Lösung: Separates "Risk-Labor" mit eigenen Regeln.

- Im genannten Zielkonflikt ist die Entscheidung für die erste Lösung aus der Perspektive der Bank zwingend, da es für die Profitabilität bis hin zum Überleben des Instituts entscheidend ist, rechtzeitig und richtig reagieren zu können.

  Weiterhin legen nicht nur der Regulator, sondern auch die Kunden und der Kapitalmarkt großen Wert auf ein zeitgerechtes Reporting von (insbesondere neuen) regulatorischen Kennzahlen. Ein verspätetes bzw. nicht sachgerechtes Berichtswesen hat deutliche negative Auswirkungen.

  Auch ergibt sich aus den MaRisk[5], den Mindestanforderungen an das Risikomanagement, dass die Systeme schnell und reagibel angepasst werden können müssen. Für alle genannten Punkte ist die Geschäftsführung haftbar, seit der 2013 erfolgten Anpassung des § 54 a KWG-E auch persönlich.

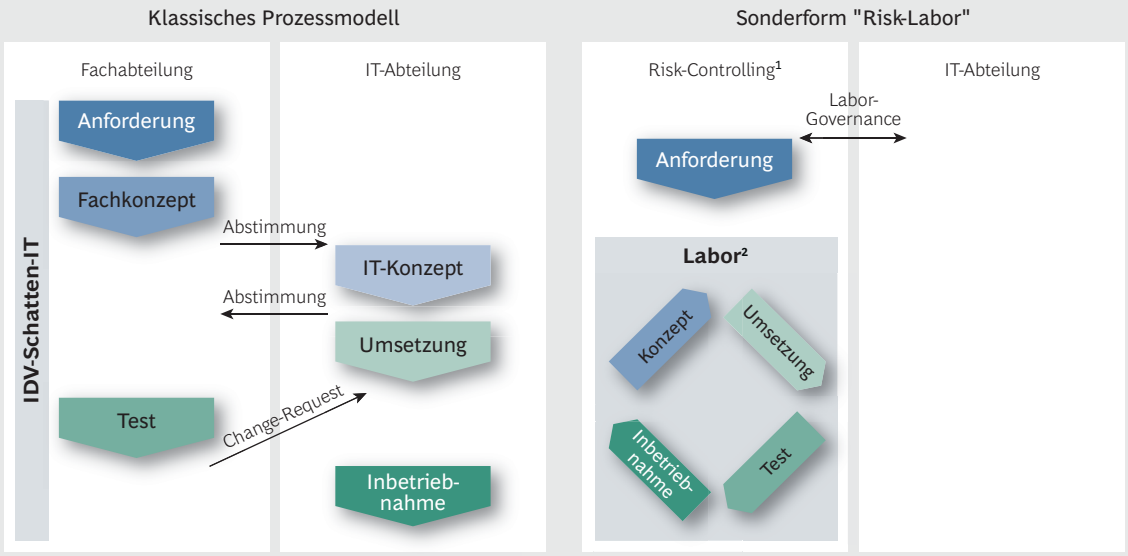
- Es ist wichtig, die Entscheidung für Lösung 1 mit der Aufsicht abzustimmen, denn von ihr sind bezüglich der IT-technischen Umsetzung und nicht zuletzt im Umgang mit den Anforderungen des BCBS 239 praxisnahe Zugeständnisse notwendig.

- Der Aufsicht sollte hierzu vorgeschlagen werden, nicht gänzlich von einschlägigen IT-Richtlinien abzuweichen, sondern Sonderregelungen für ein sogenanntes "Risk-Labor" zu akzeptieren.

- Insbesondere ist bereits zu diesem Zeitpunkt zu definieren, anhand welcher Kriterien eine Überführung des Risk-Labors in den operativen Regelbetrieb erfolgen soll bzw. muss. Es empfiehlt sich auch, die Überleitungsregeln bereits dann zu definieren. Haben sich Teile des Risk-Labors (z. B. spezielle Ratingmodelle) etabliert und können in den produktiven Betrieb überführt werden, so ist natürlich sicherzustellen, dass die ausgesetzten Vorschriften nachträglich durch Nachholung von Entwicklung, Test und Dokumentation erfüllt werden.

- In diesem Risk-Labor wird in einem klar abgegrenzten und vom Risiko-Fachbereich verantworteten Bereich an Kopien produktiver Systeme oder an Neuentwicklungen gearbeitet. Die sonst üblichen Dokumentations-, Entwicklungs- und Testvorschriften werden hier auf ein Mindestmaß reduziert. Hierzu muss sichergestellt sein, dass Ergebnisse dieser Systeme innerhalb des Risk-Labors verbleiben und nicht automatisiert berichtet werden. Bei den erzeugten Berichten muss klar gekennzeichnet sein, dass diese im Risk-Labor entstanden sind.

ABBILDUNG 3 | Umsetzung des "Risk-Labors" im Vergleich zum klassischen Prozessmodell



Quelle: BCG-Analyse
[1]Für klar definierte Themenkomplexe
[2]Auf klar definierter BCBS-konformer technischer Architektur

EXKURS
Beispielhafte Anpassung der Vorschriften in einem "Risk-Labor"

Abgrenzung: Der Themenbereich, der im Risk-Labor umgesetzt werden darf, muss explizit durch den Vorstand freigegeben werden. Die Verantwortung der IT beschränkt sich auf die Bereitstellung der Infrastruktur. Die weitere Verantwortung, auch die der Umsetzung, liegt allein im Fachbereich.

Dokumentation: Die Fachanforderungen fließen direkt in die Umsetzung ein. Der Code wird detailliert kommentiert und stellt im Ergebnis sowohl die Fach- als auch die IT-Spezifikation dar. Der Aufwand für eine weitere Umsetzungsspezifikation und zusätzliche Abstimmungszyklen entfällt.

Entwicklung: Die genutzte Technik und Architektur müssen klar geregelt sein (z. B. Oracle-Datenbank, Java). Der Code muss so entwickelt werden, dass er für den abgegrenzten Aufgabenbereich passend ist. Hierzu dürfen auch Entwicklungsvorgaben umgangen werden, wenn dies durch den Aufgabenbereich zu rechtfertigen ist (z. B. hinsichtlich Erweiterbarkeit und Performance).

Test/Freigabe: Es muss ein automatisierter Prozess (Unit-Testing) durchlaufen werden, der grob die Plausibilität der Änderung überprüft. Vom Fachbereich ist ein Vorher-nachher-Test durchzuführen, und die Ergebnisse sind miteinander zu vergleichen. Anschließend muss die Verwendung durch einen Manager des Fachbereichs und dem Umsetzungsverantwortlichen im Vieraugenprinzip freigegeben werden.

Ausblick

Um eine klare Perspektive zur Auflösung des beschriebenen Zielkonflikts zu haben und diese Position der regulatorischen Aufsicht gegenüber glaubwürdig vertreten zu können, ist es notwendig, ein Zielbild und einen Entwicklungsfahrplan für die IT-Architektur zu definieren.[6] Hierzu kann es sinnvoll sein, perspektivisch die komplette Risiko- bzw. Banksteuerung auf High-Performance-Bank-Steering[7] umzustellen. Die Idee ist hierbei die Einrichtung einer fachlichen und technischen Layer-Struktur, in der flexible Rechenkerne und Szenarioanalysen risikoartenübergreifend auf eindeutig definierte Daten ("Single Point of Truth") zugreifen und fachlich von entsprechend angepassten Prozessen flankiert werden und in der die Reporterstellung separat in einem eigenen Layer erfolgt. Ziel dieser Architektur ist es, die Anwender in die Lage zu versetzen, jede relevante Fragestellung und jedes mögliche Szenario innerhalb kürzester Zeit zu beantworten bzw. zu berechnen.

Fussnoten

1. Zum Beispiel nationale Regulatoren, Wirtschaftsprüfer, Europäische Bankenaufsichtsbehörde, Treuhänder, Ratingagenturen, Investoren.

2. Dabei handelt es sich um ein nahezu sequenzielles Erarbeiten von Anforderungsdokument, Fachkonzept, IT-Konzept, Umsetzung und abschließendem Test.

3. Dabei handelt es sich um ein iteratives Vorgehensmodell in der Softwareentwicklung. Die Entwicklung erfolgt in kürzeren Phasen, die aber so gestaltet sein müssen, dass sie für den Abnehmer einen Nutzen haben.

4. Individuelle Datenverarbeitung: Datenverarbeitung im Fachbereich, häufig auf Basis von Microsoft-Office-Produkten.

5. Zum Beispiel aus AT 4.3.2: "Die Risikosteuerungs- und -controllingprozesse müssen gewährleisten, dass die wesentlichen Risiken (…) frühzeitig erkannt, vollständig erfasst und in angemessener Weise dargestellt werden können (…)"

6. *Moving Beyond Compliance: How Banks Should Leverage Technology to Capitalize on Regulatory Change*, The Boston Consulting Group (October 2011).

7. *High Performance Bank Steering: Leveraging and Capitalizing on High Performance Technology*, The Boston Consulting Group (August 28, 2013).

Die Autoren

Dr. Walter Bohmayr ist Partner und Managing Director im Wiener Büro der Boston Consulting Group. Sie erreichen ihn unter bohmayr.walter@bcg.com.

Björn Brings ist Consultant im Kölner Büro der Boston Consulting Group. Sie erreichen ihn unter brings.bjoern@bcg.com.

Jörg Erlebach ist Partner und Managing Director im Frankfurter Büro der Boston Consulting Group. Sie erreichen ihn unter erlebach.joerg@bcg.com.

Ulrik Lackschewitz ist Group Head of Financial & Risk Controlling bei der Nord/LB. Sie erreichen ihn unter ulrik.lackschewitz@nordlb.de.

Kontakt

Für weitere Diskussionen zu dieser Studie kontaktieren Sie bitte einen der Autoren.