



Finanz Colloquium
Heidelberg

Banken-Times **SPEZIAL**

IT / ORGA / NEUE MEDIEN

Januar & Februar 2014

Finanz Colloquium Heidelberg

eMail: info@fc-heidelberg.de

Web: www.fc-heidelberg.de

In Zusammenarbeit mit:



Roland Hein
- Geschäftsführer -

bit Informatik GmbH

WIP - Der Wissenschaftspark Trier
Am Wissenschaftspark 32
54296 Trier

Tel.: +49 651 966 29-112

Fax: +49 651 966 29-100

eMail: roland.hein@bit-informatik.de

Web: www.bit-Informatik.de

Sehr geehrte Damen und Herren,

unser Newsletter enthält in dieser Ausgabe Beiträge zur **Datenqualität, IT-Berechtigungen** und **Prozessmanagement**.

Die Inhalte haben wir zusammen mit unserem [Kooperationspartner bit Informatik](#) gestaltet. bit Informatik bietet Standardsoftware zur Umsetzung von gesetzlichen und bankfachlichen Anforderungen an, Schwerpunkte liegen in der Umsetzung von Programmeinsatzverfahren sowie der Vergabe und Kontrolle von IT-Berechtigungen.

Zur Abbestellung dieses Newsletters oder zur Aufnahme von Kollegen/Kolleginnen in den Verteiler senden Sie uns bitte eine eMail an btspezial@fc-heidelberg.de. Wenn Sie einen eigenen Gastbeitrag verfassen möchten, freuen wir uns ebenfalls über Ihre Nachricht.

Mit besten Grüßen aus Trier und Heidelberg,

Roland Hein, Geschäftsführer, bit Informatik GmbH

Thomas Göhrig, Geschäftsführer, Finanz Colloquium Heidelberg

Auswirkungen des BCBS 239 „Grundsätze zur Aggregation von Risikodaten und Risikoberichterstattung“ auf die Datenhaltung und das Datenmanagement der Institute

1. Einleitende Worte

Das Thema Daten und Datenqualität zieht sich seit jeher durch die Risikosteuerungsinstrumente einer Bank. Jeder Risikocontroller weiß, dass die Resultate der Methoden und Modelle maßgeblich von der Datenqualität beeinflusst werden. Oft ist es nicht die Anwendung der Methoden und Modelle, sondern die Datenbeschaffung, -veredelung und –konsistenzprüfung, welche in der Praxis am meisten Zeit binden. Zudem ist dies oft mit manuellem Aufwand verbunden. Auch der Baseler Ausschuss hat dies erkannt und im Januar 2013 die „Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung (BCBS 239)“ veröffentlicht. Dort wird als wesentliche Lehre aus der Finanzmarktkrise formuliert, „dass die Informationstechnologie- (IT) und Datenarchitektur vieler Banken für die umfassende Steuerung finanzieller Risiken nicht geeignet war. (BCBS (2013), S. 1)“

Auch wenn das BCBS 239 nicht direkt im deutschen Recht Gültigkeit erlangt, ist anzunehmen, dass eine Umsetzung über die nationale Aufsicht zeitnah erfolgen wird. Dieser Artikel stellt die wesentlichen Inhalte des BCBS 239 vor, strukturiert diese und gibt erste Handlungsimplicationen für die Praxis.

2. Definition der Risikodatenaggregation

Im ersten Schritt gilt es, den im Papier verwendeten Begriff der Risikodatenaggregation zu definieren. Dies geschieht in Tz. 8, visualisiert in Abbildung 1:

Definition: Risikodatenaggregation

„Der Begriff Risikodatenaggregation [umschreibt] die **Definition, Erhebung und Verarbeitung** von **Risikodaten** gemäss den Anforderungen an die Risikoberichterstattung einer Bank mit dem Ziel, dieser einen **Abgleich** der eigenen Performance gegenüber der bankinternen **Risikotoleranz** bzw. -**bereitschaft** zu ermöglichen. Hierzu zählen das **Auswählen, Zusammenführen** sowie **Aufschlüsseln** von Datensätzen.“

Abbildung 1: Definition der Risikodatenaggregation gem. Tz. 8

Quelle: BCBS (2013), Tz. 8.

Der Begriff ist an dieser Stelle sehr weitreichend gefasst, umschreibt er doch den gesamten Prozess der Datenerhebung in einem Institut. Auch wird deutlich, dass das Thema der Definition von Daten dazu führen soll, dass in einem Institut sowohl dieselben Begrifflichkeiten als auch konsistente Inhalte verwendet werden sollen. Dies ist in den Häusern oftmals noch nicht vollumfänglich umgesetzt.

3. Wesentliche Inhalte des BCBS 239

Das BCBS ist in verschiedene Grundsätze aufgeteilt. Abbildung 2 auf der Folgeseite verdeutlicht diese und beschreibt deren Inhalte.

Die Inhalte des BCBS 239 sind umfassend und weitreichend (Vgl. auch KPMG (2013), S. 3). So wird direkt zu Beginn das Thema Datenqualität im **Corporate Governance** Bereich verankert. Hierdurch wird die Wichtigkeit des Themas deutlich. Der Begriff **Datenarchitektur** bedeutet, dass ein entsprechendes **Data Warehouse** vorhanden sein muss, welches die Daten konsistent aggregiert und nach Möglichkeit vollautomatisch aufbaut. Im Idealfall können Daten dann ohne weitere Veredlung über entsprechende Front Ends im Drill-Down Modus ausgewertet werden. Auch die Datenerhebung in **Stressphasen** wird häufig erwähnt. In Krisen muss das System der Datenerhebung auch höhere Taktungen als im Normalfall verkraften. Zudem wird auf die Aktualität der Daten abgestellt. Je zeitnäher aggregierte Daten zur Verfügung stehen, desto besser. Trotzdem sollen Daten **genau, integriert und vollständig** sein, zudem soll das System so dynamisch aufgebaut sein, dass Anpassungen schnell möglich sind. Explizit genannt werden Ad-Hoc Meldungen an die Aufsicht – was wiederum auf höhere Anfragen in der Zukunft schließen lässt. In Bezug auf die Reportings wird die **adressatengerechte Aufbereitung** bei gleichzeitiger **Erfassung aller wesentlichen Erkenntnisse** in den Vordergrund gestellt. Dies ist durchaus eine ambitionierte Aufgabe, da dies in der Praxis oft mit manuellen Schritten verbunden ist. Die klare Aufforderung zur (Voll)automatisierung wird deutlich, zumal in der deutschen Umsetzung eine **Frist von 10 Tagen für die Reporterstellung** im Raum steht (Vgl. Zimpel (2013), S. 13).

Nr	Aspekt	Grundsatz
1	Governance	Die Risikodaten-Aggregationskapazitäten und Verfahren zur Risikoberichterstattung einer Bank sollten strengen Prinzipien zur Unternehmensführung in Übereinstimmung mit anderen vom Basler Ausschuss veröffentlichten Grundsätzen und Empfehlungen unterliegen.
2	Datenarchitektur und IT-Infrastruktur	Eine Bank hat eine interne Datenarchitektur und IT-Infrastruktur zu entwerfen, einzurichten und zu pflegen, die die Risikodaten-Aggregationskapazitäten und Verfahren zur Risikoberichterstattung nicht nur unter gewöhnlichen Umständen, sondern auch in Stressphasen oder Krisen vollumfänglich unterstützt, wobei die übrigen Grundsätze unverändert gelten.
3	Genauigkeit und Integrität	Eine Bank sollte in der Lage sein, genaue und verlässliche Risikodaten zu generieren, um den Genauigkeitsanforderungen im Berichtswesen unter gewöhnlichen Umständen sowie in Stressphasen oder Krisen gerecht zu werden. Die Daten sind möglichst auf automatisierter Basis zu aggregieren , um die Fehlerwahrscheinlichkeit so gering wie möglich zu halten.
4	Vollständigkeit	Eine Bank sollte in der Lage sein, sämtliche wesentlichen Risikodaten innerhalb des Konzerns zu generieren und zu aggregieren . Die Daten sollten nach unterschiedlichen Kategorien geordnet zur Verfügung stehen (u.a. Geschäftsfelder, Konzerngesellschaften, Art des Vermögenswerts, Branche und Region), wobei das jeweils zu betrachtende Risiko für die Auswahl derjenigen Kategorien maßgeblich ist, die die Identifizierung und Meldung von Risikopositionen, Risikokonzentrationen sowie aufkommenden Risiken ermöglichen.
5	Aktualität	Eine Bank sollte in der Lage sein, aggregierte und aktuelle Risikodaten in einem angemessenen zeitlichen Rahmen zu generieren ; die Grundsätze hinsichtlich Genauigkeit, Integrität, Vollständigkeit und Anpassungsfähigkeit gelten dabei unverändert. Die genaue Terminierung hängt von der Art und der potenziellen Volatilität des zu erfassenden Risikos ab sowie von dessen Beitrag zum Gesamtrisikoprofil der Bank. Die genaue Terminierung ist darüber hinaus abhängig von den bankinternen Häufigkeitsanforderungen an die Risikoberichterstattung – unter Berücksichtigung der Charakteristik und des Gesamtrisikoprofils der Bank (sowohl unter gewöhnlichen Umständen als auch in Stressphasen oder Krisen).
6	Anpassungsfähigkeit	Eine Bank sollte in der Lage sein, aggregierte Risikodaten zu generieren , um eine große Bandbreite an Ad-hoc-Anfragen an die Risikoberichterstattung bearbeiten zu können; hierzu zählen u.a. Anfragen in Stressphasen oder Krisen , Anfragen im Zusammenhang mit geänderten internen Anforderungen sowie Anfragen der Aufsicht.
7	Genauigkeit	Risikomanagementberichte müssen aggregierte Risikodaten genau und präzise vermitteln und Risiken akkurat wiedergeben. Einzelne Berichte müssen abgeglichen und validiert werden.
8	Umfassender Charakter	Ein Risikomanagementbericht muss alle wesentlichen Risikobereiche , die einen Bankkonzern betreffen, abdecken. Umfang und Detailliertheit eines Berichts haben dabei der Bedeutung und Komplexität der Geschäftstätigkeit der Bank, deren Risikoprofil sowie den Anforderungen der Adressaten Rechnung zu tragen.
9	Klarheit und Nutzen	Risikomanagementberichte müssen klar und prägnant formuliert sein. Sie müssen leicht verständlich und gleichzeitig umfassend genug sein, um fundierte Entscheidungen zu ermöglichen. Die in ihnen enthaltenen Informationen müssen relevant und auf die Bedürfnisse der Adressaten abgestimmt sein.
10	Häufigkeit	Die Häufigkeit , mit der Risikomanagementberichte erstellt und verbreitet werden, ist vom obersten Verwaltungsorgan und von der Geschäftsleitung (oder gegebenenfalls anderen Adressaten) zu bestimmen . Dabei sind die Bedürfnisse der Adressaten ebenso zu berücksichtigen wie die Art der Risiken, die gemeldet werden, die Geschwindigkeit, mit der Risiken sich wandeln können, sowie die Bedeutung der Berichte für ein solides Risikomanagement und eine effektive und effiziente Entscheidungsfindung in der gesamten Bank. In Stressphasen oder Krisen ist die Häufigkeit der Berichte zu erhöhen .
11	Verbreitung	Risikomanagementberichte müssen unter Gewährleistung der Vertraulichkeit an die zuständigen Stellen verteilt werden.
12	Überprüfung	Die Aufsichtsinstanzen müssen in regelmäßigen Abständen die Einhaltung der elf bisher genannten Grundsätze innerhalb einer Bank überprüfen und evaluieren.
13	Korrektur- und Aufsichtsmaßnahmen	Die Aufsichtsinstanzen müssen über geeignete Instrumente und Ressourcen verfügen, um die effektive und zeitnahe Korrektur von Mängeln einer Bank im Hinblick auf ihre Datenaggregationskapazitäten und Verfahren zur Risikoberichterstattung zu verlangen, und diese Instrumente und Ressourcen auch einzusetzen. Dabei sollten ihnen unterschiedliche Instrumente zur Verfügung stehen, darunter Säule 2.
14	Grenzüberschreitende Zusammenarbeit	Die Aufsichtsinstanzen müssen mit den entsprechenden Behörden anderer Länder bei der Überwachung und Überprüfung der Grundsätze sowie bei der Umsetzung eventueller Korrekturmaßnahmen zusammenarbeiten .

Abbildung 2: Grundsätze des BCBS 239

Quelle: Eigene Darstellung in Anlehnung an BCBS (2013), S 6 – 17.

Die Aufsichtsinstanzen sind angehalten, die Einhaltung der Grundsätze zu überwachen. Hierzu wird sogar die Säule 2 explizit erwähnt, was auf eine baldige Integration in die MaRisk im Bereich AT 4 – 7 schließen lässt. Auch die grenzüberschreitende Zusammenarbeit der Behörden wird entsprechend verankert.

4. Handlungsbedarf für die Institute

Auch wenn bis zur Integration in deutsches Recht noch einige Zeit vergehen wird, sind die Institute gut beraten, schon vorzeitig einige Vorkehrungen zu treffen. Einige der einzuleitenden Maßnahmen werden einen längeren zeitlichen Vorlauf benötigen:

1. So ist sicherzustellen, dass alle wesentlichen Risikomanagementdaten – hierzu zählen mittlerweile nahezu alle veredelten Monats- oder gar Tagesdaten – in einem **Data Warehouse** aufgebaut und auch ausreichend historisiert werden. Hierbei ist besonderer Wert auf die im BCBS angesprochene Dynamisierung zu legen.
2. Des Weiteren bietet es sich an, eine zentrale Stelle im Haus zu benennen, welche als „**Datenqualitätsmanager**“ für die Konsistenz, Richtigkeit und Vollständigkeit der Daten verantwortlich ist. Dazu gehören z.B. Ratings, Sicherheiten, Kundensystematiken, Zinsen, Tilgungen, Bonitätsprämien, verbuchte/vorgemerkte EWB's, Betreuer, Kundentyp u.v.m.
3. Ein weiterer wichtiger Aspekt ist die Integration und **Konsistenz** von „**Meldedaten**“ und „**Steuerungsdaten**“. Noch ist es an vielen Stellen so, dass verschiedene Abteilungen für die Bereiche „Meldung“ und „Risikocontrolling“ zuständig sind. Aktuelle Entwicklungen im europäischen Melderecht (FinaV, COREP, FINREP, etc.) führen jedoch dazu, dass sich diese Datenbasen immer mehr angleichen. Eine vollständige Konsistenz und die Möglichkeit der vollautomatischen Überführbarkeit ineinander sind in naher Zukunft umzusetzen.
4. Die **Risikoreports** sollten einer erneuten Überprüfung hinsichtlich der 14 Grundsätze unterzogen werden. Auch hier ist weniger oft mehr – allerdings erfordert dies auch die entsprechenden Workflows im Hintergrund, welche es dem Risikocontroller ermöglichen, wichtige von unwichtigen Dingen schnell unterscheiden zu können.

5. Fazit und Ausblick auf die Zukunft

Das BCBS greift viele Dinge auf, die in einer modernen Banksteuerung selbstverständlich sein müssten. Die Anforderungen des BCBS gehen an vielen Stellen jedoch weit über das hinaus, was klassische Volksbanken und Sparkassen leisten müssen. Das BCBS zielt **eindeutig** auf große, systemrelevante Institute ab, eine Umsetzung für diese ist bis 2016 geplant. Aus dem Papier selbst ist eine geplante Gültigkeit für nicht-systemrelevante Institute nicht erkennbar. Es bleibt zu hoffen, dass, wenn die Implementierung in Säule 2 erfolgt, diese mit dem ausreichenden Augenmaß vorgenommen wird, um auch an dieser Stelle den Grundsatz der doppelten Proportionalität beizubehalten.

Literatur zum Thema

BCBS (2013): Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung, Januar 2013, erhältlich auf: http://www.bis.org/publ/bcbs239_de.pdf, Abfrage vom 15.12.2013.

KPMG (2013): 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, Frankfurt 2013, erhältlich auf: <http://www.kpmg.com/DE/de/Documents/BCBS-239-2013-KPMG.pdf>, Abfrage vom 15.12.2013.

Zimpel, R. (2013): Einheitliches Risikomanagement BCBS # 239: Grundsätze zur Aggregation von Risikodaten und Risikoberichterstattung, in: News 02/2013, S. 11 – 13, erhältlich auf: http://www.msg-gillardon.de/fileadmin/user_upload/pdf/fachartikel/NEWS/2013-02/BCBS-239-NEWS-2013-02.pdf, Abfrage vom 15.12.2013.

Dr. Svend Reuse, Abteilungsleiter Controlling, Sparkasse Mülheim an der Ruhr

Seminartipp zum Thema: [Datenqualität im Risikomanagement](#)

Die Sicherstellung aktueller und korrekter Basisdaten sowie eine transparente und zeitnahe Datenverdichtung sind eine hohe prozessuale Herausforderung. Im Fokus der Veranstaltung „[Datenqualität im Risikomanagement](#)“ am **10. April 2014 in Köln** stehen die einheitliche Klassifizierung valider Daten aus diversen IT-Systemen und die möglichst automatisierte Bereitstellung eines zentralen Reportings. Die Inhalte richten sich u.a. auch an die Bereiche Orga/IT und Revision. Am Vortag findet das passende Kombi-Seminar „[Risikoreporting - Verschärfte Vorgaben für \(Risiko-\) Berichterstattung](#)“ statt.

Weitere interessante Veranstaltungen im 1. Halbjahr 2014

[Prüfung IT im Fokus von MaRisk und Bundesbank, 12.-13.05.2014 in Frankfurt](#)

[Herausforderung IT – Strategie, 14.05.2014 in Frankfurt](#)

[IT-Dokumentation: schlank und revisionssicher, 15.05.2014 in Frankfurt](#)

[Vergabe und Kontrolle von IT-Berechtigungen, 25.06. in Frankfurt/M.](#)

[2. Fachtagung IT-Sicherheit, 26.-27.06. in Frankfurt/M.](#)

Hier können Sie unseren aktuellen [Seminarkatalog](#) für 2014 herunterladen.

Facetten der IT-Berechtigungsarten

Die Abteilungen Betriebs- und IT-Organisation sowie Prozessmanagement von Kreditinstituten wie Genossenschaftsbanken, Privatbanken oder Sparkassen stehen heute vor der Herausforderung, neue, von den Fachabteilungen geforderte Software Anwendungen zügig zum produktiven Einsatz zu bringen. Gleichzeitig müssen aber auch die bankfachlichen Anforderungen wie zum Beispiel das ordnungsgemäße Programmeinsatzverfahren oder die MaRisk gemäß AT 4.3, 4.4 und 7.2 (u.a. internes Kontrollsystem) eingehalten werden.

Gerade durch die Novellierung der MaRisk im November 2012 wurden die Anforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der Deutschen Bundesbank gegenüber den Kreditinstituten konkretisiert.

In der Regel setzen heute die Kreditinstitute oft mehr wie 100 Anwendungen ein, die sich in Kategorien wie Betriebssysteme, Groupware Software, Terminalserver-Systeme sowie Anwendungen einteilen lassen. Jede dieser Anwendungen wiederum verwendet mehrere hundert Einzelrechte, die in Profile zusammengefasst werden. Dies geschieht über den Hersteller einer Software (Standardprofile) und ist somit für das Kreditinstitut gegeben und nicht änderbar. Andererseits ist aber das Kreditinstitut auch gefordert, eigene Berechtigungsprofile zu definieren (Individualprofile). Die Komplexität wird damit abgerundet, dass all diese Berechtigungen (Einzelrechte als auch Profile) den heute in einem Kreditinstitut verwendeten Objekten Mitarbeiter, Stelle, Abteilung bzw. organisatorische Einheit oder dem Institut selbst zugeordnet werden müssen. Diese Objekte, basierend auf Organigrammen, finden in den Kernbanksystemen sowie Personalsystemen Anwendung.

Im Rahmen eines anwendungsübergreifenden Soll-Rollenkonzepts muss eine Zuordnung der Berechtigungen zu den verwendeten Objekten transparent nachvollziehbar sein. Jede Berechtigung muss darüber hinaus in regelmäßigen Abständen in einem risikoorientierten Verfahren bestätigt werden (IKS). Es muss also festgelegt werden, ob es sich um ein sensibles Recht handelt, das mindestens halbjährlich zu überprüfen ist oder eine weniger kritische Berechtigung mit einem jährlichen Prüfungsturnus (Stichwort Rezertifizierung nach MaRisk 4.3.1). Zudem müssen alle Berechtigungen innerhalb einer Anwendung als auch anwendungsübergreifend auf Abhängigkeiten, d.h. unzulässige Berechtigungskombinationen, hin überprüft werden. Diese Kennzeichnungen sind nicht nur vorzunehmen, sondern müssen bei den täglich angewandten Prozessen von Berechtigungsveränderungen berücksichtigt werden.

Neben den bereits genannten Softwareberechtigungen gibt es weitere Berechtigungsarten bzw. Kompetenzen, die aufgrund von bankfachlichen Anforderungen ebenfalls zu dokumentieren sind. Bei der ersten Berechtigungsart handelt es sich um die Rubrik der physischen Zugangsberechtigungen. Hier wird über ein Kartensystem oder auch Transponder festgelegt, zu welchen Gebäuden, Etagen oder Räumen einem Mitarbeiter Zugang gewährt wird. Unter dieser Rubrik sind ebenso zu betrachten, welche Schlüssel einem Mitarbeiter ausgehändigt wurden. Eine Verwaltung von Schlüsseln spielt zum Beispiel bei Filialen eine wichtige Rolle. Mitarbeiter wie der Geschäftsstellenleiter, der Kundenberater, der Kassierer oder der Hausmeister verfügen über verschiedene Schlüssel und damit unterschiedliche physische Zugangsberechtigungen.

Eine weitere Berechtigungsart bilden die heute verwendeten mobilen Geräte. Aufgrund der erweiterten Verfügbarkeit der Mitarbeiter für die Kunden werden Geräte wie Blackberries, iPhones, iPads etc. ausgerollt. Diese mobilen Geräte werden auf Basis unterschiedlicher Berechtigungsprofile wie zum Beispiel Vorstand, Kundenberater, IT-Organisation etc.

konfiguriert. Somit besteht heute nicht nur die Anforderung, aus Kostengründen zu verwalten, welcher Mitarbeiter(in) über ein mobiles Gerät verfügt, sondern ebenfalls in einem Soll-Rollenkonzept festzulegen, welche Aufgabe (Aufgaben- und Stellenbeschreibung) ein mobiles Gerät verlangt.

Bei der dritten Berechtigungsart betrachtet man die fachlichen Kompetenzen. Hierbei handelt es sich um Kompetenzen die z. B. für die Kredit- oder Wertpapierberatung (Kompetenzstufen) notwendig sind. Unter dieser Rubrik ist aber auch die geschäftliche Vertretungsmacht (Handlungsvollmachten) zu sehen. Das heißt, man dokumentiert zum Beispiel, über welche Kompetenzen (Disposition) der Mitarbeiter oder der Leiter in der Abteilung Einkauf verfügt. Hierzu würden auch die kaufmännische Vollmacht Prokura mit ihren Arten Einzel-, Filial- sowie der echten Gesamtprokura zu zählen sein.

Mit der Abbildung und damit Dokumentation von Belehrungen, über die ein Mitarbeiter aktuell verfügt oder verfügen sollte, wäre die vierte Berechtigungsart zu untersuchen. Belehrungen haben die Eigenschaft, dass diese meistens über ein Ablaufdatum verfügen, d.h. in 12, 24 oder 36 Monaten auslaufen und damit wieder zu aktualisieren sind. Bestimmte Aufgaben, die von einem Mitarbeiter ausgeführt werden, setzen zwingend eine Belehrung voraus. Somit besteht eine direkte Beziehung zwischen einer Belehrung und einer definierten Stelle und ist demnach Bestandteil des Soll-Rollen-konzepts. Unter Belehrungen sind hier die Geldwäsche und die Mitarbeiteranzeigeverordnung für Anlageberater sowie für Vertriebsbeauftragte zu sehen, aber auch Belehrungen wie zum Beispiel zum Thema Brandschutz.

Verlässt man das Thema, welche Berechtigungen heute in einem Kreditinstitut existieren, so würde man unter dem Aspekt einer zentralen, anwendungsübergreifenden Benutzerrechteverwaltung auch untersuchen und festlegen müssen, welche Personengruppen denn über Berechtigungen im eigenen Institut verfügen. An erster Stelle denkt man hier sofort an die eigenen Mitarbeiter. Daneben wird man aber schnell feststellen, dass neben den internen Mitarbeitern auch externe Mitarbeiter zu berücksichtigen sind. Zu nennen wären hier zum Beispiel Verbundpartner, Dienstleister der Datenverarbeitung oder dem Facility Management, Prüfer des Verbandes, der BaFin, der Bundesbank oder dem Finanzamt bzw. Rentenversicherung. Hierzu zählen aber auch Praktikanten.

Neben diesen natürlichen Personen, die in einem Kreditinstitut über verschiedenste Berechtigungen verfügen, müssen aber auch die „technischen Personen“ betrachtet werden. Einige Softwareanwendungen verfügen über technische User, die wiederum über sensible Berechtigungen verfügen. Daneben existieren Administratorerkennung, die einer Person zugewiesen wurden. Somit arbeiten wenige Mitarbeiter, oftmals in der DV-Organisation, mit zwei Benutzerkennungen: der Standardkennung und einer zweiten Administratorenkennung zum Ausführen bestimmter Administrationsarbeiten.

Zur Verwaltung dieser mitunter sehr komplexen Berechtigungen müssen praxistaugliche Prozesse und Abläufe institutionalisiert werden. Eine MaRisk-konforme Vergabe und Kontrolle der Rechte ist in einem angemessenem Zeitaufwand heute nur noch mit spezieller Software für das Berechtigungsmanagement durchführbar. Hier ist insbesondere auf eine möglichst breite Integration der heterogenen IT-Systemlandschaft in einer zentralen Administrationskonsole zu achten.

Roland Hein, Geschäftsführer, bit Informatik GmbH

Seminartipps zum Thema

[Prüfung IT im Fokus von MaRisk und Bundesbank, 12.-13.05.2014 in Frankfurt](#)

[Vergabe und Kontrolle von IT-Berechtigungen, 25.06. in Frankfurt/M.](#)

Aktuelle Buchneuerscheinung

[Bearbeitungs- und Prüfungsleitfaden Datenschutz & IT-Sicherheit 3. Auflage](#)

Die technisch-organisatorischen Maßnahmen des Datenschutzes und der IT-Sicherheit in Kreditinstituten sind geprägt von zunehmenden gesetzlichen und regulatorischen Anforderungen. Des Weiteren stellt die hohe Sensibilität der Kunden bei Datenschutzverstößen und technischen Problemen ein erhebliches Reputationsrisiko für die Bank dar. Die IT-Systeme als Rückgrat der Bank haben daher höchste Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten. Diesbezüglich stehen insbesondere die betrieblichen Datenschutz- und IT-Sicherheitsbeauftragten vor großen Herausforderungen. [weiter lesen](#)

Weitere Buchtipps

[Prüfung IT im Fokus von MaRisk und Bundesbank](#)

[Bearbeitungs- und Prüfungsleitfaden Social Media in Banken und Sparkassen](#)

Hier können Sie unseren neu erschienenen [Buchkatalog](#) für das 1. Hj 2014 herunterladen.

Prozessmanagement und Schriftlich fixierte Ordnung (SFO) – Vision und Wirklichkeit

Derzeit hat eine besondere Gruppe von Menschen, nämlich (mehr oder weniger, alle) Organisationsleiter von Banken und Sparkassen, eine „Vision“ für ihr Institut: die **Einführung von Prozessmanagement**.

Durch ein Prozessmanagement im Institut wird Transparenz über die Prozesse geschaffen und die Grundlagen zur Prozesssteuerung erarbeitet. Der Einstieg zur erfolgreichen Einführung eines Prozessmanagements sowie dessen Umsetzung in die SFO erfolgt über eine

Prozesslandkarte. Diese stellt eine Übersicht über die grundlegenden Prozesse des Instituts dar. Wesentliches Merkmal dieser Prozesse ist eine „End-to-End“-Betrachtung, also „vom Kunden zum Kunden“. Im Idealbild sind alle notwendigen Informationen aus dem Prozess ersichtlich. Weiterführende fachliche Informationen sind in wenigen Textdokumenten enthalten, auf welche aus den Prozessen heraus verwiesen wird.

Die **Anforderungen** seitens der BaFin sind in den MaRisk AT 5 Organisationsrichtlinien in Verbindung mit KWG § 25a formuliert. Vorstand und Führungskräfte erwarten (aufsichts-)rechtskonforme, mitarbeitergerechte Informationen sowie eine effiziente, funktionsfähige und ordnungsgemäße Organisation durch präzise Schnittstellendefinitionen und ein eindeutiges Rollenmodell. Führungskräfte sehen darin ein Hilfsmittel zur Delegation und zur Einarbeitung neuer Mitarbeiter. Mitarbeiter erwarten eine komfortable Such-Funktion, Klarheit, Eindeutigkeit, Verständlichkeit und Aktualität der Informationen. Dadurch sollen Rückfragen vermieden bzw. deren Anzahl stark begrenzt werden. Stabsfunktionen erwarten reibungslose Übergaben an den Schnittstellen und eine klare Definition ihrer Aufgaben, Rechte und Verantwortlichkeiten. Die Organisation erwartet die Etablierung des Prozessgedankens im Institut und eine höhere Standardisierung im Anweisungswesen. Sie sieht darin die Basis für Optimierungen und Effizienzsteigerungen. Die Revision erwartet die Erfüllung von (aufsichts-)rechtlichen Anforderungen (insb. KWG, MaRisk), eine ordnungsgemäße Organisation sowie eine Grundlage für die Prüfungsarbeit. Technisch wird ein stabiles, einfaches und schnelles System mit intuitiver Bedienung und einem aktuellen Look-and-Feel erwartet.

Doch die **Realität** sieht momentan ganz anders aus: Die Organisationsrichtlinien sind oft unvollständig und auf mehrere Systeme verteilt, Gliederung und Aufbaustruktur sind „historisch gewachsen“ und zu detailliert. Inhaltlich werden häufig Redundanzen und Widersprüche sowie unzureichende Verständlichkeit bemängelt. Prozessvisualisierungen sind eher die Ausnahme. Das Organisationshandbuch (OHB) hat eine sehr geringe Akzeptanz bei den Mitarbeitern („ist eh alles veraltet“, „wird sowieso nicht so gelebt“). Die Kommunikation über Aktualisierungen und wesentliche Änderungen ist nicht ausreichend und deren Aufbereitung ohne Erläuterung kaum nachvollziehbar. Zudem ist die technische Plattform oftmals veraltet, die Systeme sind instabil, haben lange Antwortzeiten und eine ungenügende Suchfunktionalität.

Und wie gestaltet sich der Weg vom IST zur Vision?

Die Antwort ist ganz einfach: Durch das Aufsetzen eines OHB-Projekts („Projekt zur Gestaltung der SFO nach den Prinzipien des Prozessmanagements“). Neben der Erarbeitung und Verabschiedung der Prozessmanagement-Organisation gehören die Festlegung von Standards und Konventionen zur Dokumentation, die Verabschiedung von Redaktions- und Freigabeprozess, die Erarbeitung von Prozesslandkarten und Gliederungsstrukturen sowie nicht zuletzt die Aktualisierung und Entschlackung der bestehenden Regelungen zu den wesentlichen Zielsetzungen eines OHB-Projekts.

Ein OHB-Projekt erfüllt die meisten Kriterien eines zum Scheitern verurteilten Projektes. Durch die lange Laufzeit und die Vielzahl von Beteiligten, läuft es Gefahr zu versanden. Dennoch ist es auch eine Riesenchance, Prozessorientierung im Institut zu verankern und Transparenz über die Prozesse zu schaffen.

Wesentliche Erfolgsfaktoren sind der Wille, sich prozessorientiert auszurichten, das Silodenken der Fachbereiche aufzugeben und das Projekt als Change-Projekt zu verstehen. Außerdem braucht es die uneingeschränkte Vorstandsunterstützung, die frühzeitige und zielgerichtete Mitarbeiterinformation sowie die Einrichtung einer schlagkräftigen

Projektorganisation und die Setzung von ambitionierten, dennoch erreichbaren, Projektmeilensteinen.

Unter diesen Voraussetzungen kann die Verwirklichung der Vision gelingen.

Claudia Meier, Geschäftsführerin, Procedera Consult GmbH

Seminartipp zum Thema

[Procedera Jahreskongress 2014: „Endlich prozessorientiert“](#). Die SFO als Schlüssel zum Prozessmanagement. 20.-21. März 2014, Berlin.

Procedera begleitet Banken, Sparkassen und Unternehmen des privaten und öffentlichen Sektors in den Bereichen Prozess- und Organisationsberatung bei der Optimierung und Neuausrichtung ihrer Unternehmen (www.procedera.de).

Impressum

Finanz Colloquium Heidelberg GmbH – Plöck 32a – 69117 Heidelberg

VisdP: Thomas Göhrig

Telefon: 0 62 21 / 99 89 8-0 - Telefax: 0 62 21 / 99 89 8-99

E-Mail: Info@FC-Heidelberg.de – Internet: www.FC-Heidelberg.de

Geschäftsführer:

Dr. Christian Göbes, Frank Sator, Dr. Patrick Rösler, Marcus Michel, Michael Helfer, Thomas Göhrig

Sitz der Gesellschaft ist Heidelberg, Amtsgericht Mannheim, HRB Nr. 335598

Zur Abbestellung dieses Newsletters oder zur Aufnahme von Kollegen/Kolleginnen in den Verteiler senden Sie uns bitte eine eMail an btspezial@fc-heidelberg.de.