



Finanz Colloquium
Heidelberg

Banken-Times **SPEZIAL**

IT / ORGA / NEUE MEDIEN

November & Dezember 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 zu **MaRisk-konformen Prozessen des Rechtemanagements** und zu **Kosten und Nutzen von Social Media-Aktivitäten**.

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 bitspezial@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

MaRisk-konforme Prozesse des Rechtemanagements

Im Newsletter Januar & Februar 2014 wurde zum Thema Facetten der IT-Berechtigungen beschrieben, welche Berechtigungsarten in einem Kreditinstitut vorkommen, die Bewertung der Berechtigungen hinsichtlich „Kritikalität“ und welchen Objekten die Berechtigungen zugeordnet werden. Zusätzlich wurde erläutert, dass nicht nur die Mitarbeiter der Kreditinstitute über Berechtigungen verfügen, sondern auch Dritte und dass nach den MaRisk Anforderungen auch technische sowie administrative User beim Ansatz eines anwendungsübergreifenden Berechtigungskonzeptes zu berücksichtigen sind. Als Fortsetzung zum ersten Beitrag ging es in der Mai/Juni Ausgabe 2014 um den Aufbau eines anwendungsübergreifenden Soll-Rollenkonzeptes. Der heutige Newsletter beschäftigt sich mit den Anforderungen der MaRisk AT 4.3.1 Aufbau- und Ablauforganisation sowie AT 7.2 Technisch organisatorische Ausstattung.

Aufgabe eines Kreditinstitutes ist es, die Prozesse der IT-Rechtevergabe sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen sowie Kommunikationswege klar zu definieren und aufeinander abzustimmen. Diese Abläufe sind regelmäßig und anlassbezogen zu überprüfen. Die Überprüfung gilt ebenfalls für Zeichnungsberechtigungen und sonstigen eingeräumten Kompetenzen sowie Schnittstellen zu wesentlichen Auslagerungen.

Damit die Anforderungen der MaRisk in einem Haus erfolgreich umgesetzt werden können, ist es unbedingt erforderlich, die in den MaRisk verwendeten Begrifflichkeiten zu erläutern bzw. abzugrenzen. Bei der Umsetzung der Anforderungen sollten die betroffenen Abteilungen wissen, was sich hinter den Begriffen Prozesse, Aufgaben, Kompetenzen, Verantwortliche und Kontrollen verbirgt. Ohne Erläuterung läuft das Institut sonst Gefahr, dass die Abteilungen aneinander vorbei sprechen und die Prozesse bei der Einführung scheitern.

Identifiziert man nach der Beschreibung der verwendeten Begrifflichkeiten die Prozesse, so kann man eine erste Einteilung in operative, administrative und Endanwender Prozesse vornehmen.

Operative Prozesse werden in der Regel von der Personalabteilung gestartet. Diese umfassen die Neuanlage, Versetzung, Austritt oder die längerfristige Abwesenheit von Mitarbeitern/Mitarbeiterinnen im eigenen Haus. Durch den Start der operativen Prozesse müssen Berechtigungen vergeben (z.B. Neuanlage) oder Berechtigungen entzogen werden (z.B. im Prozess Austritt). Bei Versetzungen treffen beide Aktivitäten zu, da auf Basis des definierten anwendungsübergreifenden Soll-Rollenkonzeptes im Vergleich der alten mit der neuen Stelle sowohl IT-Berechtigungen vergeben als auch entzogen werden müssen. Zusätzlich kann es erforderlich sein, kritische Berechtigungen wie zum Beispiel Vorstandsrechte oder Rechte der Personalabteilung sowie administrative Rechte im 4-Augen-Prinzip zu prüfen. Aufgabe bei den operativen Prozessen ist es, festzulegen welche Personen die Prozesse starten dürfen, welcher Personenkreis diese Prozesse zur Überprüfung vorgelegt bekommen und welche Vorlaufzeiten notwendig sind. Alle Aktivitäten wie zum Beispiel Genehmigung, Ablehnung oder Änderung des Prozesses im zweiten Prozessschritt müssen lückenlos dokumentiert werden. Um dies sicherzustellen, bedarf es einer engen Abstimmung zwischen den Abteilungen IT, Organisation und Personal in Bezug auf das Prozessmanagement.

Hinter der Kategorie **administrative Prozesse** verbergen sich Prozesse die auf die Veränderung des Rechtenkonzeptes abzielen. Ein anwendungsübergreifendes Soll-Rollenkonzept basiert darauf, dass ein Kreditinstitut festgelegt hat, welche IT-Berechtigungen oder auch Zeichnungsberechtigungen im Zusammenhang mit Zahlungsverkehrskonten an den Objekten Mitarbeiter, Stelle, Abteilung oder dem Institut festgemacht bzw. welche Einzelberechtigungen einem Profil wie zum Beispiel Kassierer oder Kundenberater zugeordnet werden. Zusätzlich wurde im Soll-Rollenkonzept festgelegt, welche Wertebereiche für bestimmte Einzelberechtigungen im Hause Anwendung finden. Ein Beispiel: bei der Einzelberechtigung „SEPA-Überweisung“ entscheidet der Wertebereich, 500 oder 50.000 EUR, wie kritisch das Recht zu sehen ist. Herausforderung bei den administrativen Prozessen ist es somit festzulegen, welche Personen/Gruppen sich für

welche Berechtigungen verantwortlich zeigen, heißt ob die Vorlage einer Genehmigung zum Beispiel auf Anwendungsebene (Stichwort Anwendungseigentümer) oder auf Objektebene (Stelle, Organisationseinheit, Profil) vorgenommen wird. Die Genehmigung oder Ablehnung von IT-Berechtigungen mit Auswirkungen auf Zahlungsverkehrskonten wird in der Regel ab einer bestimmten Betragshöhe zum Beispiel größer 50.000 EUR vom Vorstand getroffen. Somit muss der Genehmigungsprozess so flexibel sein, kritische Berechtigungen zuvor festgelegten Führungskräften vorzulegen.

Ein besonderer Augenmerk muss auf den Prozess **Soll-/Ist-Abgleich** gelegt werden, hier erfolgt eine regelmäßige Überprüfung der Berechtigungen zwischen dem Soll-Rollenkonzept und dem juristischen Ist-Bestand, der von vielen Kreditinstituten derzeit eher stiefmütterlich behandelt wird. Aufgrund der zum Beispiel in Notfallmanagement ermittelten Risikostufe und Schutzkategorie einer Anwendung mit eigenem Rechtesystem sowie der Einzelbewertung der Berechtigungen in Admin-Recht, kritisch, sensibel oder zahlungsverkehrsrelevant bzw. im Genossenschaftsverband anhand der Ausprägungen IKS-Relevanz 1 bis 5, muss auf Basis der Kontrollanforderungen (Revision) festgelegt werden, ob halbjährlich oder jährlich ein Soll-/Ist-Abgleich durchzuführen ist. Auch hier muss pro Anwendung der Prozessablauf, heißt Einbindung des Anwendungseigentümers, Führungskräfte, Kenntnisnahme der Revision, etc. festgelegt werden.

Abschließend legt das Kreditinstitut die **Prozessabläufe für die Endanwender** fest. Hier geht es darum, zu dokumentieren, wie eine Kennwortrücksetzung oder Kennwortentsperrung vorzunehmen ist bzw. wie der Prozess der Beantragung von Berechtigungen ablaufen wird. Bei der Kennwortrücksetzung ist zu dokumentieren, dass nur für Personen eine Rücksetzung oder Entsperrung vorgenommen wird, die zuvor zweifelsfrei authentifiziert wurde. Bei der Beantragung von Berechtigungen startet in der Regel der Mitarbeiter den Prozess. In einem zweiten Schritt erfolgt die Vorlage beim direkten Vorgesetzten, abhängig des Wertebereiches wird die nächst höhere Führungskraft zusätzlich zwecks Genehmigung eingebunden. Im vierten Prozessschritt wird ein für das Soll-Rollenkonzept festgelegter Verantwortlicher entscheiden, ob das Recht im Fall 1 nur der beantragenden Person vergeben wird, alternativ im Fall 2 das beantragte Recht ins Soll-Rollenkonzept überführt wird. Das heißt, nicht nur der beantragende Serviceberater erhält das Recht, sondern alle Serviceberater des Hauses. Im weiteren Schritt erfolgt die Vergabe der Berechtigung durch den Administrator. Im letzten Prozessschritt würde bei Bedarf eine 4-Augen-Prüfung vorgenommen werden. Dieses Beispiel erläutert, wie komplex der Kommunikationsweg werden kann und damit die Wichtigkeit der Protokollierung.

Derzeit wohl wichtigster Prozess zur Umsetzung der MaRisk 4.3 ist der Prozess der **Rezertifizierung**. Hier erhalten die Führungskräfte im Rhythmus von 6, 12 und 24 Monaten Prozessvorlagen über die Berechtigungen ihrer zugeordneten Mitarbeiter/Mitarbeiterinnen.

Diese IT-Berechtigungen und Zeichnungsberechtigungen sind von der Führungskraft zu prüfen, bei Bedarf kann die Führungskraft weitere Verantwortliche in den Prozess dynamisch einbinden. Beanstandungen der Führungskräfte müssen nachgearbeitet werden, d.h. das Soll-Rollenkonzept muss anhand der administrativen Prozesse angepasst werden. Diese Beanstandungen werden in der Regel von den Verantwortlichen des Soll-Rollenkonzeptes vorgenommen.

All diese Prozesse müssen nach Abschluss archiviert und wie im Fall des Prozesses der Rezertifizierung 24 Monate vorgehalten werden.

Sind die Prozessabläufe erarbeitet und sollen im Institut zum Einsatz kommen, ist es wichtig zuvor alle Nutzer zu informieren und klarzustellen, dass Veränderungen von Berechtigungen nur noch über die Anwendung der Prozesse erfolgen kann und darf. Hier ist ein Sponsor wie zum Beispiel der Vorstand sehr hilfreich.

Roland Hein, Geschäftsführer, bit Informatik GmbH

Seminartipps zum Thema:

[Vergabe und Kontrolle von IT-Berechtigungen, 29.04.2015 in Berlin](#)

Veranstaltungen im 1. Halbjahr 2015

[Wirksame Notfallprozesse und Wiederanlaufplanung, 21.04.2015 in Frankfurt/M.](#)

[3. Fachtagung IT-Sicherheit, 27.-28.04.2015 in Berlin](#)

[IT-Dokumentation: schlank und revisionssicher, 30.04.2015 in Berlin](#)

[Prüfung IT im Fokus von MaRisk und Bundesbank, 29.-30.06.2015 in Frankfurt/M.](#)

[Sicherstellung der IT-Compliance, 01.07.2015 in Frankfurt/M.](#)

[IT-Strategie praxistauglich und prüfungssicher, 02.07.2015 in Frankfurt/M.](#)

Neuer Seminar- und Buchkatalog

In unserem druckfrischen [Seminarkatalog für das Jahr 2015](#) finden Sie für Ihre frühzeitigen Budget-/Seminarplanungen 2015 in allen Rubriken zahlreiche neue, z.T. auch sehr innovative Seminare, wie z.B. Aufsichts-Englisch und Speed-Reading.

Unserem neuen [Verlagsprogramm für das 2. Halbjahr 2014](#) können Sie unser neues Verlagsprogramm sowie die noch zu erscheinenden Titel von 2014 entnehmen. Insgesamt werden wir im 2. Halbjahr 10 neue Bücher auf den Markt bringen.

Kosten und Nutzen von Social Media-Aktivitäten

Social Media hat in den Alltag vieler Banken und Sparkassen Einzug gehalten. Die Möglichkeiten, mit Hilfe der (am weitesten verbreitenden) Social Media-Dienste, wie zum Beispiel Facebook, Xing, Twitter, YouTube usw., mit dem Kunden zu kommunizieren, wurden in den vergangenen Jahren vielerorts geschaffen. Das Einrichten der einzelnen Plattformen geht in der Regel schnell vonstatten und auch der laufende Betrieb ist bei vielen Diensten kostenlos bzw. zumindest kostengünstig.

Unabhängig vom oftmals kostenlosen Betrieb (i. S. von Nutzungsgebühren) verursachen die Social Media-Präsenzen jedoch durchaus **Kosten**. Hierunter fallen Personalkosten für den oder die Social Media-Manager bzw. -Redakteure. Hinzu kommen Ausgaben für Technik, Wartung und Abschreibung von Hardware und Software. Weiter zu nennen sind die Budgets, die für das Betreiben der Profile von Nöten sind: Werbebudgets für Facebook- und/oder Google-Anzeigen, Printanzeigen, Flyer usw. Nicht zuletzt erzeugen sogenannte Apps für die Durchführung von Social Media-Aktionen und im Speziellen die ggf. hierfür beauftragten Dienstleister entsprechende Kosten.

Es stellt sich somit die Frage, welche Aktionen in Social Media für ein Unternehmen lohnenswert sind und welche nicht. Die Beantwortung ist jedoch stark abhängig von den gesteckten Zielen, die ein Unternehmen mit einem Social Media-Engagement verfolgt. Das einfachste **Controlling** dieser Aktivitäten kann mit den „Bordmitteln“ der Social Media-Dienste erfolgen. Zu nennen sind hier exemplarisch die Seitenstatistiken von Facebook, die Abrufzahlen der Videos im YouTube-Channel, die Zugriffsstatistik des eigenen Weblogs oder die Anzahl der Re-Tweets bei Twitter,

Unter der Annahme, dass es sich bei Social Media in erster Linie um Kommunikation mit Kunden und Interessenten der Bank bzw. Sparkasse handelt, ist es sinnvoll, die Ressourcen in Aktivitäten zu investieren, die beim Kunden im Idealfall Begeisterung für das Unternehmen hervorrufen. Entsteht dann eine hohe Interaktionsrate bei den verschiedenen Aktivitäten, so kann diese Aktivität grundsätzlich als erfolgreich gewertet werden.

Die Sparkasse Pforzheim Calw betreibt seit einigen Jahren diverse Social Media-Plattformen. Als eines der ersten Kreditinstitute in Deutschland ist sie in **Twitter** aktiv, war bei **Facebook** „Early-Adopter“ und betreibt ein eigenes **Corporate-Blog**. Ein **YouTube-Channel** sowie ein **XING-Unternehmensprofil** runden die Aktivitäten mit den am weitesten verbreitenden Social Media-Plattformen ab.

Rückblickend können eine Vielzahl von Maßnahmen als erfolgreich bewertet werden. Insbesondere die Aktionen, die Kunden und Interessenten zu Beteiligten gemacht haben. Dies waren zum Beispiel:

Verteilung von Spenden durch die Bevölkerung

Hier konnten Schulklassen Projekte zum Thema Nachhaltigkeit einreichen, welche in einem gewissen Zeitraum umgesetzt werden mussten. Über die Attraktivität und Sinnhaftigkeit dieser Projekte wurde in Facebook durch Kunden und Interessenten abgestimmt. Die Gewinnerklassen erhielten entsprechende Geldmittel zur Umsetzung der geplanten Projekte. Einige Tausend Stimmen konnten hierbei gezählt werden.

Produktkampagne Girokonto für junge Erwachsene

Neben der klassischen Produktwerbung und dem Internet-Auftritt wurde in YouTube eine Video-Serie veröffentlicht, die auf den ersten Blick nichts mit der Produktkampagne zu tun hatte. Positive Kommentare und viele Abrufe waren der Lohn der Aktion.

Allerdings tragen nicht nur „große“ Aktionen zum Erfolg der Social Media-Präsenzen bei. Oftmals sind es – wie im richtigen Leben auch – die kleinen Dinge, die positive Resonanz erzeugen. Dies sind womöglich Aktivitäten aus dem Sparkassenleben: etwa das Posten eines Bildes vom Betriebssport. Auch nützliche Hinweise für Kunden, zum Beispiel zum Thema Online-Sicherheit, führen regelmäßig zu positiven Reaktionen. Im Blog der Sparkasse werden die Berichte der Auszubildenden über deren Ausbildung mit großem Interesse und hohen Abrufzahlen gelesen.

Auch mit einem Augenzwinkern versehene Aktivitäten sind in Social Media erfolgreich: So beteiligte sich stellvertretende Vorstandsvorsitzende der Sparkasse Pforzheim Calw an der ALS Ice Bucket Challenge. Da unter anderem beim entsprechenden YouTube-Video nicht die Eiskübel-Aktion im Vordergrund stand, sondern der Aufruf zum Spenden – auch für regionale Projekte – erhielt die Aktion ausschließlich positive Rückmeldungen.

Fazit: In jedem Haus gibt es eine Vielzahl von Aktivitäten, bei denen es sich lohnt, sie einer breiten Masse zu zeigen. Auch die Möglichkeit der aktiven Beteiligung von Kunden und Interessenten führt häufig zum Erfolg und anerkennenden Reaktionen in den Social Media-Kanälen. Dabei können diese Aktivitäten mit relativ geringem Aufwand und niedrigem Budget betrieben werden. Erzielen diese Aktionen eine **hohe Interaktionsrate**, steht einer positiven Imagebildung als einem der wesentlichen Ziele, und damit dem Erfolg der Social Media-Aktivitäten, nichts mehr im Wege.

Joachim Erich Schröder, Referent Medialer Vertrieb, Sparkasse Pforzheim Calw

Buchtipps zum Thema:

[Bearbeitungs- und Prüfungsleitfaden Social Media für Banken und Sparkassen, 2012, Finanz Colloquium Heidelberg, 216 Seiten](#)

FCH-Fachzeitschriften in elektronischer Form!

In Zeiten ständiger Erreichbarkeit und beruflicher Mobilität sind immer mehr Menschen mit ihrem mobilen Büro unterwegs. Sei es auf Handys, Tablets, E-Readern oder Notebooks, E-Formate von Büchern und Zeitschriften sind für diese Zielgruppe die ideale Lösung, alle Arten von Informationen kompakt, stets aktuell abrufbar und ohne zusätzliches Gepäck mit sich zu führen. Das Finanz Colloquium Heidelberg will Sie dabei wie folgt unterstützen: Wir möchten Ihnen die Möglichkeit bieten, unsere Fachzeitschriften zusätzlich zur klassischen Papierversion auch in elektronischer Form zu beziehen. Allerdings wissen wir nicht, welche Formate bzw. welchen Vertriebskanal Sie als unsere Leser bevorzugen. Deshalb bitten wir um Ihre Mithilfe:

Zunächst einmalig können Sie auf unserer Homepage www.FC-Heidelberg.de im Bereich „Mein FCH“ eine kostenlose Testausgabe des BankPraktiker 10/2014 als EPUB-Datei für E-Reader und Smartphones herunterladen. Die Registrierung ist selbstverständlich kostenlos und unverbindlich.

Als kleines Dankeschön für Ihre Zeit können sich alle teilnehmenden Kunden aus unserem Sortiment ein BankPraktiker WIKI ihrer Wahl aussuchen, das wir Ihnen dann gerne kostenfrei zustellen.

FCH Compliance Rechtsmonitoring:

Gerne unterstützen wir Sie auch im Rahmen eines Dienstleistungsvertrages bei Ihrem Rechtsmonitoring, in dem wir rechtlich relevante Änderungen (Gesetze, Verordnungen, Rundschreiben usw.) monatlich auswerten. Diese Auswertung ist vom Aufwand her abhängig von der Zahl der jeweiligen Änderungen. Um Ihnen dennoch einen monatlich gleichbleibenden Preis zu bieten, haben wir die Aufwände durchschnittlich kalkuliert. Dabei gehen wir von einer Ersparnis für Sie von im Durchschnitt 10 Aufwandstagen je Monat aus. Diese „ersparte“ Auswertungsleistung stellen wir mit einem Betrag von nur 750,00 Euro netto in Rechnung.

Das Ergebnis der Auswertungen finden Sie dann in unserem monatlichen Newsletter bzw. ab dem kommenden Jahr über Ihr eigenes Log-In auf unserer Homepage. Weitere Infos und eine kostenfreie Probeausgabe finden Sie unter:

<http://www.fchcompliance.de/index.php/rechtsmonitoring.html>

Bei Fragen sprechen Sie uns bitte gerne an:

Sabine.Warner@FC-Heidelberg.de

Sandra.Leicht@FC-Heidelberg.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.