



Finanz Colloquium
Heidelberg

Banken-Times **SPEZIAL**

IT / ORGA / NEUE MEDIEN

Mai & Juni 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 **Dokumentation und Prozessen von Programmeinsatzverfahren** sowie zum **Aufbau eines anwendungsübergreifenden Soll-Rollenkonzepts**.

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

Datengetriebene Dokumentation und Prozesse von Programmeinsatzverfahren

Der Einsatz von IT-Systemen sowie IT-Prozessen und damit die Sicherstellung der Integrität, der Verfügbarkeit, der Authentizität sowie der Vertraulichkeit der Daten sind in den Mindestanforderungen an das Risikomanagement (MaRisk) im allgemeinen Teil der 7.2 technisch-organisatorische Ausstattung klar beschrieben. Die Herausforderung für ein Kreditinstitut ist eine praxisgerechte Umsetzung des **Lebenszyklus** einer Software, von der Software-Beschaffung über ein Programmeinsatzverfahren inklusive der Risikoklassifizierung und der Schutzbedarfsanalyse, das Einspielen von Software-Updates bis hin zur Software-Ablösung **zu dokumentieren**. Wünschenswert ist die im Software Lifecycle erhobenen Daten in das Verfahrensregister einfließen zu lassen.

Die Anwendungen, die Kreditinstitute heute einsetzen, lassen sich im Wesentlichen in drei Kategorien einteilen. Anwendungen die vom angeschlossenen **Rechenzentrum** zur Verfügung gestellt werden, **Standardanwendungen** die von Dritten heißt externen DV-Dienstleistern eingekauft wurden als Ergänzung zum Anwendungsportfolio des Rechenzentrums und abschließend den **Eigenentwicklungen**. Besondere Herausforderung bei der dritten Kategorie der Eigenentwicklungen stellen die Datenträgersysteme dar, Stichwort MS Excel Dateien.

Zu Beginn des Lebenszyklus steht die **Software-Beschaffung**. In diesem Prozess geht es darum, die für eine Fachabteilung geeignetste Software zu ermitteln. Der Prozess berücksichtigt hierbei nicht nur die fachlichen Anforderungen, sondern auch die einmaligen Anschaffungskosten sowie die laufenden Kosten (Wartung). Wichtige Aufgabe der Abteilung IT ist zu prüfen, ob die Anwendung auch die Anforderungen der Rechenzentrumskonformität erfüllt. Wird schon beim Prozess der Software-Beschaffung eine Risikoklassifizierung sowie

eine Schutzbedarfsanalyse vorgenommen, so können diese Informationen bereits in den sich anschließenden Prozess Programmeinsatzverfahren überführt werden und verkürzt damit die Durchlaufzeiten der Abläufe erheblich. Kommt der Software-Beschaffungsprozess zu einem positiven Ergebnis, dient dieser als Vorstandsvorlage zur Genehmigung der Anschaffung.

Der zweite Schritt bedeutet im Prozess **Programmeinsatzverfahren** die beteiligten Abteilungen wie Fachbereich, IT- und Betriebsorganisation, Personal-/Betriebsrat, Datenschutz- und Informationssicherheitsbeauftragter, Controlling, Prozessmanagement, etc. datengetrieben einzubinden. Datengetrieben bedeutet hierbei, dass aufgrund der eingegebenen Daten zum Beispiel der Personal-/Betriebsrat oder der Datenschutzbeauftragte nur aktiv in den Prozess eingebunden werden, wenn Parameter wie zum Beispiel mitarbeiterbezogene oder kundenbezogene Daten mit einem „Ja“ beantwortet wurden. Weitere sinnvolle Parameter für den datengetriebenen, dynamischen Ablauf sind zum Beispiel der Wert für den MaRisk Bezug mit Auswirkungen für die Prozessschritte Risikocontrolling oder Compliance bzw. gegebenenfalls weitere Aktivitäten, wenn die Anwendung über ein eigenes Berechtigungssystem verfügt. Abzugrenzen hiervon sind Parameter, die einen verpflichtenden oder zwingenden Prozessschritt verlangen. Eine Risikostufe A oder B im Gegensatz zur Risikostufe C bedingen die Prozessschritte Programmfreigabe als auch eine Einsatzfreigabe. Notwendige Felder müssen somit als Pflichtfelder gelten, es muss aber für ein Institut die Möglichkeit existieren, pro Prozessschritt nicht zwingend notwendige Felder als Kann-Felder zu definieren oder bei Bedarf gänzlich auszublenden. Als Pflichtfelder sind die Werte **Verfügbarkeit, Vertraulichkeit und Integrität** zu sehen, die von der Fachabteilung erfasst und von Informationssicherheitsbeauftragten überprüft werden, um die Schutzbedarfsanalyse festzuschreiben. Sinnvoll an dieser Stelle ist es, dass der Informationssicherheitsbeauftragte auch die Auswirkungen der Notfallplanung (BCM) bewertet. Analog zur Schutzbedarfsanalyse ist die Pflege des Verfahrensregisters durch die Fachabteilung (Ersterfassung) und dem Datenschutzbeauftragten im weiteren Verlauf (Prüfung und gegebenenfalls Ergänzung) vorzunehmen. Das **Verfahrensregister** dokumentiert pro Anwendung an zentraler Stelle Parameter die als technisch-organisatorische Maßnahmen im Bundesdatenschutzgesetz nach §9 geregelt sind, Stichwort Zutritts-, Zugangs-, Zugriffskontrolle sowie der Weitergabe der Daten bis hin zu den Regelfristen für die Löschung der Daten bzw. die Dokumentation der internen sowie externen Empfänger der Daten.

Stehen **Software-Updates** an, muss in einem Prozess geregelt werden, ob eine erneute Programmeinsatzfreigabe vorgenommen werden muss oder das Update/Patch nach Abstimmung zwischen Fachabteilung und IT durch Analyse der Update-Beschreibung, heißt kritische oder wesentliche Änderung „ja/nein“, ohne Programmeinsatzfreigabe eingespielt werden kann.

Um den Lebenszyklus ganzheitlich zu dokumentieren, benötigen die Kreditinstitute noch einen Prozess zur **Software-Ablösung**. Auch in diesem Prozess werden die dafür notwendigen Abteilungen datenbezogen aktiv eingebunden und im letzten Prozessschritt erfolgt die Deinstallation der Software. Der Prozess aktualisiert den Eintrag im Verfahrensregister.

Gemäß den Empfehlungen von Kreditinstituten, die das **Projekt Software Lifecycle** umgesetzt haben, ist zuerst mit den Prozessen Programmeinsatzverfahren und Software-Update zu beginnen. Diese beiden Prozesse werden mit selektiven Fachbereichen produktiv eingesetzt und dann in einer zweiten Phase nach und nach auf alle Fachbereiche ausgerollt. Eine aktive Unterstützung der Fachbereiche durch die Abteilung Prozessmanagement ist hierbei sehr wichtig. Anschließend erfolgt die Aktivierung der Prozesse Software-Beschaffung

sowie Software-Ablösung. Das Verfahrensregister sollte hierbei frühzeitig berücksichtigt, heißt in die Prozesse integriert, werden. Anwendungen des Produktportfolios des Rechenzentrums werden hierbei gerne zuerst elektronisch abgebildet. Daran anschließend folgen die Anwendungen der Drittanbieter und Eigenentwicklungen. Anwendungen auf Trägersystemen erfolgen oftmals in der letzten Phase des Projektes, da sich hier ein Kreditinstitut in vielen Fällen mit einer großen Anzahl von Dateien auseinander setzen muss.

Roland Hein, Geschäftsführer, bit Informatik GmbH

Seminartipp zum Thema:

[Grauzone Individuelle Datenverarbeitung \(Excel & Co.\), 18. November 2014, Düsseldorf](#)

Weitere interessante Veranstaltungen im 2. Halbjahr 2014:

[Operatives Dienstleistermanagement, 10. November 2014, Berlin](#)

[Prüfung Dienstleistermanagement, 11. November 2014, Berlin](#)

[Wirksame Notfallprozesse und Wiederanlaufplanung, 12. November 2014, Berlin](#)

[IT-Projekte & neuer AT 8.2, 17. November 2014, Düsseldorf](#)

[Neu-Produkt-Prozess \(NPP\): Umsetzung & Prüfung, 20. November 2014, Düsseldorf](#)

[Prüfung der Arbeitsplatz- und Unternehmenssicherheit, 26. November 2014, Köln](#)

[Jahrestreffen IT-Revision, 27.-28. November 2014, Köln](#)

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

Checklisten-Download und Banken-Times Archiv online

Für alle Bücher aus der Reihe unserer „**Bearbeitungs- und Prüfungsleitfäden**“ stellen wir die enthaltenen Checklisten auf unserer Webseite unter „[Mein FCH](#)“ als veränderbare WORD-Datei zum Download zur Verfügung. Den Zugangscode finden Sie im Buch.

Zusätzlich stehen im Bereich „Mein FCH“ auch alle erschienenen **Banken-Times** und Banken-Times SPEZIAL Ausgaben als PDF zum Download bereit.

Aufbau eines Soll-Rollenkonzepts

Als Fortsetzung zu dem Beitrag „Facetten der IT-Berechtigungen“ in der Ausgabe Januar & Februar 2014 geht es jetzt darum, das Thema **anwendungsübergreifendes Soll-Rollenkonzept** zu erarbeiten und dieses Soll-Rollenkonzept im Kontext der dafür notwendigen Prozesse zu betrachten. Veränderungen von Berechtigungen an einem Objekt wie zum Beispiel Mitarbeiter in einem Kreditinstitut finden in der Regel auf zwei Arten statt. Einerseits durch **operative Prozesse**, die durch die Personalabteilung gestartet werden, andererseits infolge **administrativer Prozesse**, die durch Abteilungen IT, Betriebsorganisation, Prozessmanagement, etc. vorgenommen werden.

Bei den operativen Prozessen erhalten Mitarbeiter/innen neue Berechtigungen oder bestehende Berechtigungen werden entzogen. Dies geschieht zum Beispiel bei der Neuanlage, Eintritt von Auszubildenden, der Versetzung, Mitarbeiter/in wechselt von der Betriebsorganisation in die DV-Revision oder der längerfristigen Abwesenheit durch Anlässe wie Mutterschutz, Elternzeit, unbezahlter Urlaub oder Krankheit. Weitere Prozesse wären eine Namensänderung, der Wiedereintritt oder der Austritt eines Mitarbeiters/in. In allen genannten Fällen verwendet die Personalabteilung hierzu vorhandene, in einem Organigramm hinterlegte Stellen. Diese Stellen bestehen aus einer eindeutigen Stellennummer, einer Stellenbezeichnung sowie einer Stellenbeschreibung. Diese Stellen sind wiederum Abteilungen zugeordnet. Den Stellen sowie Abteilungen sind Berechtigungen zugeordnet. Somit beschränkt sich die **Aufgabe der Personalabteilung** darauf, einen Mitarbeiter auszuwählen und zu einem terminierten Datum diesem **Mitarbeiter/in eine Stelle zuzuordnen oder zu entfernen**. Gegebenenfalls erfolgt die Freigabe eines operativen Prozesses durch ein aktiviertes 4-Augen-Prinzip. Welche Berechtigungsbearbeitungen vorzunehmen sind, ergibt sich aus den Berechtigungen, die der Stelle bzw. der Abteilung zugeordnet wurden. Neben den Stellen- und Abteilungsrechten erhält der Mitarbeiter/in auch noch Institutsrechte.

Durch **Release Änderungen**, in der Regel zweimal im Jahr zum Beispiel durch das Rechenzentrum, wird dem Kreditinstitut mitgeteilt, dass **neue Berechtigungen** hinzu gekommen sind oder in wenigen Fällen auch bestehende Berechtigungen entfernt werden. Diese neuen Rechte müssen den Objekten wie Stelle, Abteilung oder Institut zugeordnet werden. Dies geschieht über administrative Prozesse, das heißt eine Person startet die Rechteänderung an einer Stelle und übergibt die Genehmigung an eine zweite Person bzw. Abteilung. Dies kann eine zentrale Abteilung aber auch die Fachabteilung sein. Bei positiver Entscheidung erfolgt dann die Umsetzung durch den verantwortlichen Rechtheadadministrator.

Damit diese operativen als auch administrativen Prozesse ausgeführt werden können, bedarf es eines anwendungsübergreifenden Soll-Rollenkonzeptes.

Beim **Aufbau eines anwendungsübergreifenden Soll-Rollenkonzeptes** wird festgelegt, welche Datenquelle als Basis herangezogen wird. Bei der ersten Variante werden die hierzu notwendigen Informationen wie Stellen und Abteilungen bzw. organisatorische Einheiten aus der Kernanwendung als Basis herangezogen. Bei der zweiten Variante werden die Daten aus dem Personalsystem exportiert. Bei den meisten Kreditinstituten ist eine Synchronisation, heißt automatischer Abgleich der Stellen und Abteilungen, zwischen dem Kernbankensystem und dem Personalsystem noch nicht erfolgt und somit nicht aktiv. Diese Maßnahme kann als Vorarbeit für die Implementierung eines Soll-Rollenkonzeptes sehr sinnvoll sein.

Hilfreich ist desweiteren die Anwendung von **Stellenschablonen**. Hierbei werden „Standardstellen“ definiert zum Beispiel Markt- oder Stabsstellen, auf deren Basis dann Stellen

angelegt werden. Vorteil, alle den Stellenschablonen zugeordneten Rechte werden auf die Stellen vererbt. Ändert man eine Stellenschablone, so wird die Änderung an einer zentralen Stelle wie zum Beispiel an einer „Stellenschablone Kassierer“ vorgenommen und auf alle im produktiven Einsatz befindlichen Kassierer Stellen übertragen.

Einzelrechte wie zum Beispiel Kontodaten lesen, ändern oder löschen werden nicht den Objekten direkt zugeordnet, sondern man definiert in den jeweiligen Anwendungen **Profile**. Diese Profile beinhalten mindestens ein Einzelrecht, in der Regel aber mehrere Einzelrechte. Die Profile werden anhand der Aufgabengebiete definiert. Anhand der Profilnamen sollte man direkt erkennen können, für welches Aufgabengebiet das Profil gebildet wurde, zum Beispiel Controlling, Markt Privatkunden, Vertriebssteuerung, etc. Sinnvoll ist auch den Profilen eine kurze Beschreibung beizufügen, dies kann beim Prozess der Rezertifizierung durch die Führungskräfte sehr hilfreich sein. Die Profilnamen bzw. Bezeichnungen sollten auch anwendungsgreifend zum Einsatz kommen. Ein weiterer Vorteil der Verwendung von Profilen ist, dass die Führungskraft sich nicht mit den zum Teil sehr technischen Einzelrechten auseinander setzen muss, die oft nur von den Administratoren verstanden werden.

Wurden die Profile in den einzelnen Anwendungen erstellt, so werden diese Profile im nächsten Schritt den Stellenschablonen zugeordnet. Profile die allen Mitarbeitern einer organisatorischen Einheit vergeben werden können, werden dem Objekt Abteilung zugeordnet. Rechte über die jeder Mitarbeiter verfügt, werden am Objekt Institut festgemacht. Anschließend werden die Stellen auf Basis der Stellenschablonen erstellt und den Abteilungen zugeordnet. Die nun entstandene Rechtestruktur aus Stellenschablonen, Stellen, Abteilung und Institut gilt es nun final im Hause abzustimmen bzw. freizugeben. Ist dies erfolgt, können die Stellen den Mitarbeitern zugewiesen werden. Rechte die nicht den Objekten Stelle, Abteilung oder Institut zugeordnet werden können, aber ein Mitarbeiter/in benötigt, werden am Objekt „Mitarbeiter“ festgemacht. Auf Basis dieses anwendungsübergreifenden **Soll-Rollenkonzeptes** können dann die operativen als auch die administrativen Prozesse ausgeführt werden. Zusätzlich kann ein Mitarbeiter als auch ein Vorgesetzter Rechte beantragen, über die eine Person noch nicht verfügt. Der Beantragungsprozess entscheidet dann, ob das Recht dem Mitarbeiter direkt zugeordnet wird oder Bestandteil des Soll-Rollenkonzeptes werden wird.

Die **Aktualität** des anwendungsübergreifenden Soll-Rollenkonzeptes wird durch die Prozesse Soll-/Ist-Abgleich, Einlesen des juristischen IST-Bestandes und Abgleich mit dem SOLL durch die Bearbeitung durch den Anwendungseigentümer oder verantwortlichen Administrators und der halbjährlichen bzw. jährlichen Rezertifizierung in Abhängigkeit der Kritikalität der Berechtigungen durch die Führungskräfte sichergestellt.

Roland Hein, Geschäftsführer, bit Informatik GmbH

Seminar- und Buchtipps zum Thema

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

[Vergabe und Kontrolle von IT-Berechtigungen, 25. Juni 2014 in Frankfurt/M.](#)

[2. Fachtagung IT-Sicherheit, 26.-27. Juni in Frankfurt/M.](#)

Aktuelle Buchneuerscheinungen

MaRisk-Prozessänderungen und Projektmanagement

Neue regulatorische Vorschriften in immer kürzeren Abständen sowie erhöhter Konkurrenzdruck bei Kreditinstituten machen eine flexible Aufbau- und Ablauforganisation notwendig. Dabei sind kleinere Anpassungen an Geschäftsprozessen ebenso unerlässlich wie größere Veränderungen im Rahmen von Projekten. Nicht zuletzt durch gestiegene Anforderungen an Neu-Produkt-Prozesse (MaRisk AT 8.1) und betriebliche Anpassungen (MaRisk AT 8.2) ist vielfach ein verbessertes Management von Projekten sowie Anpassungsprozessen erforderlich. [weiter lesen](#)

Bearbeitungs- und Prüfungsleitfaden: Neue MaComp, 3. Auflage

Die Vielzahl an gesetzlichen und aufsichtsrechtlichen Neuregelungen zur Wertpapier-Compliance stellt die Compliance-Funktion im Allgemeinen sowie den Compliance-Beauftragten im Besonderen vor wachsende Herausforderungen. Im Mittelpunkt steht zum einen die WpHG-Mitarbeiteranzeigeverordnung (WpHG-MaAnzV) aufgrund ihrer verschärften § 34d WpHG-Anzeigepflichten mit Blick auf den Einsatz von Mitarbeitern aus der Anlageberatung sowie als Vertriebs- und Compliance-Beauftragter. [weiter lesen](#)

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

Fachbeiträge auf unserem FCH Blog

Auf unserem Blog <http://blog.fc-heidelberg.de/> stellen wir ausgewählte Fachbeiträge unserer Banken-Times und Banken-Times SPEZIAL Newsletter sowie die Praxistipps der Zeitschriften-Artikel kostenlos zur Verfügung.

Übersicht der interessante und aktuelle Fachbeiträge auf unserem Blog:

- [Änderung der regulatorischen Rahmenbedingungen von Banken](#)
- [Erweiterte Berichtspflichten der Internen Revision](#)
- [Regionales Servicecenter – Leistungsbündelung schafft Wettbewerbsvorteile](#)
- [Revisionsseitige Begleitung der Optimierung von Kreditprozessen](#)
- [Risikoanalysen beim Outsourcing](#)
- [Die Rolle von Prozessorientierung und Unternehmenskultur für den Erfolg der Bank](#)

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.