Compliance Management als Herausforderung aus Sicht der Informationstechnologie

Umsetzung der Vorschriften mit gleichzeitiger Flexibilisierung der Geschäftsprozesse

Abstract:
Regulierungen des Compliance Managements, wie sie z.B. aus dem Sarbanes Oxley Act oder Basel II erwachsen, führen zu Anforderungen an die IT vieler Unternehmen, die die Ressourcen der CIO Organisationen überlasten. Der Artikel gibt eine Übersicht über Themen des Compliance Managements und zeigt gleichzeitig Lösungsmöglichkeiten für die beiden genannten Unterthemen, die zu einer deutlichen Verbesserung der Infrastruktur und der Geschäftsprozesse führen und gleichzeitig eine Minimierung der Risiken (auch der persönlichen Haftung) mit sich bringen können. Dazu werden moderne Tools vorgestellt, die sowohl die Informationsinfrastruktur so erweitern, dass sie „compliance-fest“ werden können, als auch eine Verbesserung der bisherigen Gesamtsituation ermöglichen, da die zugrundeliegenden Werkzeuge und Methoden nicht nur Abläufe erleichtern, sondern auch modernes Business Process Management möglich machen.

Inhaltsverzeichnis:

©Dr. Elmar Paul Selbach HCLT GmbH Am Söldnermoos 17 D85399 München-Hallbergmoos
Tel.: +49-89-607-68671 Fax: +49-89-607-68671 elmar.selbach@hclt.de

1. Überblick

Compliance Management ist der Oberbegriff für ethische, gesetzliche und ökologische Normen, die in Firmen und Körperschaften in die Geschäftsprzesse integriert werden müssen. Aus Sicht der IT stellt das Thema Compliance Management eine der größten Herausforderungen für die Umsetzung neuer Vorgaben dar.

2. Unterteilung des Compliance Management

Im wesentlichen besteht Compliance Management aus zwei großen Blöcken, soweit es Geschäftsprozesse betrifft. Zum einen spricht man von Corporate Governance bezogenen Regulierungen, zum anderen von Vorschriften zur Risikominimierung, hier insbesondere bei Finanzgeschäften.

Corporate Governance hat mehrere Ziele:
- Beschreibung und Durchsetzung von Best Practices und gemeinsamer Standards für alle Industrien
- Sicherstellung finanzieller Transparenz
- Übernahme persönlicher Verantwortung durch das Executive Management für alle Fehler und Verletzungen der Sorgfaltspflichten
- Komplette Verfügbarkeit aller relevanten Informationen für Anteilseigner und Behörden
- Korrektheit der herausgegeben Informationen
- Minimierung der möglichen Schäden an der Reputation der Unternehmen

Hier gibt es verschiedene Ansätze für Regelwerke Das derzeit wichtigste und bekannteste dürfte der Sarbanes-Oxley Act sein, der in den USA herausgegeben wurde und alle Firmen betrifft, die dort zur Rechnungslegung verpflichtet sind.

Auch IAS (International Accounting Standard) und IFRS gehören zu den genannten Regelwerken, deren Umsetzung derzeit häufig auf der Agenda der CIOs und CFOs steht. Seltener muss man sich auf Ebene der Geschäftsleitung um Standards wie AZ/NZS 4360:1999 kümmern, der lediglich Australien und Neuseeland betrifft

Risikomanagement betrifft, wie gesagt, mehr die finanzielle Seite des Compliance Managements:
- Primär sind davon Finanzinstitute betroffen, aber auch Unternehmen, die kreditähnliche Geschäfte betreiben
- Ziel ist, alle finanziellen und operativen Risiken eindeutig messbar zu machen und zu zuordnen
- Allen Geschäftspartnern, Anteilseignern und Regulierungsinstitutionen muss eine vollständige Übersicht über eingegangene Verpflichtungen und Risiken, sowohl finanzieller als auch operativer Art, ermöglicht werden
- Es muss eine ausreichende finanzielle Vorsorge auf der Kapitalseite der handelnden Institution getroffen werden, das heißt im wesentlichen, Sicherstellung einer Eigenkapitaldecke, die ausreicht, größere Risiken für Anteilseigner auszuschließen

Die wichtigsten Vorschriften für den Bereich Risikomanagement sind derzeit Basel II, CAD 3 sowie die diversen FSA Vorschriften.

Die beiden oben genannten Themen **Corporate Governance** und **Risikomanagement** sind diejenigen, die derzeit für die IT relevant sind.

Der Vollständigkeit halber sollte aber erwähnt werden, dass auch andere Felder existieren, die zum großen Komplex Compliance Management gehören, aber für die IT derzeit nicht im Vordergrund stehen. Compliance Management ist keinesfalls eng abgegrenzt, hier tauchen ständig neue Vorschriften und Verpflichtungen auf, deren Komplexität hohe Anforderungen an eine flexible und veränderbare IT stellen.

Als Beispiele für die Vielfalt der Regulierungen kann man die „Gruppenfreistellungsverordnung GVO" oder den SA8000 Standard anführen, die zu vollständig neuen Ablaufmodellen (GVO) und stark veränderten Geschäftsprozessen der IT und deren internen „Kunden" in strategischen Kernbereichen geführt haben.
Diese sollen hier aber nur die Breite des Spektrums des Themas Compliance Management andeuten, im weiteren werden sie nicht behandelt.

Gruppenfreistellungsverordnung GVO

Diese Regel basiert auf den Art. 81 und 82 EGV (Vertrag der Europäischen Gemeinschaften) und bezieht sich im wesentlichen darauf, den ungehinderten Warenverkehr in Europa zu ermöglichen. Davon können verschiedene Warengruppen freigestellt werden, die Verkehrsfreiheit kann also eingeschränkt sein. Dies betrifft im wesentlichen den Handel mit Kraftfahrzeugen, bei denen die EU mittlerweile Wettbewerbsverbote außer Kraft gesetzt hat. Für die OEM (Fahrzeughersteller) hat das dazu geführt, dass sie beispielsweise Informationskanäle auch für Fremdanbieter öffnen mussten. Das war zwar nicht die wesentliche Konsequenz aus der Änderung der GVO, brachte aber für die IT erhebliche Änderungen, da z.B. die internen Werkstattinformations- und Dokumentationssysteme umgestellt werden mussten, ein Prozess, der heute noch anhält.

SA8000 Standard:

Dies ist im wesentlichen ein Zertifikat für Handelsunternehmen, die in Ländern der dritten Welt fertigen lassen. Damit verpflichtet sich das betreffende Unternehmen, soziale Mindeststandards einzuhalten, z.B. auf Kinderarbeit zu verzichten und auch nicht mit Firmen zusammenzuarbeiten, die fragwürdige Praktiken einsetzen. Detaillierte Informationen darüber finden sich auf der Webseite: **www.cepaa.org**

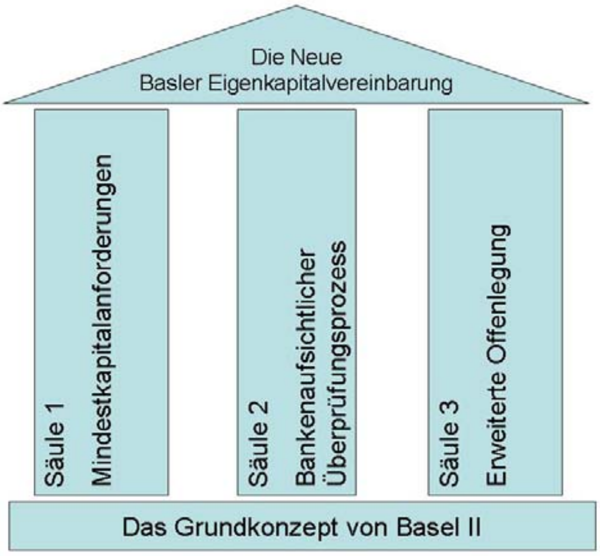
Beide Standards, SA8000 wie GVO, sind derzeit für die IT von untergordneter Bedeutung, wichtig sind Basel II und Sarbanes Oxley.

3. Konsequenzen für die IT und den CIO

Es ist offensichtlich, dass alle diese zu erheblichen Konsequenzen in der IT und auch für die Person des CIO führen.

Am Beispiel der Regulierungen **Basel II** und **Sarbanes Oxley Act** soll dies hier weiter ausgeführt werden.

Basel II ist eine von der Europäischen Zentralbank erlassene Vorschrift mit dem Ziel, finanzielle Risiken aus Bankgeschäften zu minimieren. Einerseits betrifft diese Regel die Banken selbst, die bei der Kreditvergabe die entsprechenden Regeln einhalten müssen, andererseits aber auch ihre Kunden, die Mindestanforderungen an die Kreditwürdigkeit zwingend erfüllen müssen (im wesentlichen die Höhe des Eigenkapitals). (Details finden sich z.B. auf den Webseiten der Deutschen Bundesbank)



Im großen und ganzen sollen Banken und ihre Kunden die Möglichkeit haben, eine holistische (ganzheitliche) Sicht ihrer Finanzen zu erhalten. Dafür müssen Prozesse, Methoden und Richtlinien sowie Implementierungstechniken aufgebaut und sicher gestellt werden, die es erlauben, Risiken firmenübergreifend zu identifizieren, zu analysieren, zu managen und zu berichten.

Dies führt zu neuen Mess- und Bewertungssystemen, Datenhaltungsvorschriften (z.B. müssen Transaktionsdaten 5 Jahre aufbewahrt werden) und Prozessabläufen. Dies sind die Bereiche, die die IT betreffen, die jetzt ihre Prozessabläufe (Schlagwort: ***Business Process Management***) neu gestalten muss und auch weitere und neue Informationen für die für die Bank- und Handelsgeschäfte zuständigen Abteilungen bereit zu stellen hat (Schlagwort: ***Business Intelligence***).

©Dr. Elmar Paul Selbach HCLT GmbH Am Söldnermoos 17 D85399 München-Hallbergmoos
Tel.: +49-89-607-68671 Fax: +49-89-607-68671 elmar.selbach@hclt.de

Dazu benötigt die IT neue Ablaufsysteme für zwei Kernbereiche:

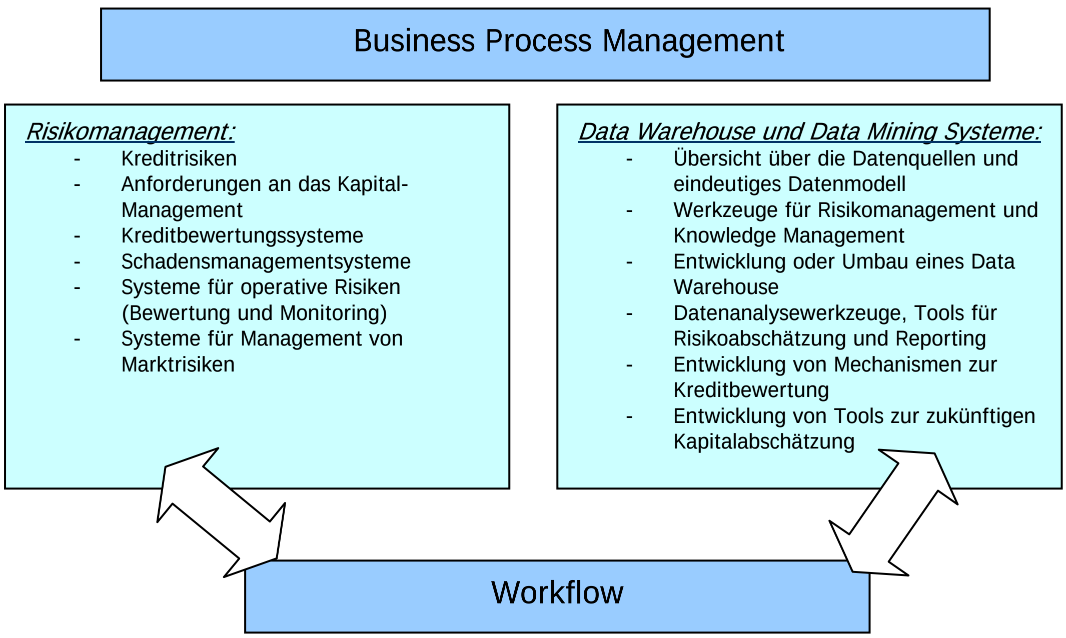
Risikomanagement:

- Kreditrisiken
- Anforderungen an das Kapital-Management
- Kreditbewertungssysteme
- Schadensmanagementsysteme
- Systeme für operative Risiken (Bewertung und Monitoring)
- Systeme für Management von Marktrisiken
- Workflow / Automatisierung von Geschäftsprozessen

Data Warehouse und Data Mining Systeme:

- Kompletter und automatisierter Prozess für die Bereitstellung von Daten
- Übersicht über die Datenquellen und eindeutiges Datenmodell
- Werkzeuge für Risikomanagement und Knowledge Management
- Entwicklung oder Umbau eines Data Warehouse
- Datenanalysewerkzeuge, Tools für Risikoabschätzung und Reporting
- Entwicklung von Mechanismen zur Kreditbewertung
- Entwicklung von Tools zur zukünftigen Kapitalabschätzung
- Business Process Management und Workflow Tools

In beiden Kategorien sind die Werkzeuge für Business Process Management quasi horizontal zu den vertikalen Anforderungen für Risiken und Datenmodelle angeordnet:



Der **Sarbanes Oxley Act** ist, wie bereits gesagt, in den USA als Antwort auf die skandalösen Auswüchse bei der Rechnungslegung einiger großer Konzerne (ENRON Skandal, als Beispiel) entstanden. Die Vorschrift konzentriert sich auf Werte und Prinzipien wie:

- Integrität und Unabhängigkeit
- Verantwortung des Managements
- Sicherstellung der internen Kontrolle
- Transparenz
- Abschreckung, nicht zuletzt durch Strafandrohung

Dazu gehört eine ganze Palette von Einschränkungen und Vorschriften, die sowohl für die IT als auch für das Executive Management als Personen erhebliche Konsequenzen haben.

Für die IT sind folgende Implikationen wichtig:

Die Planungen für die Anpassung der IT Systeme und die damit verbundenen Controlling Werkzeuge richten sich jetzt weniger nach den bisher üblichen linearen Abläufen, sprich: die Funktionalität der IT hatte Vorrang, sondern muss sich auf die vollständige Übereinstimmung mit den Vorschriften konzentrieren.

Ohne vorhergehende tiefgehende Analyse und Bewertung der finanziellen Kontrollsysteme ist das nicht zu bewerkstelligen.
Für einige Kernbereiche ist es zwingend erforderlich, die IT zu zentralisieren, auch wenn dies zunächst zu Schwierigkeiten führt. Letztere führen dann oft zu einer strategischen Neubewertung der gesamten Infrastruktur und Abläufe.

Auch wenn dies bedeutet, kleinere IT Systeme zu einem großen zusammenzulegen, kann dies vorteilhaft sein, wenn gleichzeitig die Geschäftsprozesse umgestaltet werden. Ohne Neumodellierung der Geschäftsprozesse und oft auch ohne neue flexible BPM Tools ist die Steuerung der Prozesse nach der strategischen Neubewertung oft nicht möglich.

Die Anforderungen an Transparenz machen jetzt auch Systeme notwendig, die in Echtzeit, also ohne Verzögerung, auf Anfragen und Reporting Bedarf reagieren. Da auch dies nicht immer vollständig maschinell ablaufen kann, liegt auch hier ein Schwerpunkt auf Geschäftsprozessen und deren Flexibilisierung (und damit auch Umsetzung mit Hilfe von Workflow Tools).

4. Umsetzung der Umstellung in der IT: Top-Down Ansatz

Die Prozesse und Anforderungen variieren von Firma zu Firma, aber es lassen sich Erfahrungen Werkzeuge und Best Practices ableiten, die die Implementierung deutlich beschleunigen und gleichzeitig Risiken abbauen.

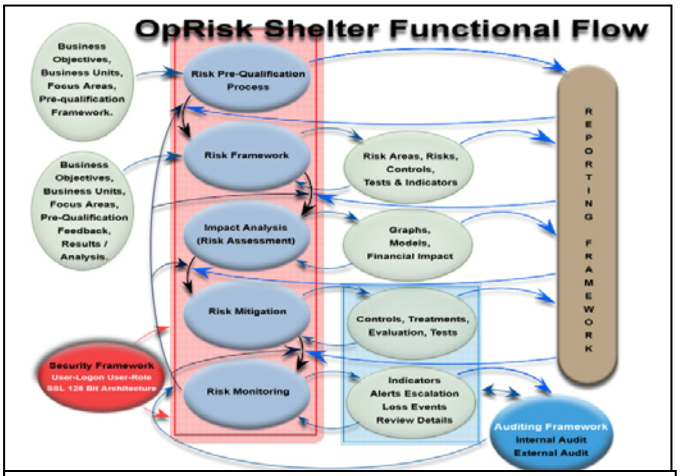


Bild: Übersicht OpRiskShelter™

Dazu hat die Firma HCLT ein sogenanntes „**OpRisk Shelter™**“ entwickelt, das aus einem Framework und wiederverwendbaren Komponenten besteht. Damit lassen sich ad hoc die beiden Säulen 1 (Mindestkapitalanforderungen) und 3 (erweiterte Offenlegung) von Basel II implementieren. Dies sind die beiden Prozesse, die für die IT die wesentliche Herausforderung darstellen.

Neben der Abdeckung der Grundanforderungen aus Basel II bietet dieses Werkzeug offene Schnittsstellen (APIs) und eine Integration mit CIO Dashboards und Standardwerkzeugen.

Damit erreicht man bereits eine erhebliche Genauigkeit und hohe Performanz in der Anpassung der IT an die Anforderungen des Risikomanagements. Eine statische Beschreibung, die der „OpRisk Shelter™“ notwendigerweise darstellt, gibt erst einmal die Sicherheit, mit den Anforderungen klar zu kommen.

Um aber den entscheidenden Schritt zu gehen, aus der Anpassung der Geschäftsprozesse und der IT auch noch einen Gewinn zu ziehen, bietet sich eine grundsätzliche Neubewertung des Denkens über Geschäftsprozesse an, wie sie Fleischmann in seinem Buch über „Distributed Systems“ (Springer 1994) unter dem Paradigma „Subjektorientierte Programmierung“ vorgeschlagen hat.

(Eine Übersicht über „Subjektorientierte Programmierung“ findet sich unter www.brainguide.de in der Rubrik IT*: Dr. Elmar Paul Selbach: „die neuen Werkzeuge des Business Process Managements*“)

5.

Umsetzung auf Ebene der Geschäftsprozesse

Operative Exzellenz und hohe Anpassungsfähigkeit ermöglicht die Ausarbeitung, Überprüfung und sofortige Implementierung des Business Process Managements und des zugehörigen Workflows. Bei diesem Schritt muss man sich als IT-Verantwortlicher allerdings von der Vorstellung verabschieden, dass eine Programmierung des Workflows vorab notwendig ist. Das Gegenteil ist der Fall. Mit fortgeschrittenen neuen Werkzeugen der dritten Generation des Business Process Managements lassen sich die Geschäftsprozesse modellieren, der Workflow ausprobieren und testen, ohne dass die IT erst einmal eingreifen muss. Das ist eine erhebliche Verbesserung gegenüber bisherigen Ansätzen, bei denen die IT vorab bereits erhebliche Ressourcen alleine für die Modellierung zur Verfügung stellen musste. Erst das macht eine Risikominimierung möglich.

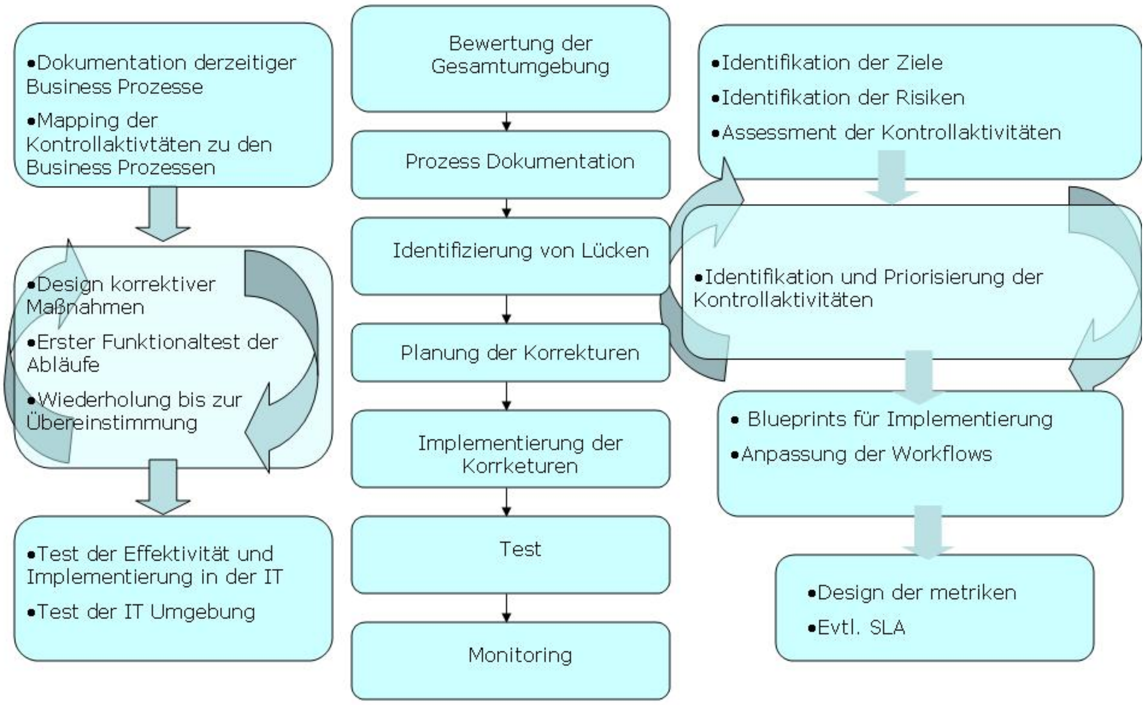


Bild: Dynamisches Business Process Management und Workflow bei Sarbanes Oxley Implementierung mit Hilfe der JPASS Methode

6. Geeignete Werkzeuge

In aktuellen Projekten kommt für die Modellierung der Geschäftsprozesse und den sofortigen Test der Abläufe das Produkt JPASS zum Einsatz, das zum einen aus einem Workflow Management Tools besteht, zum anderen eine Methode für einen effizienten Test und Beschreibung von Geschäftsprozessen bietet.

Bevor eine endgültige Modellierung der Workflows stattfindet, kann man mit JPASS den vorgesehenen Ablauf konsistent erstellen, die Nomenklatur anpassen und überprüfen und abschließend den kompletten Arbeitsablauf ohne Verzögerung testen. Dabei entsteht sofort ein JAVA Code, der als Ausgangsbasis für eine endgültige Version eines Business Prozesses dient, und der mit Hilfe eines UML Tools wie Eclipse anforderungsfest gemacht werden kann.

Der Vorteil der JPASS Methode liegt darin, dass Beteiligte auch ohne Kenntnis von Programmiersprachen oder komplexer BPM Werkzeuge innerhalb weniger Stunden einen kompletten Workflow so gestalten können, wie er den Anorderungen der Aufbauorganisation entspricht und auch die unterschiedlichen Anforderungen verschiedener Abteilungen integriert. Aufgabe der IT ist dann lediglich, die entstandenen Sources (J2EE) in eine dokumentierte und wartbare Form zu bringen.

Der Aufwand für die BPM Modellierung reduziert sich drastisch, denn anstatt in mehreren Wochen, wie bisher, kann ein Modell innerhalb von Stunden fertig stehen.

Damit können die notwendigen Anforderungen und Analysen in einem derart frühen Stadium erfolgen, dass eine Anpassung der Geschäftsprozesse innerhalb der Abteilungen der Aufbauorganisation erfolgen, die letztendlich für die Transaktionen auch die Verantwortung tragen: das sind die Bilanzprüfer oder Vertriebsabteilungen ebenso wie Controlling oder Kreditprüfung, um nur Beispiele zu nennen.

Die IT kommt erst ins Spiel, wenn die Beteiligten wirklich wissen, was sie wollen. Sie kann dann auf Basis des bereits existierenden Codes, der automatisch generiert wird, letztendlich saubere Lösungen so bereitstellen, dass die Kunden der IT sich auch im Bild der Geschäftsprozesse und deren Ablauf wiederfinden.

7.

Zusammenfassung

Es macht keinen Sinn, Compliance Anforderungen als Problem zu betrachten, das kurzfristig zu lösen ist, und nach dessen Lösung man mit dem Tagesgeschäft weitermachen kann.

Tatsächlich sind die Herausforderungen des Compliance Managements derart komplex, dass sie eine völlige Neubetrachtung der Abläufe und Strukturen innerhalb und zwischen Organisationen erfordern. Dazu gehört auch, die IT derart zu strukturieren und zu flexibilisieren, dass sie auch auf neue, noch nicht bekannte Herausforderungen ohne Verzug reagieren kann.

Gerade die Globalisierung dürfte beim Thema Compliance Management noch für einige Überraschungen sorgen, deshalb ist es besser von vorne herein eine ganzheitliche Sicht der Prozesse und Lösungen anzustreben.

Optimisieren der IT setzt voraus, dass die CIO Organisation zunächst einmal die Strukturen der Datenerfassung analysiert. Dies bringt eine robuste Data Warehouse Strategie hervor, mit der sich die Grundforderungen der Finanzabteilungen, des Managements, der Regulierungsbehörden und Anteilseigner nach Transparenz erfüllen lassen.

Mit der Automatisierung von Standardprozessen und der automatisierten Dokumentation derselben sowie der Einführung von flexiblen Workflow-Management Werkzeugen gewinnt die IT dann so viel Spielraum, dass sie gelassen auf neue Anforderungen reagieren kann.

Dazu helfen Werkzeuge und Methoden wie JPASS aber auch Frameworks wie der OpRiskShelter von HCLT, die auf vielfältige Erfahrungen in diesem Bereich zurückgreifen kann.