Berliner Schriften zu modernen Integrationsarchitekturen

herausgegeben von
Prof. Dr.-Ing. habil. Andreas Schmietendorf
Hochschule für Wirtschaft und Recht Berlin, FB II

Band 2

Andreas Schmietendorf (Hrsg.)

4. Hochschul-Roundtable der CECMG/DASMA

Compliance- und Risk-Management
im Kontext komplexer und hoch integrierter
Unternehmensarchitekturen

3. März 2009, Bonn

Shaker Verlag
Aachen 2009

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Printed in Germany.

ISBN 978-3-8322-8135-9
ISSN 1867-7088

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Vorwort

Die Berücksichtigung des Compliance- und Risiko-Managements im Kontext von modernen Integrationsarchitekturen stellt eine ambitionierte Herausforderung für am Markt agierende Unternehmen dar. Allgemein kann unter Compliance-Management der Umgang mit einzuhaltenden Gesetzen und Regeln verstanden werden. Die enge Wechselwirkung zum Risiko-Management ergibt sich aus der einhergehenden Möglichkeit, Auswirkungen ggf. verletzter Compliance-Anforderungen im Sinne von Risiken identifizieren und bewerten zu können. Aspekte des Compliance-Managements beziehen sich unter anderem auf die Gestaltung von Geschäftsprozessen, genutzte Informationsobjekte, beteiligte Organisationseinheiten, die Vertragsgestaltung bzw. -überwachung genutzter IT-Services, aber auch auf die verwendete technische Infrastruktur. Eine besondere Herausforderung stellt daher das notwendige Zusammenwirken von juristisch-, wirtschaftlich- und technologisch orientierten Unternehmenseinheiten dar.

Mehr als 20 Teilnehmer aus dem industriellen und akademischen Umfeld beschäftigten sich im Rahmen des 4. Hochschul-Roundtables mit der Themenstellung des Compliance- und Risiko-Managements. Veranstaltet wurde der Roundtable von der Hochschule für Wirtschaft und Recht Berlin – Fachbereich II Wirtschaftsinformatik/Systementwicklung in Kooperation mit dem Software Messlabor der Otto-von-Guericke-Universität Magdeburg sowie der Central Europe Computer Measurement Group (cecmg) und der deutschsprachigen Anwendergruppe für Software-Metrik und Aufwandschätzung (DASMA). Als kompetenter Gastgeber konnte die Deutsche Telekom AG – Zentrale Bonn gewonnen werden.

Ziel war es, die vielfältigen Inhalte des Compliance Managements zu identifizieren, ggf. branchenspezifische Besonderheiten herauszuarbeiten und Wechselwirkungen zum Risk-Management aufzuzeigen. Im Mittelpunkt der Betrachtung standen dabei mittelständische und große Unternehmen. Darüber hinaus erfolgte eine primäre, aber nicht ausschließliche Orientierung auf IT-bezogene Themenstellungen. In diesem Zusammenhang wird typischerweise von IT-Compliance-Management gesprochen. Auf eine Unterscheidung zwischen der Informationstechnologie als Träger der Compliance-Anforderungen bzw. der Informationstechnologie als Mittel zur Unterstützung der Aufgaben des Compliance-Managements wurde bei der Initiierung des Roundtables bewusst verzichtet.[1]

Zur Anregung der Diskussion konnten erfahrene Referenten aus dem industriellen Kontext gewonnen werden, wobei die vorgetragenen Themenstellungen bewusst disjunkt gewählt wurden.

[1] Vgl. Klotz, M.; Dorn, D.-W.: IT-Compliance – Begriff, Umfang und relevante Regelwerke, in Praxis der Wirtschaftsinormatik, HMD Heft 263, dpunkt.verlag, Heidelberg 2008

Auf dieser Grundlage sollte der „Blick über den Tellerrand“ ermöglicht, Diskussionen provoziert bzw. das Übertragen von Erfahrungen aus anderen Wissensgebieten forciert werden.

Im Einzelnen beschäftigten sich die Vortragenden mit den folgenden Themen:

- Dr. Frank Simon, SQS Software AG (Leiter Research & Innovation)

  Lizenzkonforme Open-Source Verwendung als Teil eines 360°-Qualitätsmanagements

- Wolfgang Behrendt, atmicon GmbH (Geschäftsführer)

  Compliance-Anforderungen beim IT-Service Management

- Dr. Ulrich Paschen, IQ Institut GmbH (Geschäftsführer)

  Compliance-Anforderungen im klinischen Umfeld

- Carsten Alexander Schirp KPMG AG (Advisory Manager)

  Ansatz zur Integration von Compliance und Zertifizierungsanforderungen in IT-Dienstleistungsunternehmen

- Jürgen Bach, bach consulting GmbH (Geschäftsführer)

  Lohnen sich die Aufwände für Compliance in Unternehmen?

- Anne Rode, IBM Deutschland GmbH (Senior Managing Consultant)

  Enterprise Risk Management

Im vorliegenden Tagungsband finden sich ausgewählte Beiträge, welche den Compliance-Aspekt in den Mittelpunkt der Betrachtung gestellt haben. Eine kurze Übersicht zu den Inhalten aller Beiträge des Roundtables findet sich im einführenden Beitrag des Herausgebers. Neben den ausgewählten Vorträgen des Roundtables wurde ein weiterer Beitrag zur Themenstellung des *Identity-Managements* von Herrn Prof. Dr. Gerd Rossa, Geschäftsführer des Instituts für System-Management GmbH aufgenommen. Der korrespondierende Vortrag wurde auf der Jahrestagung der cecmg in Königswinter im April 2009 gehalten.

An dieser Stelle sei noch einmal allen Referenten, Autoren und Teilnehmern herzlich gedankt, die zum Gelingen des Roundtables beigetragen haben.

Ein besonderer Dank gilt den Sponsoren! Ohne die Firmen *atmicon GmbH - Pulheim*, *bach consulting GmbH - Hennef*, *Deutsche Telekom AG - Bonn*, *IQ Institut GmbH - Hamburg*, *IT Architekturbüro - Hamburg*, *KPMG AG - Köln*, *SQS Software Quality Systems AG – Köln* wäre weder die Durchführung des Roundtables noch die Drucklegung dieses Tagungsbandes möglich gewesen wäre. Korrespondierende Kurzreferenzen zu den beteiligten Sponsoren finden sich in den Anlagen zum Tagungsband.

Ein spezielles Dankeschön geht an den Gastgeber des Roundtables, Herrn Martin Rothaut von der Deutschen Telekom AG - IT-Management Group Headquarters and Shared Services (GHS) in Bonn. Seine Verantwortung für die SOX-Einführung bei der GHS bzw. seine langjährige Beschäftigung mit der Themenstellung des Compliance- und Risk-Managements innerhalb des Telekom-Konzerns haben die Durchführung eines derartigen Roundtables überhaupt erst ermöglicht. Natürlich gilt ihm auch Dank für die Bereitstellung eines „wirklichen Roundtables“[2] in der Zentrale des Telekom-Konzerns und die Organisation des ausgezeichneten Caterings.

Ebenfalls bedanken möchte ich mich bei Herrn Michael Wipprecht von der T-Systems Enterprise Services GmbH - System Integration in Berlin für die Unterstützung der Vor- und Nachbereitung des Roundtables.

Ein spezieller Dank geht einmal mehr an Frau Leany Maaßen vom Shaker Verlag Aachen für ihre schnelle und unkonventionelle redaktionelle Unterstützung bei der Erstellung dieses Ergebnisberichts.

Berlin, Mai 2009

Andreas Schmietendorf

[2] entsprechende Fotos sind in den Anlagen zu finden

Kontakt zum Herausgeber:

Prof. Dr.-Ing. habil. Andreas Schmietendorf

HWR Berlin, Berlin School of Economics and Law
Fachbereich II – Wirtschaftsinformatik/Systementwicklung
Neue Bahnhofstraße 11-17
10245 Berlin
Telefon: +49-(0)3375-216195
Fax: +49-(0)30-29384401

E-Mail: andreas.schmietendorf@hwr-berlin.de
URL: http://userpage.hwr-berlin.de/~schmiete

Geleitwort des Gastgebers

Compliance und Risikomanagement sind in den letzten Jahren zu einem bedeutenden Faktor im Umfeld komplexer und hoch integrierter Unternehmensarchitekturen geworden. Der Begriff Compliance wird unter anderem im Best Practice Standard „IT Infrastructure Libary Version 3 (ITIL V3 ®) als „die Einhaltung sämtlicher externer und interner Vorgaben" definiert. Führende deutsche Unternehmen sind in den letzten Jahren immer wieder durch fehlende Compliance oder falsches Risikomanagement ins Straucheln geraten.

Unternehmen wie Deutsche Telekom AG sind von einer Reihe von Gesetzen, internen und externen Regelungen sowie nationalen und internationalen Standards in Hinsicht auf eine erfolgreiche Erreichung ihrer Geschäftsziele abhängig. Neben gesetzlichen Vorgaben, wie Regelungen aus dem Bundesdatenschutzgesetz oder dem Telekommunikationsgesetz, sind vor allem Vorgaben aus finanz- und betriebswirtschaftlichen Regelwerken, wie dem Sarbanes Oxley Act, für den Unternehmenserfolg bedeutsam geworden. Die Einhaltung dieser Vorschriften bedeutet nicht nur eine Verringerung betriebswirtschaftlicher Risiken sondern vielmehr auch eine Erhöhung des Unternehmenswertes. Es wird die Qualität der Berichterstattungen erhöht, die Unternehmenstransparenz nachhaltig gefördert und die Sicherheit unternehmenswichtiger Assets verbessert.

Konkret bedeutet Compliance für die Deutsche Telekom AG die Einhaltung gesetzlicher Anforderungen und konzerninterner Regelwerke. Ziel ist es, Haftungsrisiken sowie sonstige Rechtsnachteile für das Unternehmen, seine Mitarbeiterinnen und Mitarbeiter und Organe zu vermeiden. Es werden allerdings im Konzern Standards angestrebt, die nicht nur die Einhaltung von Gesetzen oder Verordnungen zugrunde legen. Es soll vielmehr ein Umfeld geschafft werden, in dem sich alle Mitarbeiterinnen und Mitarbeiter bei ihrer täglichen Arbeit an ethische Verhaltensgrundsätze halten. Deutsche Telekom AG, als Beispiel für viele international fungierende Unternehmen, müssen heute schon unzählige Anforderungen aus unterschiedlichen Standards und Gesetzen erfüllen. Dabei ist der Erhalt dieser Compliance im Unternehmen als besondere Herausforderung hervorzuheben. Unternehmen verändern sich und erschließen beispielsweise neue Geschäftsfelder. Daraus ergeben sich neue Anforderungen an den Erhalt der Compliance. Auch ohne Veränderung des Unternehmens ergeben sich regelmäßig neue Anforderungen an die Compliance. Gesetze, regulatorische Bestimmungen und Vorgaben nehmen stetig zu. In naher Zukunft werden auf die Compliance von Unternehmen erneut zusätzliche Anforderungen, wie beispielsweise aus dem Bilanzmodernisierungsgesetz (BilMoG), das verschieden EU-Richtlinien in deutsche Gesetzgebung umsetzt, zukommen. Compliance in Unternehmen kann also als lebendiger, nie endender Prozess gesehen werden, der im Unternehmen etabliert und gelebt werden muss.

Compliance umfasst in der Regel alle Unternehmensbereiche. Die IT stellt sich im modernen Unternehmen als Hilfsmittel, Bestandteil oder Kernelement fast aller Geschäfts- und Verwaltungsprozesse dar. Damit ist ein fundamentaler Bestandteil der Compliance auch die IT-Compliance. Defizite in der IT-Compliance gefährden die Gesamt-Compliance eines Unternehmens nachhaltig. Als typische Beispiele sind hier SOX oder der Bereich Datenschutz zu nennen. Die IT-Compliance fokussiert sich dabei hauptsächlich auf die Aspekte Vertraulichkeit, Verfügbarkeit und Integrität von Daten. Die Bedeutung eines sicheren und verantwortlichen Umgangs mit jeglicher Art von Daten wird auch in Zukunft ein Kernthema der IT in Unternehmen werden bzw. bleiben. Diese Entwicklung zeichnet sich auch in den Bestrebungen der „International Organization for Standardization“ (ISO) ab. Für das zweite Quartal 2010 ist der Standard ISO 29100 „A privacy framework“ angekündigt, der den Schutz privater Daten thematisiert.

Im Bereich der IT-Compliance stehen uns jedoch schon heute geeignete Werkzeuge und Standards zur Verfügung, um den gegeben Anforderungen zu begegnen. Hier werden im Bereich der Deutschen Telekom AG neben diversen Sicherheitsstandards der ISO auch Werkzeuge und Best Practices wie „IT Infrastructure Libary“ (ITIL®) oder „Control Objectives for Information and Related Technology (CobiT®)“ zur Sicherstellung von Zielen eingesetzt. Der Einsatz dieser standardisierten Werkzeuge und Vorgehensmodelle erleichtert es, Compliance in einer derart komplexen und integrierten Unternehmensarchitektur mit unzähligen regulatorischen Anforderungen konzernweit zu schaffen.

Dieser Roundtable zum Thema „Compliance- und Risk-Management im Kontext komplexer und hoch integrierter Unternehmensarchitekturen“ stellt diesen Aspekten folgend die IT-Compliance in den Mittelpunkt der Vorträge. Wir sind froh, die Plattform für diesen Roundtable bieten zu können. Unser Dank gilt in den Referenten, die durch ihre interessanten Vorträge diese Veranstaltung erst ermöglichten und neue Sichtweisen bei allen Teilnehmern anregten.

Unser besonderer Dank gilt Herrn Prof. Dr. Andreas Schmietendorf, HWR Berlin, für die inhaltliche Organisation und Abstimmung des Roundtables. Wir bedanken uns bei allen Mitwirkenden, die durch ihre fundierten Diskussionen und Ergänzungen zu dem beigetragen haben, was einen Roundtable ausmachen sollte. Wir wünschen Ihnen viel Erfolg bei der Ausgestaltung der Anregungen, die Ihnen dieser Tagungsband hoffentlich mit in den beruflichen Alltag gibt.

Bonn, März 2009

Martin Rothaut

Gastgeber des 4. Hochschul-Roundtables

Inhaltsverzeichnis