

Vorwort zur Teilkonferenz

IT-Risikomanagement: IT-Projekte und IT-Compliance

Prof. Dr. Günter Müller

Institut für Informatik und Gesellschaft,
Abteilung Telematik
Universität Freiburg i. Br.
Friedrichstr. 50
79098 Freiburg
mueller@iig.uni-freiburg.de

Prof. Dr. Wolfgang König

Institut für Wirtschaftsinformatik
und E-Finance Lab
Goethe-Universität Frankfurt
Mertonstr. 17
60054 Frankfurt
wkoenig@wiwi.uni-frankfurt.de

Der betriebliche Einsatz von IuK-Technologie bedeutet für Unternehmen nicht nur eine Möglichkeit, Geschäftsprozesse zu optimieren und ihre Produktivität zu steigern, sondern auch zunehmend ein Risiko. Die steigende Komplexität der Informationssysteme, der technologische Wandel sowie vielfältige interne und externe Angriffe reduzieren deren Verfügbarkeit, Integrität und Vertraulichkeit. Darüber hinaus verlangen die aktuellen regulatorischen Anforderungen zu Compliance ein umfassendes IT-Risikomanagement in den Unternehmen. Hierzu gehören unter anderem das betriebliche Kontinuitätsmanagement, das Management der Informationssicherheit sowie das Management der Betriebs-, Projekt- und strategischen Risiken. Die Verfügbarkeit jederzeit aktueller und unternehmensweiter Informationen über die Risikolage erfordert eine Bewertung von u. a. informatischen und organisatorischen Maßnahmen unter ökonomischen Gesichtspunkten, wodurch die Verbindung zur Unternehmenssteuerung geschaffen wird. Die damit verbundenen Herausforderungen und Lösungsansätze stehen im Fokus der Teilkonferenz „IT-Risikomanagement“.

Die Beiträge reflektieren das weite Spektrum, das mit dem Management von IT-Risiken verbunden ist. In seinem Beitrag „Fehlschläge bei IT-Großprojekten der Öffentlichen Verwaltung – ein Beitrag zur Misserfolgsvorschau in der Wirtschaftsinformatik“ greift Peter Mertens eine rhetorische Vorlage von Henry Lucas auf und zeigt die Ursachen für die Misserfolge von IT-Projekten im öffentlichen Sektor. Die Identifikation von Erfolgs- und Risikofaktoren sind ebenfalls Gegenstand des Beitrags von Stefanie Betz und Juho Mäkiö, während Roland Gabriel et al. ein Modell zur Analyse organisatorischer Veränderungen und deren Rückwirkung auf die IT-Compliance vorstellen.

Heinz Lothar Grob et al. liefern einen Beitrag zur Entscheidungsunterstützung, wie viel in IT-Sicherheit investiert werden sollte, indem sie zeigen, wie Investitionen in IT-Sicherheit bewertet werden müssen. Die Flexibilität von Geschäftsprozessen und deren

Unterstützung durch IT ist Ausgangspunkt für den Beitrag von Stefan Sackmann, der zu Recht darauf verweist, dass sich die Beziehungen von IT zu den Geschäftsprozessen im Fluss sind und mit diesem Wandel eine Veränderung des IT-Risikos einhergeht. Schwachstellen sind das technische Gegenstück zu der von Sackmann identifizierten Dynamik. Lutz Lowis zeigt Methoden und Grenzen, der automatisierten Erkennung von Schwachstellen für Service-orientierte Architekturen.

Dimitris Karagiannis schlägt in einer zu den bisherigen Ausführungen übergeordneten Form ein Meta-Modell vor, das das Zusammenspiel von Geschäftsprozessen und dem Management von IT-Compliance nachvollziehbar abbildet. Mit wissenschaftlich demselben Ziel, konzipieren Christoph Brandt et al. ein mathematisches Modell zur Beurteilung von IT-Risiken, indem sie die IT-Infrastruktur in graphentheoretischer Form abstrahiert darstellen. Die Gemeinsamkeit zu der Arbeit von Kioumars Namiri und Nenad Stojanovic ist der Bezug auf ein formales Rahmenwerk, unterschiedlich ist die formale Definition von regelkonformen Geschäftsprozessen. Abweichungen davon bestimmen das Risiko.

Das Management von IT-Risiken stellt sich als ein offenes und außerordentlich viel versprechendes Forschungsgebiet der Wirtschaftsinformatik dar. Methodisch ist die Interdisziplinarität offensichtlich und es zeigt sich sehr rasch, dass die formale Erfassung auf Grenzen stößt und manuelles Eingreifen und menschliches Entscheidungsvermögen erforderlich bleibt. Trotzdem sind auch die formalen Verfahren und Methoden noch weiter zu verbessern, und die Beiträge haben die Richtung dazu gewiesen, damit ein betriebswirtschaftlich sinnvolles Management der IT-Risiken möglich wird. Die Beiträge zur Teilkonferenz zeigen, dass die Wissenschaft die Herausforderungen in kreativer Weise annimmt und zu originellen und viel versprechende Lösungsansätzen fähig ist.

Ein besonderer Dank für ihren Beitrag zum Gelingen des Tracks „IT-Risikomanagement: IT-Projekte und IT-Compliance“ gilt den Mitgliedern des Programmkomitees Prof. Dr. H. U. Buhl (Uni Augsburg), Prof. Dr. H. Federrath (Uni Regensburg), Prof. Dr. R. Grimm (Uni Koblenz), Prof. Dr. M. Keil (Georgia State University), PD Dr. D. Kundisch (Uni Freiburg i. Br.), Dr. M. Reichenbach (Commerzbank AG) und Frank Romeike (RiskNET GmbH).

Dezember 2007,

Prof. Dr. Günter Müller und Prof. Dr. Wolfgang König