Risk Management, Compliance und Governance für widerstandsfähige Informationssysteme

Vorwort

Widerstandsfähige Informationssysteme sind in der Lage, unvorhergesehene Ereignisse abzufedern. Auf Grund der Komplexität, Dynamik und Interkonnektivität moderner Informationssysteme ist es weder möglich, alle potenziellen Risiken zu identifizieren noch erkannte Risiken in ihrem vollen Umfang zu steuern. Wettbewerbsfähige Informationssysteme müssen die oftmals hohen Anforderungen der Verfügbarkeit, Integrität und Vertraulichkeit auch nach Eintritt unerwarteter Ereignisse noch erfüllen können. CIOs sind daher gefordert, die Leistungsfähigkeit ihrer Informationssysteme trotz unerwarteter Ereignisse zu sichern.

Die aktuelle Wirtschaftslage zeigt anschaulich, dass zurzeit mit Risiken noch nicht effektiv genug umgegangen wird. Das Ziel muss es daher sein, zukünftig das Ausmaß von Schäden durch effektive Maßnahmen zur Risikoeliminierung und -reduktion zu verringern. Problematisch ist hier die ganzheitliche Integration in die vorhandene Organisationsstruktur, da isoliertes Risikomanagement keine Verknüpfungen und Auswirkungen zwischen verschiedenen Risikobereichen im Unternehmen aufzeigen kann.

Regulatorische Anforderungen verpflichten Unternehmen zur Einhaltung von Verhaltensgrundsätzen, Gesetzen und Richtlinien. So müssen einerseits Auflagen durch Vorschriften und Gesetze berücksichtigt werden, andererseits spielen freiwillige, durch Wertvorstellungen, Moral und Ethik festgelegte, interne Grundsätze eine besondere Rolle. Neben Maßnahmen zur Überwachung der Einhaltung der aufgestellten Vorgaben muss ein generelles Verständnis für Risiken unternehmensweit etabliert werden.

Im Rahmen der IT-Governance müssen Compliance-Vorgaben, Risikosteuerung und Risikoüberwachung umgesetzt und in die Unternehmensstruktur und -prozesse integriert werden. Herausforderungen an das Risikomanagement umfassen die Identifikation und Quantifizierung von Risiken für Informationssysteme. Hierfür müssen Risikoinformationen zeitnah und detailliert bereitgestellt werden, aus denen adäquate Steuerungsmaßnahmen abgeleitet werden können.

Die für diesen Workshop akzeptierten Beiträge können in zwei Kategorien unterteilt werden. Die erste Kategorie umfasst Beiträge, die eine integrative Perspektive auf das Thema GRC vermitteln. Benjamin Schwering und Alexander Pellengahr untersuchen den stark regulierten Bankensektor und beurteilen die Relevanz von Prüfungsstandards für IT-Auslagerung. Patrick Wolf und Matthias Goeken analysieren die noch unzureichende Integration des IT-Risikomanagements in ein unternehmensweites Risikomanagement. Nicolas Racz, Edgar Weippl und Andreas Seufert untersuchen den Einsatz von Risikomanagement-Frameworks auf Gemeinsamkeiten und Rationierungspotenziale.

Die zweite Kategorie umfasst die organisatorische Einbettung und Anwendung von Governance, Risk Management und Compliance. Konrad Walser untersucht die Beziehungen zwischen IT-Governance und dem Unternehmensarchitekturmanagement und fokussiert auf deren Nutzen für die Sicherstellung des Business-IT-Alignment. Manfred Pauli, Michael Schermann und Helmut Krcmar schlagen einen Ansatz für die Verzahnung von IT-Risikomanagement und Unternehmensarchitekturmanagement zur Verbesserung der Informationsgrundlage des IT-Risikomanagements vor. Silvia Knittl und Wolfgang Hommel verdeutlichen den Einsatz von Cloud-basierten Diensten im Umfeld von Hochschulen und stellen die damit verbundenen Risiken vor.

Die vorliegenden Beiträge zeigen die aktuelle Forschung in den Bereichen Risk Management, Compliance und Governance. Unser Dank gebührt den Mitgliedern des Programmkomitees, Herr Prof. Dr. Matthias Goeken, Herr Prof. Dr. Hannes Federrath, Herr Prof. Dr. Knut Hildebrand, Herr Christian Martini und Herr Robert Kamrau für die Unterstützung des Workshops. Ebenso danken wir den vielen Gutachtern, die durch kritische, aber konstruktive und umfangreiche Begutachtung der Beiträge den Autoren wertvolle Hilfestellungen bei der Weiterentwicklung ihrer Ansätze geliefert haben. Wir bedanken uns ebenso bei Frau Alexandra Gerstner, Herrn Prof. Dr. Ing. habil. Klaus-Peter Fähnrich und Herrn Prof. Dr. Bogdan Franczyk sehr herzlich für ihre Unterstützung und die Organisation der Informatik 2010.

Es bleibt zu hoffen, dass die Ideen und Konzepte zu Governance, Risk Management und Compliance für widerstandsfähige Informationssysteme von Wirtschaft und Wissenschaft aufgegriffen werden und neue Potenziale und Forschungsfelder erschlossen werden können.

Dr. Michael Schermann
Prof. Dr. Helmut Krcmar

Programmkomitee

Christian Martini, Siemens AG
Robert Kamrau, IBM Deutschland GmbH
Prof. Dr. Matthias Goeken, Frankfurt School of Finance & Management
Prof. Dr. Hannes Federrath, Lehrstuhl Wirtschaftsinformatik 4, Universität Regensburg
Prof. Dr. Knut Hildebrand, Fachbereich Wirtschaft, Hochschule Darmstadt