

## Informatik 2010 | Service Science – Neue Perspektiven für die Informatik

### **Risk Management, Compliance und Governance für widerstandsfähige Informationssysteme**

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 möglicher Ereignisse zu sichern.

Das Ziel dieses Workshops ist es, aktuelle Forschungsergebnisse aus den Bereichen des IT-Risk Managements, der IT-Compliance sowie der IT-Governance zu bündeln und Ansatzpunkte für Methoden und Werkzeuge zur Entwicklung und für den Betrieb widerstandsfähiger Informationssysteme zu identifizieren.

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.

Compliance-Maßnahmen verpflichten Unternehmen auf die Einhaltung von Verhaltensmaßregeln, Gesetzen und internen Richtlinien. Einerseits müssen Auflagen durch Vorschriften und Gesetze eingehalten werden, andererseits spielen freiwillig durch Wertvorstellungen, Moral und Ethik festgelegte interne Grundsätze eine besondere Rolle. Neben Maßnahmen zur Überwachung der Einhaltung der aufgestellten Maßregeln muss ein generelles Verständnis unternehmensweit etabliert werden. Hauptherausforderung hier ist die Etablierung einer grundlegenden, einheitlichen Beschreibungssprache für Compliance-Informationen.

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.

#### **Mögliche Themen für Beiträge**

Im Rahmen des Workshops werden aktuelle Forschungsarbeiten und Herausforderungen in der Praxis zum Thema Governance, Risk Management und Compliance (GRC) vorgestellt und diskutiert. Das Themenspektrum des Workshops umfasst folgende Punkte, ist jedoch nicht darauf beschränkt:

- Grundlagen und Konzepte widerstandsfähiger Informationssysteme
- Anforderungen, Design und Entwicklung widerstandsfähiger Informationssysteme
- Referenzmodelle und Standards für Risk, Compliance und Governance

- Konzepte, Methoden und Tools für Risikomanagement, Governance und Compliance sowie deren Integration
- Einführung und Betrieb von GRC-Systemen: Erfolgsfaktoren, Trends, Good Practices
- Integrierte interne Kontrollsysteme
- Empirische Befunde bzw. Fallstudien zur Umsetzung von IT-Governance sowie Risk- und Compliance Management
- Modellierung und Analyse der Widerstandsfähigkeit, Risiken und potenziellen Steuerungsmaßnahmen
- Integration von GRC in andere Prozesse des Informationsmanagements, z.B. Service Management, Requirements Engineering und Enterprise Architecture Management
- Beschreibung und Austausch von Informationen zu GRC (Sprachen, Modelle)
- Integration von IT-Risikomanagement in ein unternehmensweites Risikomanagement

### **Programmkomitee**

Prof. Dr. Helmut Krcmar, Technische Universität München (Organisator)

Michael Schermann, Technische Universität München (Organisator)

Christian Martini, Siemens AG

Robert Kamrau, IBM (angefragt)

Prof. Dr. Matthias Goeken, Frankfurt School of Finance & Management

Prof. Dr. Hannes Federrath, Universität Regensburg

Prof. Dr. Knut Hildebrand, Hochschule Darmstadt

### **URL**

<http://grc.winfobase.de>