

Neue MaRisk konkretisieren die Anforderungen an das OpRisk-Management!



Finanz Colloquium  
Heidelberg

# Steuerung von IT-Risiken im OpRisk-Management

Anforderungen aus MaRisk-/BAIT und neuem OpRisk-Standardansatz • Steuerungspflichten von IT-Risiken • Prüfungspraxis

## Ermittlung der IT-Risiken nach MaRisk und BAIT – Überleitung in die OpRisk-Steuerung

10:00 - 12:00 Uhr

- Gesetzliche und (neue) aufsichtsrechtliche Anforderungen im Überblick – SREP, MaRisk, BAIT
- Unmittelbare Konsequenzen für das (IT-)Risikomanagement – Ableitung von **Schutzziele**n, **Identifikation** betroffener Anwendungen/Prozesse, Definition von **Sicherheitskonzepten** und regelmäßige **Erfolgskontrollen**
- Häufige **Schwachstellen** – Falsch identifizierte oder unzureichend bewertete IT-Risiken – Keine systematische **Weitermeldung** von Risiken an das Risikocontrolling – **Beispiele** aus aktuellen Prüfungen
- Kriterien zur Auswahl institutsspezifischer quantitativer **Instrumente/Methoden** und Berücksichtigung im Risikomanagementprozess
- Enge Abstimmung des ISB mit dem OpRisk-Management

**Jan Zurek**

Informationssicherheitsbeauftragter  
ReiseBank AG

## IT-Risiken als OpRisk – Konsequenzen für Bewertung und Risikocontrolling

13:00 - 14:45 Uhr

- Definition von Frühwarnindikatoren im operationellen Risiko zur Überwachung und Steuerung
- Erfassung und Überwachung von offenen/akzeptierten (**IT-Rest-**)Risiken und deren Auswirkungen auf Säule II (OpRisk) – Rechtzeitige Erfassung als **OpRisk** bei entsprechender Veränderung
- Bewertung von **Risikoszenarien** – Schwerpunkte und Praxisbeispiele
- Betrachtung von **IT-Dienstleister-Abhängigkeiten** bei der Bewertung von IT-Risiken – Verschärfte Anforderungen an die Bewertung von **Ausstiegsszenarien** und die **prozessorientierte (Risiko-)Analyse**

**Verena Morio**

Senior-Referentin im  
Risikomanagement  
Sparkasse KölnBonn

## Prüfung der Angemessenheit von Steuerungs- und Überwachungsprozessen bzgl. der Steuerung von IT-Risiken im OpRisk-Management

15:15 - 17:00 Uhr

### Dirk Schumann

IT-Risk & -Compliance Manager, CISA /  
CISM / CRISC IT-Risikomanagement  
DZ BANK AG

- Sicherstellung der Integrität, der Verfügbarkeit, der Authentizität und der Vertraulichkeit der Daten bei IT-Systemen und den zugehörigen Prozessen
- Genaue Analyse des Risikomanagement-Prozesses mit Berücksichtigung des Risikoappetits
- Besondere Herausforderungen bei der Risikoinventur hinsichtlich der Identifizierung und Bewertung der IT-Risiken
- Prüfung der Risikoinventur – In welchen Abständen ist eine Prüfung angemessen? – Kriterien zur Risikoinventur
- Häufige Mängel in der Risikosteuerung

Mit freundlicher Unterstützung von:

