

## ***RC131 IT-Risikomanagement in der Praxis***

### **Kurzbeschreibung:**

Nur noch sehr wenige Geschäftsprozesse funktionieren ohne stabile und sichere IT-Systeme. Jedes Unternehmen, muss sich daher mit den Wirkungsszenarien von IT-Risiken auseinandersetzen und sich u.a. mit den folgenden Fragen beschäftigen: Wie werden IT-Risiken identifiziert und vor allem bewertet? Wie werden IT-Risiken präventiv oder zumindest reaktiv gesteuert? Wie kann eine Business-Impact-Analyse fundiert durchgeführt werden? Wie kann die betriebswirtschaftliche Sinnhaftigkeit von Maßnahmen analysiert und simuliert werden? Welche Methoden stellt Ihnen die Werkzeugkiste des Risikomanagements zur Verfügung?

Das Intensiv-Seminar **RC131 IT-Risikomanagement** vermittelt Ihnen fundiertes Wissen zum Aufbau sowie zur Weiterentwicklung eines wirksamen und effektiven IT-Risikomanagementsystems.

Alle Teilnehmer erhalten eine umfangreiche Dokumentation in gedruckter und elektronischer Form. Bei virtuellen Trainings erhalten die Teilnehmer alle Unterlagen im digitalen Format. **Außerdem erhalten alle Teilnehmer das Buch "Stochastische Szenariosimulation in der Unternehmenspraxis – Risikomodellierung, Fallstudien, Umsetzung in R" (Romeike/Stallinger, Springer Verlag 2021)** sowie ein Zertifikat der Risk Academy.

### **Zielgruppe:**

IT-Risikomanager, CISO, CIO, Geschäftsführer, Mitarbeiter aus den Bereichen Informationssicherheit und Security und Interne Revision.

### **Voraussetzungen:**

Grundkenntnisse der Informationssicherheit, Kenntnisse des Tagesgeschäfts von IT-Operations sind von Vorteil.

### **Sonstiges:**

**Dauer:** 2 Tage

**Preis:** 1790 Euro plus Mwst.

### **Ziele:**

Lernen Sie im Workshop **RC131 IT-Risikomanagement** praxiserprobte Werkzeuge zur Umsetzung eines IT-Risikomanagements im Unternehmen kennen. Das Seminar basiert auf verschiedenen Fallstudien und bietet einen effizienten, in der Praxis bewährten und gut strukturierten Einstieg in das Thema. Außerdem erhalten beim virtuellen Training alle Teilnehmer ein einstündiges individuelles Coaching (online oder telefonisch) zur Vertiefung oder zur Klärung konkreter Fragen bei der Umsetzung in der Praxis. Der Schwerpunkt des Trainings liegt auf praxiserprobten Methoden zur Umsetzung eines wirksamen IT-Risikomanagements.

#### Inhalte/Agenda:

- ♦ IT-Risikostrategie
- ♦ Nationale und internationale Standards im IT-Risikomanagement: ISO/IEC 27001, ISO/IEC 27005, ISO 31000:2018, COSO etc.
- ♦ KRITIS-Regulierung, EU-Richtlinie NIS 2 (Network and Information Security 2), Digital Operational Resilience Act (DORA) etc.
- ♦ Prozess des IT-Risikomanagements in der Praxis
- ♦ Werkzeuge und Methoden im IT-Risikomanagement: Kollektionsmethoden, analytische Methoden und Kreativitätsmethoden
- ♦ Aggregation von IT-Risiken in der Praxis (analytische Methoden, Simulationsmethoden)
- ♦ Business Continuity Management (BCM) und Business Impact Analyse (BIA)
- ♦ Maßnahmen zur präventiven und reaktiven Steuerung von IT-Risiken und deren Wirksamkeitsmessung
- ♦ IT-Reifegrad basierend auf NIS 2, ISO 2700x und Risikobewertung
- ♦ IT-Risikomanagement als Teil des unternehmensweiten Risikomanagementsystems
- ♦ Empfängerorientiertes Reporting im IT-Risikomanagement (KPIs, Visualisierung etc.)
- ♦ Diverse Fallstudien zur praktischen Umsetzung eines IT-Risikomanagements
- ♦ IT-seitige Umsetzung eines IT-Risikomanagement (u.a. basierend auf R, Python)