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 "Risikomanagement" (Frank Romeike, Springer Verlag 2018) 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 Seminar **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. Der Schwerpunkt des Trainings liegt auf praxiserprobten Methoden zur Umsetzung eines wirksamen IT-Risikomanagements.

Entsprechend beinhaltet das Training nicht:

- Compliance-getriebene Umsetzung nach BSI Grundschutz oder ISO 2700x/ISMS
- Checklistenartige Umsetzung einer „Risikobuchhaltung“
- Qualitative Risk Maps oder vergleichbare subjektive Methoden

Inhalte/Agenda:

- ♦ Regulatorische gesetzliche Grundlagen des (IT-)Risikomanagements
- ♦ Risikomanagement als wichtigstes Element von NIS2
- ♦ Informationssicherheit vs. IT-Risikomanagement
- ♦ Warum viele (IT-)Risikomanagement-Systeme heute nicht wirksam sind
- ♦ Der Risikomanagement-Prozess in der Praxis
- ♦ Werkzeuge im IT-Risikomanagement
- ♦ Praxisübung: Bow-Tie-Analyse inkl. Business Impact Analyse (BIA)
- ♦ Aggregation von (IT-)Risiken
- ♦ Kommunikation über IT-Risiken in der Sprache der Entscheider
- ♦ Leitfaden zur Analyse von Cyber-Risiken in der Praxis
- ♦ Elemente eines wirksamen (IT-)Risikomanagements in der Praxis
- ♦ Relevanz eines wirksamen IT-Risikomanagements für die Unternehmenssteuerung
- ♦