

## Erwerben Sie die spezifischen Kenntnisse eines IT Risk Managers für die Planung und

### Etablierung eines IT-Risikomanagementsystems gemäß ISO 31000, ISO 27005 und BSI IT-Grundschutz

Die **Haupttätigkeit** eines IT Risk Managers besteht darin, die **IT-Risiken** eines Unternehmens anhand der spezifischen **Bedrohungslage** zu identifizieren, realistische **Risikoszenarien** zu entwickeln und die Abschätzung der **Schadensauswirkungen** auf den Geschäftsbetrieb vorzunehmen.

Weitere Aufgaben, die in die Zuständigkeit eines IT Risk Managers fallen, sind insbesondere die Abstimmung und Koordination der **IT-Risikostrategie**, die Festlegung von Kriterien der **Risikobewertung** und der **Risikoakzeptanz** sowie die Planung angemessener Maßnahmen der **Risikobehandlung** zur Unterstützung der Unternehmensziele.

Der IT Risk Manager muss, um die Einhaltung der gesetzlich vorgeschriebenen **Risikofrüherkennung** zu gewährleisten, ein **aktives risikoorientiertes Vorgehen** in allen Geschäftsabläufen etablieren sowie die Planung und Umsetzung der Sicherungsmaßnahmen in den Bereichen **Informationssicherheit** und **Business Continuity** kontrollieren und steuern.

Des Weiteren ist für den Aufbau eines organisationsspezifischen **Risikomanagementsystems** (RMS) die **erfolgreiche Integration** der Planung, der Kontrolle und der Steuerung von **Prozessen** und ergänzenden **Dokumenten** sowie die **Dokumentation** eines **Risikomanagementhandbuchs** erforderlich.

#### ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich des IT-Risikomanagements, der Aufgabenbeschreibung des „Risikomanagers“ gemäß ONR 49003 und des erforderlichen Fachwissens für die Etablierung eines RMS gemäß ISO 31000, ISO 27005 sowie des BSI IT-Grundschutz.

Die Teilnehmer können nach Abschluss der Ausbildung die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines RMS zur Umsetzung bringen.

#### INHALT

- IT-Management und IT-Risikomanagement
- Die Risikostrategie
- Aufbau, Begrifflichkeiten und Umsetzung eines RMS
- Aufgaben des „Risk Managers“ im RMS
- Die Risikomanagementorganisation und Verantwortlichkeiten im RMS
- Fachbegriffe der Normen und des Risikomanagements
- Die IT Compliance
- Die Risikofrüherkennung
- Die IT Governance
- IT-Sicherheitsgesetz und KRITIS
- Informationssicherheit und Cybersicherheit
- ISO 31000
- ONR 4900x-Normenfamilie
- ISO 27005
- ISO 270xx-Normenfamilie
- BSI-Standard „200-3 Risikoanalyse“
- Der Risikomanagementprozess
- Durchführung eines Risiko-Assessments
- Die Risikoanalyse
- Die Risikoidentifikation
- Die Risikoabschätzung
- Die Risikopriorisierung
- Die Risikokriterien zur Risikobewertung und Risikoakzeptanz
- Die Risikobehandlung
- Die Restrisiken
- Schadenshöhe und Eintrittswahrscheinlichkeit
- „Brutto“- und „Netto“-Risiken
- Proaktives und reaktives Risikomanagement
- Die Risikoakzeptanz
- Die Risikointegration in den Geschäftsbetrieb
- Risikoorientierte Steuerung von Geschäftsabläufen
- Bestimmung geschäftskritischer Geschäftsprozesse
- Abhängigkeiten und Wechselwirkungen des IT-gestützten Geschäftsbetriebs erkennen
- Kennzahlen und KPIs im IT-Risikomanagement
- Kommunikation und Reporting des Risikomanagements
- Aufrechterhaltung und Verbesserung des RMS
- Unterstützende Managementsysteme wie ISMS und BCMS
- Maßnahmen der Informationssicherheit
- Maßnahmen des Business Continuity Management (BCM)
- Business Impact Analyse (BIA)
- Kontinuitätsstrategien

**Abschluss:** Teilnahmebestätigung

**Optional:** Prüfung mit Personenzertifikat (DGI®)

#### ZIELGRUPPE

- Angehende IT Risk Manager
- IT-Leitung / IT-Administratoren
- IT-Sicherheitsbeauftragte / Chief Information Security Officer
- Verantwortliche im Risikomanagement
- Verantwortliche in der Revision / IT-Revision
- Führungskräfte / Projektleitung
- Unternehmensberater / Wirtschaftsprüfer

#### IHR DOZENT

##### Herr Ronny Neid

Herr Neid ist Diplom-Betriebswirt sowie u. a. zertifizierter IT-Risk und Business Continuity Manager und IT-Sicherheitsbeauftragter. Als Vorstand | COO der DGI berät Herr Neid im Bereich der IT-Sicherheit und des Datenschutzes und entwickelt Sicherheitskonzepte. Herr Neid doziert zu zahlreichen korrelierenden Themen der Informationssicherheit.

