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.

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

Unseren **Seminarkatalog** sowie unsere **aktuellen Termine** finden Sie unter

www.DGI-AG.de

Gerne senden wir Ihnen unverbindlich **weiteres Informationsmaterial** zu.

Akademie der
DGI Deutsche Gesellschaft
für Informationssicherheit AG

Kurfürstendamm 57
D - 10707 Berlin

Telefon +49 30 31 51 73 89 - 10
Fax +49 30 31 51 73 89 - 20

E-Mail AKADEMIE@DGI-AG.de
Web www.DGI-AG.de

IT Risk Manager (DGI®)

gemäß ISO 31000, ISO 27005 und BSI IT-Grundschutz

AKADEMIE der DGI® Deutsche Gesellschaft für Informationssicherheit AG

Der qualifizierte IT Risk Manager

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.

DGI®

Inhalt der Ausbildung

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

- 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