



IS-/IT-Risikomanager nach ISO 31000, ISO 27001 und ISO 27005

Unser Seminar vermittelt Ihnen die Grundlagen zum IT-Risikomanagement. Sie lernen wie Sie in Ihrem Unternehmen das Risikomanagement aufbauen, einführen und betreiben können.

Zertifikat "Risikomanager für Informationssicherheit, IT-Sicherheit und Datenschutz nach ISO 31000, ISO 27001, ISO 27005 und ISO 27701"

Unser Experten-Zertifikat ermöglicht es Ihnen als Mitarbeiter Ihre Kompetenz im Umfeld Informationssicherheit eindeutig zu belegen.

Listenpreis

3.290,00 € exkl. MwSt

3.915,10 € inkl. MwSt

Dauer

5 Tage

Gebühr für Prüfungen/Examen

420,00 € exkl. MwSt / 499,80 € inkl. MwSt

Prüfungsversicherung

159,00 € exkl. MwSt / 189,21 € inkl. MwSt

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihr Ansprechpartner



Manuela Krämer
Leitung
Informationssicherheit

Kontakt/Fragen:

m.kraemer@cbt-training.de

Telefon: +49 (0)89-4576918-12

Inhalte

Sie erhalten ein ausführliches Manuskript zum Kurs sowie viele Übungen und Fallbeispiele, die im Kurs bearbeitet und besprochen werden. Viel Best Practices runden das Seminar ab!

- **Einführung**
 - Was ist Risiko?
 - Abgrenzung zu "Chance"
 - Risiken im alltäglichen Leben
 - Risiken (und Chancen) bei der unternehmerischen Tätigkeit (Prozesse, Informationen, unterstützende Werte)
 - Abgrenzung Informationssicherheit und IT-Sicherheit (IS-Risiken - IT-Risiken)
- **Grundlagen Risikomanagement/Risk Management**
 - Was ist Risikomanagement?
 - Definition des Begriffes "Risiko"
 - Ziele des Risikomanagements
 - Risikomodell und Risikofaktoren
 - Risikoorganisation / Rollen & Verantwortlichkeiten / Governance-Aspekte
- **Anforderungen an Informationssicherheits-/IT-Risikomanagement aus betrieblicher Sicht**
 - Gesetzliche und regulatorische Vorgaben
 - Risikomanagement als Kern eines Managementsystems nach ISO-Managementsystemstandards



- **Der Risikomanagement-Prozess**
 - Normen und Standards Risikomanagement allgemein (ISO 31000, ONR 49000)
 - Normen und Standards Informationssicherheits- und IT-Risikomanagement (ISO 27001, ISO 27005, BSI 200-3, COBIT, ITIL)
 - Der Risikomanagement-Prozess nach ISO 31000 (ISO 27005)
 - Rahmenbedingungen festlegen
 - Risiken beurteilen (identifizieren, analysieren, bewerten)
 - Risiken behandeln
 - Kommunikation und Überwachung
- **Der wirtschaftliche Aspekt des Informationssicherheits-/IT-Risikomanagements**
 - Quantitative versus qualitative Aussagen
 - ROSI: Return on Security Investment
 - Kosten-/Nutzen-Betrachtungen
- **Der Informationssicherheits-/IT-Risikomanagement-Prozess in der Praxis**
 - Risikomanagement im Lifecycle von Informationen, Systemen und Applikationen
 - Methoden und Werkzeuge
 - Durchführung eines Risk-Assessments anhand einer Beispiel-Firma
- **Informationssicherheits-/IT-Risikomanagement im Unternehmen: Schnittstellen zu anderen Bereichen**
 - Enterprise Risk Management (unternehmensweites Risikomanagement)
 - IT-Notfallplanung
 - Business Continuity Management (Geschäftsfortführung)
 - Datenschutz
 - Projektmanagement
 - Einkauf
- **Informationssicherheits-/IT-Risikomanagement in spezifischen Anwendungsfällen**
 - Outsourcing-Projekte
 - Cloud-Nutzung
 - Cyber-Risiken
- **Zusammenfassung der Schulung, Besprechung der noch offenen Fragen, Prüfung (Optional)**

Weiterführende Kurse:

Für eine Beratung rufen Sie uns gerne an!

- Advanced Privacy & Counter Surveillance Training
- IT-GRC Governance, Risk & Compliance Management Systems
- Change Management
- ISO27701 DSMS / PIMS
- BCM Business Continuity Manager
- IT-GRC Governance, Risk & Compliance Management Systems
- Cyber Security Incident Manager



Ziele

Im Zeitalter der Digitalisierung von Geschäftsprozessen sind Informationen ein wertvolles Gut für Unternehmen. Stehen sie nicht zur Verfügung, sind sie verfälscht oder ist ihre Vertraulichkeit gestört, so entsteht ein Schaden für das Unternehmen. Doch wie entsteht ein solcher Schaden? Was sind die Einflussfaktoren? Und wie relevant ist der Schaden für die Organisation?

In vielen Organisationen werden diese Fragen auch im Zeitalter des Cyber-Crime immer noch gar nicht oder nur unzureichend behandelt. Die Risiken der digitalen Gegenwart und Zukunft werden nicht eruiert und daher auch nicht gesteuert. Und das, obwohl alle gängigen Standards und Normen aber auch gesetzliche Vorgaben im Bereich der Informationssicherheit, der IT-Sicherheit oder des Datenschutzes das Management von Risiken als Grundlage setzen.

Die Einführung eines Risikomanagement für Risiken der Informationssicherheit bildet in einer sich immer weiter digitalisierenden Zukunft daher eine unabdingbare Voraussetzung für alle Unternehmen und Organisationen.

Lernen Sie in unserem Seminar die Grundlagen zu Risikomanagement kennen. Erfahren Sie, wie Sie in Ihrem Unternehmen das Risikomanagement für Informationssicherheit/IT-Sicherheit aufbauen, einführen und betreiben können.

Anhand eines Fallbeispiels mit einer Beispielfirma, das Sie die Seminarwoche über begleiten wird, erfahren Sie, wie Informationssicherheits-Risikomanagement in der Praxis eingeführt und betrieben werden kann.

Daneben wird Ihnen unser Referent viele praxiserprobte Beispiele aus seiner täglichen Beratungs- und Auditorentätigkeit aufzeigen.

Dem Seminar liegen die anerkannten und international anerkannten Standards und Normen des Risikomanagement zugrunde.

Zielgruppe

Der Zertifizierungskurs, der als Workshop ausgerichtet ist, richtet sich an Leiter und Mitarbeiter aus folgenden Bereichen:

- Informationssicherheit, IT-Sicherheit, (IT) Revision, Risikomanagement, Recht, Datenschutz, Compliance, Fraud-Management und IT-Betrieb.

Voraussetzungen

- Kenntnisse der Informationssicherheit nach ISO 27001 (alternativ BSI-Grundschutz oder andere vergleichbare Norm) oder Kenntnisse Risikomanagement allgemein nach ISO 31000.
- Nachfolgendes CBT-Seminar als Grundlagenkurs wäre wünschenswert: "ISO/IEC 27001 Lead Implementer & Lead Auditor CERT/ISO.LEAD.AUD.IMP"



Prüfung/Zertifizierung

CERT Risikomanager für Informationssicherheit, IT-Sicherheit und Datenschutz nach ISO 31000, ISO 27001, ISO 27005 und ISO 27701

Prüfung, deutsch
Multiple-Choice & Freitext Prüfung

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice Prüfung. Die **CBT CERT Prüfung** wird direkt nach Kursende abgenommen. Sie gilt als bestanden, wenn mindestens 70% der Fragen richtig beantwortet wurden.

Nach Bestehen der Prüfung erhalten Sie ein personenbezogenes **CBT CERT Zertifikat**, das Ihnen die erfolgreiche Kursteilnahme inklusive bestandener Prüfung bestätigt.

Hat ein Teilnehmer die **CBT CERT Prüfung** nicht bestanden, so kann er diese entweder direkt im Anschluss an die erste Prüfung oder während unserer Öffnungszeiten Online Live mit Prüfungsüberwachung (Kamerapflicht, MS-Teams) nach vorheriger schriftlicher Anmeldung (mind. 14 Tage vor Termin) gegen die genannte Prüfungsgebühr wiederholen. Die Prüfung kann höchstens 2-mal wiederholt werden. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Prüfungsversicherung zum CBT CERT:

Haben Sie zum Kurs und zur Prüfungsgebühr unsere Prüfungsversicherung bestellt, berechtigt diese zur **einmaligen kostenfreien Prüfungswiederholung** zu o.g. Bedingungen. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Ohne Prüfungsversicherung zahlen Sie bei Wiederholung die volle Prüfungsgebühr.

Gültigkeit CBT CERT ZERTIFIKAT:

Das **CBT CERT Zertifikat** ist 3 Jahre gültig und muss anschließend durch eine erneute Prüfung bei CBT Training & Consulting GmbH aktualisiert / verlängert werden.

Alle Prüfungsunterlagen werden 3 Jahre aufbewahrt.
