




## SC124 Kritische Infrastrukturen gem. ISO 27001 u. ISO 27019

| <p><b>Kurzbeschreibung:</b></p> <p>Unser ISMS-Seminar "ISMS-Einführung und Betrieb für Energieversorgungsunternehmen" legt die entscheidenden Grundlagen für den Aufbau eines Informationssicherheits-Managementsystems gem. ISO/IEC 27001 i.V. mit ISO/IEC 27019.</p> <p><b>Übungen, Fallbeispiele und Raum für Diskussion aus der Praxis lassen die trockene Normentheorie spannend werden.</b></p> <p><b>Zielgruppe:</b></p> <p>Gesetzliche Vorgaben und die Zunahme von Cyberbedrohungen stellen die Energieversorgungsbranche vor neue Herausforderungen in der Informationssicherheit.</p> <p><u>Der Kurs richtet sich vor allem an:</u></p> <ul style="list-style-type: none"> <li>- Betreiber von Energieversorgungsnetzen Strom/Gas §11 (1a) EnWG (Verteilnetz-/Übertragungsnetzbetreiber)</li> <li>- Betreiber von Energieanlagen gem. §11 (1b) EnWG (Kraftwerke, Gasspeicher etc.)</li> <li>- KRITIS-Betreiber gem. §8a BSI-Gesetz (z.B. virtuelle Kraftwerke)</li> <li>- Unternehmen mit ISMS-Betrieb gem. ISO/IEC 27001 und Prozess-IT-Hintergrund</li> </ul> <p><b>Voraussetzungen:</b></p> <p>Das Seminar richtet sich gleichermaßen an Einsteiger und Berufserfahrene. Vorkenntnisse über Managementsysteme (z.B. ISO/IEC 27001, ISO 9001 etc) sind hilfreich, aber keine Voraussetzung.</p> <p>Sofern im eigenen Unternehmen bereits ein ISMS implementiert ist, sollten sich die Teilnehmer vorab darüber informieren, um ggf. Fragen stellen zu können und Kursinhalte besser einordnen zu können.</p> | <p><b>Ziele:</b></p> <p>Ziel des Kurses ist ein Managementsystem gem. ISO/IEC 27001 grundlegend zu verstehen und Anforderungen an Zertifizierungen und Prüfungen ableiten zu können.</p> <p><b>Sie erhalten fundiertes Wissen für die Planung, Implementierung, Überwachung und Verbesserung und den laufenden Betrieb eines ISMS.</b></p> <p>Darüber hinaus bildet der Kurs eine gute Basis für weitere Aufbaukurse, z.B. Lead Auditor 27001 (IRCA).</p> <p>Ein reger Informationsaustausch unter den Teilnehmern wird angestrebt.</p> <p>Der Kurs hat <i>nicht</i> das Ziel einen Template- und Dokumentationssatz vorzustellen, sondern richtet sich an Personen, welche ein normgerechtes Managementsystem betreiben wollen. Der Kurs stellt keine Rechtsberatung zur Anwendung von gesetzlichen und regulatorischen Anforderungen dar.</p> <p>Am Ende des Trainings besteht die Möglichkeit eine Prüfung abzulegen. Nach Bestehen wird ein separates qSkills-Zertifikat ausgestellt.<br/> <b>Alle Prüfungsinhalte werden im Seminar angesprochen.</b> (Zusatzkosten/Prüfungsgebühr: 100,- Euro).</p> <p><b>Der Zertifikatstitel lautet: "ISMS-Implementierer für ISO/IEC 27001 und ISO/IEC 27019.</b></p> <p><b>Termine</b></p> <p><b>Dieser Workshop findet an folgenden Terminen statt:</b><br/> <b>Am ersten Tag ist Kursbeginn um 10:00 Uhr und der Kurs endet am letzten Tag um ca. 16:30.</b></p> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th>Ort</th> <th></th> <th>Beginn</th> <th>Ende</th> </tr> </thead> <tbody> <tr> <td>Virtuell</td> <td><br/>Virtuell<br/><a href="#">Karte</a></td> <td>11.05.2020</td> <td>13.05.2020</td> </tr> </tbody> </table> | Ort        |            | Beginn | Ende | Virtuell | <br>Virtuell<br><a href="#">Karte</a> | 11.05.2020 | 13.05.2020 |
|---|--|------------|------------|--------|------|----------|--|------------|------------|
| Ort   |  | Beginn     | Ende       |        |      |          |  |            |            |
| Virtuell  | <br>Virtuell<br><a href="#">Karte</a>   | 11.05.2020 | 13.05.2020 |        |      |          |  |            |            |

**Sonstiges:**

**Dauer:** 3 Tage

**Preis:** 1650 Euro plus Mwst.

Nürnberg

**i**  
Nürnberg  
Karte

30.11.2020 02.12.2020

## Inhalte/Agenda:

- Dieser Kurs wird bis zum 30.5.2020 nur als Remote- /Online Training durchgeführt!
  
- Es wird mit folgenden Normen intensiv gearbeitet: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 27019 sowie den IT-Sicherheitskatalogen.
  - ◆ **Teil 1: Kurze Einführung: Informationssicherheit verstehen und Gefährdungslage**
  
  - ◆ **Teil 2: Die ISO/IEC 27001-Normenfamilie, sowie gesetzliche, regulatorische Anforderungen**
    - ◇ Überblick über die Normenvielfalt
    - ◇ Aufbau der ISO/IEC 27001, 27002 und ISO/IEC 27019
    - ◇ IT-Sicherheitskataloge §11 (1a), (1b) EnWG (IT-Sik)
    - ◇ Konformitätsbewertungsprogramm der BNetzA
    - ◇ BSI-Gesetz und BSI-Kritis-Verordnung, §8a-Anforderungen
    - ◇ Branchenspezifische Sicherheitsstandards (B3S)
  
  - ◆ **Teil 3: Das Managementsystem ISO/IEC 27001, Kapitel 4 - 10**
    - ◇ Kapitel 4: Kontext der Organisation
      - Was ist der interne und externe Kontext, interessierte Parteien?
      - Wie sollte der sog. Anwendungsbereich hergeleitet werden und wie könnte ein Scope-Dokument aufgebaut werden?
      - Welchen Einfluss auf den Scope nehmen IT-SiK und §8a-Anforderungen
  
    - ◇ Kapitel 5: Führung
      - Anforderungen und Rollen der Geschäftsführung im ISMS
      - Bestandteile einer Informationssicherheitspolicy/-Leitlinie
      - Rollen und Verantwortlichkeiten im ISMS
  
    - ◇ Kapitel 6: Planung
      - ISMS-Risikomanagement: Normanforderungen und Lösungsansätze für die Praxis, um die Anforderungen aus IT-Sik oder §8a BSI-G zu erfüllen
      - Bestandteile eines Risikomanagements gem. ISO/IEC 27005
      - Aufbau einer Erklärung zur Anwendbarkeit (SoA)
      - Wie werden unternehmensspezifische Maßnahmen angemessen implementiert? "Alle lesen aus der gleichen Norm, doch was bedeutet das konkret für Energieversorger?"
      - Risikomatrix, Risiko-Owner und Risikobehandlungsoptionen/-Pläne
  
    - ◇ Kapitel 7: Unterstützung
      - Ressourcen, Kompetenzen, Awareness, dokumentierte Information
  
    - ◇ Kapitel 8: Betrieb
      - Anforderungen und Herausforderungen an die Aufrechterhaltung eines Managementsystems
  
    - ◇ Kapitel 9: Bewertung und Leistung
      - Messen und Bewerten mit Messwerten und KPIs
      - Durchführung interner Audits, Aufbau von Auditplänen und Auditprogrammen
      - Bestandteile einer Managementbewertung
  
    - ◇ Kapitel 10: Verbesserung
      - Anforderungen an Korrekturmaßnahmen aus Audits und Sicherheitsvorfällen
      - Etablierung eines KVP-Prozesses
  
  - ◆ **Teil 4: Vorstellung und Diskussion ausgewählter technisch-organisatorischer Maßnahmen aus ISO/IEC 27001, Anhang A**
    - ◇ ISO/IEC 27001/27002: u.a. Asset-Management, Lieferantenmanagement, Vorfallsmanagement
    - ◇ ISO/IEC 27019: Inhalte der 14 neuen Controls und Nutzung der ergänzenden Umsetzungsempfehlungen, u.a. physische Sicherheit von Leitwarten und Betriebsstätten.

◇ Meldepflichten aus §11 (1c) EnWG und §8b (3) BSI-G. Aufbau einer Kontaktstelle zur jederzeitigen Erreichbarkeit durch das Bundesamt für Sicherheit in der Informationstechnik

◆ **Teil 5: Zertifizierung & Prüfungen**

◇ Der Zertifizierungszyklus

◇ Der Weg zur erfolgreichen Zertifizierung - auf was muss geachtet werden?

**Empfänger:**  
qSkills GmbH & Co. KG  
Südwestpark 65  
90449 Nürnberg  
eMail: [info@qskills.de](mailto:info@qskills.de)  
Fax: +49 (0)911-80103-39



**Absender:**  
Firma: \_\_\_\_\_  
Strasse: \_\_\_\_\_  
PLZ/Ort: \_\_\_\_\_

## Anmeldung zum Workshop SC124 Kritische Infrastrukturen gem. ISO 27001 u. ISO 27019

**Termin:** Von \_\_\_\_\_ bis \_\_\_\_\_  
**Dauer:** 3 Tage  
**Preis:** 1650 EUR + MWST. pro Teilnehmer

**Teilnehmer 1:**  
Name: \_\_\_\_\_ Vorname: \_\_\_\_\_  
Abteilung: \_\_\_\_\_  
Telefon: \_\_\_\_\_ Mobil: \_\_\_\_\_  
Telefax: \_\_\_\_\_  
eMail: \_\_\_\_\_  
eMail2: \_\_\_\_\_

**Teilnehmer 2:**  
Name: \_\_\_\_\_ Vorname: \_\_\_\_\_  
Abteilung: \_\_\_\_\_  
Telefon: \_\_\_\_\_ Mobil: \_\_\_\_\_  
Telefax: \_\_\_\_\_  
eMail: \_\_\_\_\_  
eMail2: \_\_\_\_\_

**Hotelwunsch:** Bitte zutreffendes Ankreuzen:  Ja |  Nein

**An- Abreise Teilnehmer 1:** Von \_\_\_\_\_ bis \_\_\_\_\_

**An- Abreise Teilnehmer 2:** Von \_\_\_\_\_ bis \_\_\_\_\_

**Rechnungsanschrift:**  
Firma: \_\_\_\_\_  
Ansprechpartner: \_\_\_\_\_  
Abteilung: \_\_\_\_\_  
Strasse: \_\_\_\_\_  
Ort: \_\_\_\_\_

Hiermit bestätige ich die verbindliche Anmeldung zu o.g. Workshop. Ich besitze die notwendigen Vorkenntnisse.  
Es gelten die AGB der qSkills GmbH & Co. KG

Ort, Datum \_\_\_\_\_ Unterschrift \_\_\_\_\_