SC124 ISMS-Implementierung für EVU/KRITIS gemäß ISO/IEC 27001:2022 und 27019

Kurzbeschreibung:

Unser Seminar **SC124 ISMS-Implementierung für EVU/KRITIS gemäß ISO/IEC 27001:2022 und 27019** legt die entscheidenden Grundlagen für den Aufbau eines Informationssicherheits-Managementsystems gem. ISO/IEC 27001 in Verbindung mit ISO/IEC 27019. Der Kurs basiert auf der Version 2022 der Norm.

Es wird mit folgenden Normen intensiv gearbeitet: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 27019 sowie den IT-Sicherheitskatalogen.

Übungen, Fallbeispiele und Raum für Diskussion aus der Praxis lassen die trockene Normentheorie spannend werden.

Zielgruppe:

Gesetzliche Vorgaben und die Zunahme von Cyberbedrohungen stellen die Energieversorgungsbranche vor neue Herausforderungen in der Informationssicherheit.

Der Kurs richtet sich vor allem an:

- Betreiber von Energieversorgungsnetzen Strom/Gas §11 (1a) EnWG (Verteilnetz-/Übertragungsnetzbetreiber)

- Betreiber von Energieanlagen gem. §11 (1b) EnWG (Kraftwerke, Gasspeicher etc.)

- KRITIS-Betreiber gem. §8a BSI-Gesetz (z.B. virtuelle Kraftwerke)

- Unternehmen mit ISMS-Betrieb gem. ISO/IEC 27001 und Prozess-IT-Hintergrund

Voraussetzungen:

Das Seminar SC124-EN ISMS implementation for energy supplier/KRITIS according to ISO/IEC 27001:2022 and 27019 richtet sich gleichermaßen an Einsteiger und Berufserfahrene. Vorkenntnisse über Managementsysteme (z.B. ISO/IEC 27001, ISO 9001, etc.) sind hilfreich, aber keine zwingende Voraussetzung.

Sofern im eigenen Unternehmen bereits ein ISMS implementiert ist, sollten sich die Teilnehmer vorab darüber informieren, um ggf. zielgerichtet Fragen stellen und Kursinhalte besser einordnen zu können.

Sonstiges:

Dauer: 3 Tage

Preis: 1650 Euro plus Mwst.

Ziele:

Ziel des Kurses ist ein Managementsystem gem. ISO/IEC 27001 grundlegend zu verstehen und Anforderungen an Zertifizierungen und Prüfungen ableiten zu können.

Sie erhalten fundiertes Wissen für die Planung, Implementierung, Überwachung, Verbesserung und den laufenden Betrieb eines ISMS.

Darüber hinaus bildet der Kurs eine gute Basis für weitere Aufbaukurse, z.B.:

- **SC185 Praxisumsetzung der ISO 27001/27002**
- **SC135 Interner Auditor**
- **SC150 ISMS Auditor/Lead Auditor (IRCA A17608)**

Ein reger Informationsaustausch unter den Teilnehmern wird angestrebt.

Der Kurs hat nicht 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.

Am Ende des letzten Trainingstages besteht die Möglichkeit eine Prüfung abzulegen. Nach Bestehen wird ein Zertifikat ausgestellt. **Alle Prüfungsinhalte werden im Seminar angesprochen.**

Der Zertifikatstitel lautet: "ISMS-Implementierer für EVU/KRITIS gemäß ISO/IEC 27001 und 27019"

Inhalte/Agenda:

- ♦ **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. Andwendungsbereich 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 kontinuierlichen Verbesserungsprozesses (KVP)

♦ **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?

♦
- ◊