SC124-EN ISMS implementation for energy supplier/KRITIS according to ISO/IEC 27001:2022 and 27019

Kurzbeschreibung:

Our seminar **SC124-EN ISMS implementation for energy supplier/KRITIS according to ISO/IEC 27001:2022 and 27019** lays the decisive foundations for setting up an information security management system in accordance with ISO/IEC 27001 in conjunction with ISO/IEC 27019. The course is based on the 2022 version of the standard.

Intensive work is done with the following standards: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 27019 and the IT security catalogs.

Exercises, case studies and room for discussion from the field make the dry standards theory exciting.

Zielgruppe:

Regulatory requirements and the rise of cyber threats are presenting the utility industry with new information security challenges.

The course is aimed primarily at:

- Operators of energy supply networks electricity / gas §11 (1a) EnWG (distribution network / transmission system operators)

- Operators of energy facilities acc. to §11 (1b) EnWG (power plants, gas storage facilities etc.)

- KRITIS operators according to §8a BSI Act (e.g. virtual power plants)

- Companies with ISMS operation according to ISO/IEC 27001 and process IT background

Voraussetzungen:

The seminar **SC124-EN ISMS implementation for energy supplier/KRITIS according to ISO/IEC 27001:2022 and 27019** is aimed equally at beginners and experienced professionals. Previous knowledge of management systems (e.g. ISO/IEC 27001, ISO 9001, etc.) is helpful, but not a prerequisite.

If an ISMS has already been implemented in your own company, participants should inform themselves about it in advance in order to be able to ask questions and better understand the course content.

Sonstiges:

Dauer: 3 Tage

Preis: 1650 Euro plus Mwst.

Ziele:

The aim of the course is to fundamentally understand a management system according to ISO/IEC 27001 and to be able to derive requirements for certifications and audits.

You will gain sound knowledge for the planning, implementation, monitoring and improvement and ongoing operation of an ISMS.

In addition, the course forms a good basis for further advanced courses:

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

A lively exchange of information among the participants is intended.

The course has *not* the goal to present a template and documentation set, but is aimed at people who want to operate a management system in compliance with standards. The course does not constitute legal advice on the application of legal and regulatory requirements.

At the end of the last training day participants can take the optional exam. Upon passing, a certificate will be issued. **All exam content will be addressed in the seminar.**

The certificate title is: "ISMS Implementer for ISO/IEC 27001 and ISO/IEC 27019"

Inhalte/Agenda:

- ♦ **Part 1: Brief introduction: understanding information security and vulnerability**.

♦ **Part 2: The ISO/IEC 27001 family of standards, and legal, regulatory requirements**

♦
- ◊ Overview of the variety of standards
- ◊ Structure of ISO/IEC 27001, 27002 and ISO/IEC 27019.
- ◊ IT security catalogs §11 (1a), (1b) EnWG (IT-Sik)
- ◊ Conformity assessment program of the BNetzA
- ◊ BSI Act and BSI Criticality Ordinance, §8a requirements
- ◊ Industry-specific security standards (B3S)

♦ **Part 3: The ISO/IEC 27001 management system, chapters 4 - 10**

♦
- ◊ Chapter 4: Context of the organization
  - ◊ · What is the internal and external context, interested parties?
  - · How should the so-called scope of application be derived and how could a scope document be structured?
  - · What is the influence of IT-SiK and §8a requirements on the scope?
- ◊ Chapter 5: Management
  - ◊ · Requirements and roles of the management in the ISMS
  - · Components of an information security policy/guideline
  - · Roles and responsibilities in the ISMS
- ◊ Chapter 6: Planning
  - ◊ · ISMS risk management: standard requirements and solution approaches for practice to meet the requirements of IT-Sik or §8a BSI-G
  - · Components of a risk management according to ISO/IEC 27005
  - · Structure of a statement of applicability (SoA)
  - · How are company-specific measures implemented appropriately? "Everyone is reading from the same standard, but what does that mean specifically for utilities?"
  - · Risk matrix, risk owners, and risk treatment options/plans.
- ◊ Chapter 7: Support>
  - ◊ · Resources, competencies, awareness, documented information.
- ◊ Chapter 8: Operations>
  - ◊ · Requirements and challenges of maintaining a management system.
- ◊ Chapter 9: Assessment and Performance
  - ◊ · Measuring and evaluating with metrics and KPIs.
  - · Conducting internal audits, building audit plans and audit programs.
  - · Components of a management review
- ◊ Chapter 10: Improvement>
  - ◊ · Corrective action requirements from audits and security incidents.
  - · Establishment of a CIP process

♦ **Part 4: Presentation and discussion of selected technical/organizational measures from ISO/IEC 27001, Annex A**

♦
- ◊ ISO/IEC 27001/27002: including asset management, supplier management, incident management.
- ◊ ISO/IEC 27019: Contents of the 14 new controls and use of the supplementary implementation recommendations, including physical security of control rooms and operating sites.
- ◊ Reporting obligations from §11 (1c) EnWG and §8b (3) BSI-G. Establishment of a contact point for accessibility at any time by the Federal Office for Information Security.

♦
- ◊ **Part 5: Certification & Examinations**
  - ◊ · The certification cycle
  - · The path to successful certification - what to look out for?

♦ ◊ ·