SC120-EN ISMS implementation according to ISO/IEC 27001:2022

Kurzbeschreibung:

The training **SC120 ISMS implementation according to ISO/IEC 27001:2022** deals with the basics of an ISMS according to ISO/IEC 27001:2022.

The need for organizations to better protect their information is highlighted by the increasing frequency of security breaches and the increasing value of information.
The information security management system (ISMS) provides a controlled and organized approach to handling an organization's sensitive information so that it is always secure and under control. Implementation affects people, processes and technical components.

Zielgruppe:

- Security Consultants
- all those who want to establish a formal information security management system in accordance with ISO 27001:2022

Note: If you work in the energy supplier/KRITIS environment, we offer **SC124-EN ISMS implementation for energy supply companies/KRITIS according to ISO/IEC 27001:2022 and 27019**, a specialised course for your specific requirements.

Voraussetzungen:

The seminar **SC120-EN ISMS implementation according to ISO/IEC 27001:2022** 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 mandatory requirement.

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 **SC120 ISMS implementation according to ISO/IEC 27001:2022** course is to gain a basic understanding of a management system according to ISO/IEC 27001 and to be able to derive requirements for certifications and audits.

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

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

- **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 aimed at.

The course does not aim to present a template and documentation set, but is aimed at people who want to operate a standard-compliant management system. The course does not constitute legal advice on the application of legal and regulatory requirements.

On the last day of the training participants can take the optional exam. A certificate will be issued upon passing. **All exam content is covered in the seminar.**

The certificate title is "ISMS Implementer for ISO/IEC 27001:2022".

Inhalte/Agenda:

- ♦ **Short introduction: Understanding information security and the threat situation**

♦ **The ISO/IEC 27001 family of standards, BSI IT-Grundschutz**
♦ ◊ Structure and interaction of ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003

♦ **The management system ISO/IEC 27001, 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 should a good scope document be constructed?
◊ Chapter 5: Management
◊ · Requirements and roles of management in the ISMS
· Components of an information security guideline
· Roles and responsibilities in the ISMS
◊ Chapter 6: Planning
◊ · ISMS risk management: standard requirements and practical solutions
· Components of risk management in accordance with ISO/IEC 27005
· Building a Statement of Applicability (SoA)
· How are company-specific measures implemented appropriately?
· Risk matrix, risk owner and risk treatment options/plans
◊ Chapter 7: Support
◊ · Resources, competencies, awareness, documented information
◊ Chapter 8: Operation
◊ · Requirements and challenges of maintaining a management system
◊ Chapter 9: Assessment and Performance
◊ · Measuring and evaluating with metrics and KPIs
· Conducting internal audits, setting up audit plans and audit programs
· Components of a management review
◊ Chapter 10: Improvement
◊ · Requirements for corrective actions from audits and safety incidents
· Establishing a CIP process

♦ **Part 4: Selected topics from ISO/IEC 27001, Annex A**
♦ ◊ Classification of information
◊ Handling of security incidents
◊ Information security aspects of business continuity management

♦ **Part 5: Certification & Examinations**
♦ ◊ The certification cycle
◊ The path to successful certification - what needs to be considered?
♦ ◊