SC120 Implementierung gemäß ISO/IEC 27001:2022

Kurzbeschreibung:

Das Training **SC120 Implementierung gemäß ISO/IEC 27001:2022** beschäftigt sich mit den Grundlagen eines ISMS gemäß ISO/IEC 27001:2022.

Die Notwendigkeit, dass Organisationen ihre Informationen besser schützen müssen, wird deutlich durch die immer häufiger auftretenden Sicherheitslücken sowie den steigenden Wert von Informationen.
Das Informationssicherheit Managementsystem (ISMS) bietet einen kontrollierten und organisierten Ansatz für den Umgang mit sensiblen Informationen einer Organisation, sodass diese stets sicher und unter Kontrolle sind. Betroffen sind bei einer Umsetzung Personen, Prozesse und technische Komponenten.

Zielgruppe:

- Sicherheitsberater
- Verantwortliche für die Einführung und Umsetzung von ISO/IEC 27001:2022

Voraussetzungen:

Das Seminar 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 letzten Tag des Trainings (ca. 16:00 - 17:00 Uhr) besteht die Möglichkeit eine Prüfung abzulegen. Nach Bestehen wird ein separates qSkills-Zertifikat ausgestellt. **Alle Prüfungsinhalte werden im Seminar angesprochen.**

Der Zertifikatstitel lautet "ISMS-Implementierer für ISO/IEC 27001:2022".

Inhalte/Agenda:

- **Teil 1: Kurze Einführung: Informationssicherheit verstehen und Gefährdungslage**

- **Teil 2: Die ISO/IEC 27001-Normenfamilie, BSI IT-Grundschutz**
  - ♦ Überblick über die Normenwelt
  - ♦ Aufbau und Zusammenspiel der ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003

- **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 sollte ein gutes ein Scope-Dokument aufgebaut werden?
  - ♦ Kapitel 5: Führung
    - ◊ Anforderungen und Rollen der Geschäftsführung im ISMS
    - ◊ Bestandteile einer Informationssicherheits-Leitlinie
    - ◊ Rollen und Verantwortlichkeiten im ISMS
  - ♦ Kapitel 6: Planung
    - ◊ ISMS-Risikomanagement: Normanforderungen und Lösungsansätze für die Praxis
    - ◊ Bestandteile eines Risikomanagements gem. ISO/IEC 27005
    - ◊ Aufbau einer Erklärung zur Anwendbarkeit (SoA)
    - ◊ Wie werden unternehmensspezifische Maßnahmen angemessen implementiert?
    - ◊ 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: Ausgewählte Themen aus ISO/IEC 27001, Anhang A**
  - ♦ Informationsklassifizierung
  - ♦ Behandlung von Sicherheitsvorfällen
  - ♦ Informationssicherheitsaspekte beim Business Continuity Management

- **Teil 5: Zertifizierung & Prüfungen**
  - ♦ Der Zertifizierungszyklus
  - ♦ Der Weg zur erfolgreichen Zertifizierung - auf was muss geachtet werden?