CL130 Cloud Information Security gemäß ISO/IEC 27017/27018

Kurzbeschreibung:

ISMS-Verantwortliche, Cloud-Architekten und IT-Sicherheitsbeauftragte erhalten eine praxisnahe Einführung in die sichere Einführung und Nutzung von Cloud-Services gemäß ISO/IEC 27017/27018. Vermittelt werden Methoden zur Integration von Cloud Services in ein ISMS sowie Konzepte für sichere Cloud-Architekturen und Implementierungen. Behandelt werden zudem vertiefende Anforderungen wie BSI-C5, die im Kontext von Informationssicherheit und Compliance praxisnah angewendet werden.

Zielgruppe:

- Informationssicherheitsbeauftragte
- CISOs
- Compliance-Beauftragte
- Cyber Security Architekten
- Cloud Competence Center
- Datenschutzbeauftragte

Voraussetzungen:

Um Kursinhalten und Lerntempo im Kurs **CL130 Cloud Information Security gemäß ISO/IEC 27017/27018** gut verstehen, sind folgende Kenntnisse nötig bzw. von Vorteil:

Funktion und Aufbaus eines ISMS nach ISO/IEC 27001.

Alternativ besuchen Sie **vorher** die Workshops **SC120 ISMS-Implementierung gemäß ISO 27001:2022** und **CL120 Cloud Compliance – Normen, Sicherheitsanforderungen, Lösungswege**.

Sonstiges:

Dauer: 3 Tage

Preis: 2100 Euro plus Mwst.

Ziele:

Wir vermitteln Ihnen das umfassende Wissen für die Planung, Implementierung, Überwachung und Verbesserung von Cloud Information Security im Kontext von anerkannten Cloud Security Frameworks. In diesem Intensivtraining erwerben die Teilnehmer fundiertes Wissen über die notwendigen Schritte für einen konformen und sicheren Cloud-Betrieb.

Für die sichere und konforme Einführung von Cloud-Services werden folgende Themen behandelt:

- Geeignete Frameworks, Normen und Standards.
- Sicherheitsarchitektur und -richtlinien für Cloud-Infrastrukturen und deren Kriterien, um sicherzustellen, dass Daten und Ressourcen angemessen geschützt sind.
- Das Shared Responsibility Modell in Bezug auf die Sicherheit.
- Neue Sicherheitsmodelle in der Cloud wie Zero Trust und deren mögliche Umsetzung.

- Identitäts- und Zugriffsmanagement, um sicherzustellen, dass nur autorisierte Benutzer auf Cloud-Ressourcen zugreifen können.
- Daten- und Anwendungssicherheit: Verschlüsselungskonzepte und Absicherung der verschiedenen Servicemodelle.
- Ein pragmatischer Überblick über mögliche Lösungsansätze bei verschiedenen Herstellern (Azure, Google Cloud, Amazon Web Services).

Zwei Normen in der ISO 27000-Reihe haben sich speziell auf dieses Thema fokussiert:

- **ISO/IEC 27017** adressiert sowohl die Nutzung von Cloud Lösungen als auch das Anbieten von Cloud Services
- **ISO/IEC 27018** bezieht sich auf den Schutz personenbezogener Daten in öffentlichen Cloud-Lösungen

Leitfragen:

1. Welche Möglichkeiten bietet die Security Frameworks und Konzepte, sowohl für Unternehmen die Cloud Services nutzen wollen als auch für Unternehmen die Cloud-Services anbieten?
2. Wie kann im Rahmen eines ISMS die Cloud Security mit ISO/IEC 27017/18 erweitert bzw. behandelt werden?
3. Welche Implementierungsmöglichkeiten (Design Principles) können im Kontext einer Security-Architektur eingesetzt werden?

Darüber hinaus bildet der Kurs CL130 eine gute Basis für weitere Aufbaukurse, z.B.:

1. SC135 Interner Auditor
2. SC150 ISMS Auditor/Lead Auditor (IRCA A17608)

Inhalte/Agenda:

- ♦ **Motivation und Grundlagen**
  - ♦ ◊ Grundbegriffe des Cloud Computing
    - ◊ · Konzepte
    - · Referenzarchitektur
    - · Shared Responsibility Model
  - ◊ Cloud Security
    - ◊ · Bedrohungen und Angriffsvektoren
    - · Sicherheitskonzepte
  - ◊ Cloud Security Services
    - ◊ · Azure
    - · Google Cloud Platform (GCP)
    - · AWS

- ♦ **Wichtige Normen/Standards, Zertifikate und Best-Practices**
  - ♦ ◊ Normen und Standards
    - ◊ · ISO/IEC 27001
    - · ISO/IEC 27017/18
    - · BSI C5
    - · NIST SP 800-xx
    - · NIST Cyber Security Framework
    - · CIS
    - · ...
  - ◊ Personenzertifikate
    - ◊ · CSA CCSK
    - · ISC2 CCSP
  - ◊ Zertifikate zu Produkten
    - ◊ · Azure Security Engineer
    - · Google Cloud Security Engineer
    - · AWS Certified Security

- ♦ **Organisatorische Anforderungen und Empfehlungen der Cloud Security**
  - ♦ ◊ Management (ISMS, Security Controls, DR, BCM)
    - ◊ · Planung der Implementierung
    - · Ausrollen der Implementierung
    - · Überprüfen und Anpassung der Implementierung
  - ◊ Management und Analyse der Risken
  - ◊ Cloud Onboarding Prozess
  - ◊ Reporting und Berichtserstattung
  - ◊ Auditierung und Compliance
  - ◊ Nutzung von Tools aus strategischer Sicht
    - ◊ · Azure: Compliance Manager
    - · Google Cloud: Security Command Center
    - · AWS: AWS Security Hub

- ♦ **Technische Anforderungen und operationeller Betrieb der Cloud Security**
  - ♦ ◊ Typische Architektur einer Cloud bzw. Multi-Cloud
  - ◊ Datensicherheit und -architektur
  - ◊ Zero Trust
  - ◊ Aufbau und Betrieb von sicheren Cloud-Anwendungen
  - ◊ Identity and Access Management
  - ◊ Überwachen der Cloud Security (Monitoring, Vorfälle, Forensik)
  - ◊ Nutzung von Tools aus taktischer und operativer Sicht

- ♦ **Diskussion und Zusammenfassung**
  - ♦