SC185 Praxisumsetzung der ISO 27001/27002

Kurzbeschreibung:

Die meisten ISMS-Beauftragen und Auditoren kennen das:
Wenn es darum geht, den Anhang A der ISO 27001 bzw. 27002 mit Leben zu füllen, kommt schnell die Frage „Was fordert die Norm?“ auf. Die Enttäuschung ist meist groß, wenn die Norm in ihrer generischen Sprache kaum konkrete Anhaltspunkte zur praktischen Umsetzung liefert.

Im Workshop **SC185 Praxisumsetzung der ISO 27001/27002** lernen Sie von erfahrenen Informationssicherheitsberatern/CISOs, wie mit dem Anhang A der ISO 27001 umzugehen ist und wie dieser beispielhaft angewendet werden kann.

Zielgruppe:

- Mitglieder der operativen Sicherheitsteams bzw. der Governance
- CISOs und Entscheider
- ISMS-Beauftragte
- Auditoren
- Zertifizierungskandidaten

Voraussetzungen:

Der Workshop **SC185 Praxisumsetzung der ISO 27001/27002** ist für alle Stufen geeignet. Anfänger bis Fortgeschrittene können am Kurs teilnehmen. Es sind keine technischen Vorkenntnisse notwendig, da im Kurs die technischen Grundlagen zum Verstehen der Anforderungen des Annexes der ISO 27001 bzw. der ISO 27002 detailliert vermittelt werden.

Sonstiges:

Dauer: 5 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

In Workshop **SC185 Praxisumsetzung der ISO 27001/27002** lernen Sie durch erfahrene Praktiker, wie Sie mit dem Thema Informationssicherheit praxisorientiert und erfolgreich umgehen. Der Fokus liegt auf funktionierenden und angepassten Konzepten und Lösungen und orientiert sich am Anhang A der ISO 27001 bzw. ISO 27002. Sie erhalten das Rüstzeug, um mit Ihrer IT und anderen Beteiligten „in den Verhandlungsring“ zu steigen und um die Wirksamkeit und Angemessenheit von insbesondere technischen Maßnahmen bewerten zu können.

Im Workshop befassen wir uns hauptsächlich mit den Controls des Anhang A des Standards bzw. der Umsetzungspraxis der ISO 27002. Aufgrund der Fülle an Controls-Ausprägungen werden teilweise Schwerpunkte gesetzt und behandelt. Individuelle Fragestellungen der Teilnehmer werden ausführlich behandelt. Einschränkung: Nicht alle branchenspezifischen Fragestellungen können im Rahmen des Workshops beantwortet werden, die Teilnahme ersetzt keine gezielte Beratung oder Auditprüfung des eigenen ISMS.

Dieser Kurs kann (auch eigenständig) ergänzend zum Kurs **SC120 ISMS-Implementierung gemäß ISO 27001:2022** besucht werden. Interessant auch für Teilnehmer des Kurses **SC121 Update 2022 für ISO/IEC 27001 / 27002**.

Inhalte/Agenda:

- ♦ **Übersicht über die Standards**

- ♦ **Aufbau eines ISMS – Wesentliche Punkte**

- ♦ **Praxisumsetzung der Anforderungen / Controls**

- ♦ **Gruppe der organisatorischen Anforderungen**
  - ♦ ◊ IS-Incident-Management (Melden und Umgang mit IS-Vorfällen-Tools für Incident-Management, Forensik-Grundlagen, Auswertung von Incidents)
  - ◊ Sicherheit bei Entwicklungsprozessen (Schutz von Testdaten, ausgelagerte Entwicklung, Test-Entwicklungs- und Produktionsumgebung, Entwicklungsmethoden)
  - ◊ Schwachstellen-Management (organisatorische Verknüpfung zum Risikomanagement, technische Methoden des Schwachstellen-Managements, Tools)
  - ◊ Verwaltung der Assets (Tools, Asset-Identifikation, -Identifizierung und -Inventarisierung, CMDB, CIS)
  - ◊ Klassifizierungsrichtlinien (Digital Rights Management, Klassifizierungsstufen, Aufbau- und Inhalte)
  - ◊ Policies (Trennung Privat/Dienst, BYOD, Private Internet- und Email-Nutzung, Kontrollrechte und -pflichten des Arbeitgebers)
  - ◊ Betriebs- und Kommunikationsmanagement, IT-Betriebsprozesse (Change Management, Kapazitätsmanagement)
  - ◊ Beschaffung, Entwicklung und Wartung von Informationssystemen
  - ◊ Benutzerverwaltung (Grundlagen Passwörter, LDAP, Identity- und Access-Management, Activ Directory)
  - ◊ Austausch von Informationen (Austauschvereinbarungen, NDAs, techn. Datenaustausch + Besonderheiten)
  - ◊ Zugang zu Informationen und Anwendungen (Tools, Rollen- und Rechteverwaltung, Audit)

- ♦ **Gruppe der personellen Anforderungen**
  - ♦ ◊ Verantwortung der Benutzer (Umgang mit Passwörtern, Social Engineering, Clear Desk und Clear Screen)
  - ◊ Mobile Computing und Telearbeit (Grundlagen, Organisation und Technik)

- ♦ **Gruppe der physikalischen Anforderungen**
  - ♦ ◊ Zutrittskontrolle (Schutzzonenkonzepte, Zutrittskontrollsysteme, CDTV, Einbruch- und Brandmeldung)
  - ◊ Physische Sicherheit (Verkabelungssicherheit, Stromversorgung, Klimatisierung, Löschanlagen, sicherer Betrieb von Infrastruktur)
- ♦ **Gruppe der technischen Anforderungen**
  - ♦ ◊ Zugangskontrolle für Netze (Grundlagen, Protokolle)
  - ◊ Monitoring (Überwachung der Systeme, Logging, Auswerten von Logfiles, rechtliche Voraussetzung von Monitoring und Logging, Spurensuche)
  - ◊ Kryptographische Maßnahmen (Grundlagen Kryptographie, Verschlüsselungsmethoden z.B. AES und RSA, organisatorische Grundlage Schlüsselmanagement)
  - ◊ Wichtige Sicherheitsprotokolle (SSL/TLS, VPN, IPSEC)
  - ◊ Schutz vor Schadsoftware (Definition, Funktion, Verfahren zum Schutz, Maßnahmen zur Entfernung)
  - ◊ Backup (Backup-Grundlagen, Storage, San, Archivierung, techn. Datensicherung, Backup-Konzepte)
  - ◊ Umgang mit Medien (Endpoint-Security, Verschlüsselung von Medien, sichere Löschverfahren)
  - ◊ Zugriff auf Betriebssysteme (Benutzerverwaltung)

- ♦ **Zusammenfassung und Diskussion**
  - ♦