Praxisbuch ISO/IEC 27001

Management der Informationssicherheit
und Vorbereitung auf die Zertifizierung

DAS VORWORT

Vorwort

Liebe Leserinnen und Leser,

dieses nunmehr in seiner fünften überarbeiteten Auflage vorliegende Buch verfolgt das Ziel, Sie auf Basis des Wortlauts der aktuellen deutschen Fassung der internationalen Norm ISO/IEC 27001 durch die Welt der Informationssicherheitsmanagementsysteme (ISMS) zu begleiten. Es wird Ihnen sowohl bei der Vorbereitung auf eine Personen- oder Organisationszertifizierung als auch bei der praktischen Anwendung als Nachschlagewerk nützlich sein.

Für alle, die sich mit Informationssicherheit und ISMS sowie verwandten Themen wie Datenschutz, IT-Governance, Risikomanagement und Compliance auseinandersetzen, führt branchenübergreifend faktisch kein Weg an ISO/IEC 27001 vorbei. Diese Norm ist seit rund zwei Jahrzehnten der international bewährte gemeinsame Nenner, der sich beispielsweise auch im *IT-Grundschutz* des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) und den *Branchenspezifischen Sicherheitsstandards (B3S)* für Kritische Infrastrukturen wiederfindet. Zuletzt wurde die englische ISO/IEC 27001 im Jahr 2022 deutlich überarbeitet; die 2024 erschienene deutsche Fassung, DIN EN ISO/IEC 27001:2024-01, ist in Anhang B dieses Buchs im Originallayout vollständig abgedruckt.

Die ersten drei Buchkapitel führen Sie zunächst kompakt in die spannende, aber auch komplexe Welt der ISMS und der Normenreihe ISO/IEC 27000 ein. In den Kapiteln 4 und 5 werden alle Anforderungen und Maßnahmen aus der DIN EN ISO/IEC 27001 in grau hinterlegten Kästen im Wortlaut wiedergegeben, im Sinne einer verständlichen Einführung im Einzelnen erläutert und mit Umsetzungsbeispielen sowie ergänzenden Hinweisen aus der Praxis angereichert. Anschließend zeigt Kapitel 6 Schnittstellen zu verwandten Standards und Rahmenwerken auf. Kapitel 7 erläutert die Vorgehensweisen bei der Zertifizierung von ISMS sowie bei der Personenqualifizierung. In Anhang A dieses Buchs finden Sie zudem alle in der DIN EN ISO/IEC 27000 definierten Fachbegriffe im Wortlaut.

Die Schwerpunkte unserer Erläuterungen orientieren sich an den Prüfungsinhalten zu den Foundation-Lehrgangskonzepten u. a. von APMG, ICO und der TÜV Süd Akademie. Jeweils am Ende der Kapitel 1 bis 7 finden Sie in Summe 40 exemplarische Prüfungsfragen, deren Schwierigkeitsgrad und Format der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie entsprechen, aber ein auch von anderen Anbietern häufig verwendetes Prüfungsschema darstellen. In Anhang C sind 40 weitere Prüfungsfragen am Stück abgedruckt; dies entspricht dem Umfang der „richtigen" Prüfung, sodass Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln können. Die begründeten Musterlösungen zu allen 80 Prüfungsfragen finden Sie dort ebenfalls.

Wir wünschen Ihnen viel Erfolg bei der Zertifizierung und der praktischen Anwendung!

München, im Juli 2024 *Die Autoren*

Aufgrund der besseren Lesbarkeit haben wir auf eine gendergerechte Sprache verzichtet. Selbstverständlich sprechen wir aber alle Personen jeglichen Geschlechts gleichermaßen an.

Verweise auf *Kapitel* beziehen sich ohne weitere Angabe immer auf dieses Buch. Verweise auf *Abschnitte* beziehen sich immer auf den entsprechenden Standard.