Erwerben Sie die spezifischen Kenntnisse eines IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) für die Planung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 und ISO 27002

Die **Haupttätigkeit** eines IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) besteht darin, die Geschäftsführung bei der Wahrnehmung ihrer Pflichten zur Sicherstellung eines angemessenen **Informationssicherheitsniveaus** zu unterstützen und den spezifischen **Schutzbedarf** der Unternehmenswerte bei der Ausführung der Geschäfts- und Produktionsprozesse zu **identifizieren**.

Weitere Aufgaben, die in die Zuständigkeit eines ITSiBe / CISO fallen, sind die Abstimmung und Koordination der **Informationssicherheitsstrategie**, die Ableitung der **Ziele** zur **Informationssicherheit**, das Erkennen der unternehmensspezifischen **Risikolagen** und **Bedrohungsszenarien** sowie die Kontrolle und Steuerung der nachhaltigen Umsetzung von angemessenen und wirksamen **Sicherungsmaßnahmen**.

Der ITSiBe / CISO muss den IT-gestützten Geschäftsbetrieb in Einklang mit den **Vorgaben** der **Governance**, der **Compliance** und des ordnungsgemäßen **IT-Betriebs** bringen, die Überprüfung eingetretener **Sicherheitsvorfälle** und **Schadensereignisse** initiieren und verbessern sowie insbesondere die Wahrung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität sicherstellen.

Des Weiteren ist für den Aufbau eines organisationsspezifischen Informationssicherheitsmanagementsystems (ISMS) die **erfolgreiche Integration** der Planung, der Kontrolle sowie der Steuerung von **Prozessen** und ergänzenden **Dokumenten** sowie die **Dokumentation** eines **Sicherheitskonzepts** erforderlich.

ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich der Informationssicherheit, der Aufgabenbeschreibung des ITSiBe / CISO sowie des erforderlichen Fachwissens für den Aufbau eines Informationssicherheits-managementsystems (ISMS) gemäß ISO 27001 und ISO 27002.

Die Teilnehmer können nach Abschluss der Ausbildung die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines normkonformen ISMS, bis hin zur Zertifizierungsreife einer Organisation, zur Umsetzung bringen.

INHALT

- Datenschutzrechtliche Anforderungen und Informationssicherheit
- IT-Management und Informationssicherheit
- Die Sicherheitsstrategie
- Ziele der Informationssicherheit
- Bedrohungslagen der Cyber Security
- IT Compliance
- IT Governance
- IT-Sicherheitsgesetz und KRITIS
- Überblick ITIL und COBIT
- IT Controlling
- IT Scorecard
- Kennzahlen und KPIs der Informationssicherheit
- Aufgaben des ITSiBe wie Planung, Kontrolle und Steuerung des ISMS
- Die Sicherheitsorganisation und Verantwortlichkeiten im ISMS
- Fachbegriffe der Normen und der Informationssicherheit
- Die 270xx-Normenreihe
- Zusammenwirken der ISO 27001 und ISO 27002
- Die Informationssicherheitsleitlinie
- Planung, Initiierung, Betrieb, Kontrolle und Aufrechterhaltung eines ISMS
- Ressourcen und Fähigkeiten zum Betrieb eines ISMS
- Verantwortlichkeiten und Rollen im ISMS
- Risikolagen und Bedrohungsszenarien
- Die Strukturanalyse
- Die Schutzbedarfsfeststellung
- Die Definition von Schutzbedarfsklassen
- Vorgehensweise des BSI IT-Grundschutz
- Übersicht IT-Grundschutz-Kompendium
- Die Erstellung eines IT-Sicherheitskonzeptes
- Umsetzung des Informationssicherheitsprozesses
- Risikomanagement gemäß ISO 31000
- Der IT-Risikomanagementprozess
- Das IT Risiko-Assessment
- Die Risikobehandlung und Maßnahmenumsetzung
- IT-Sicherheitszertifizierungen und Auditierung
- Business Continuity Management (BCM) gemäß ISO 22301
- Business Impact Analyse (BIA)
- Erstellung eines IT-Notfallkonzeptes

Abschluss: Teilnahmebestätigung

Optional: Prüfung mit Personenzertifikat (DGI®)

ZIELGRUPPE

- Angehende ITSiBe / CISO
- IT-Leitung / IT-Administratoren
- Verantwortliche in der Informationssicherheit
- Verantwortliche im Risikomanagement
- Verantwortliche im Business Continuity Management
- Verantwortliche in der Revision / IT-Revision
- Führungskräfte / Projektleitung
- Datenschutzbeauftragte
- Unternehmensberater / Wirtschaftsprüfer

IHR DOZENT

Herr Ronny Neid

Herr Neid ist Diplom-Betriebswirt sowie u. a. zertifizierter IT-Risk und Business Continuity Manager und IT-Sicherheitsbeauftragter. Als Vorstand | COO der DGI berät Herr Neid im Bereich der IT-Sicherheit und des Datenschutzes und entwickelt Sicherheitskonzepte. Herr Neid doziert zu zahlreichen korrelierenden Themen der Informationssicherheit.

Seminar LUI 2616 | Stand Januar 2020