

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 Informationssicherheitsmanagementsystems (ISMS).

In **Abgrenzung** zu der Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®) wird in dieser Ausbildung vertiefend auf die Ausgestaltung eines organisationspezifischen ISMS gemäß **ISO 27001** und **ISO 27002** eingegangen. Unter Zuhilfenahme von zahlreichen **Leseproben** zu relevanten **Sicherheitskonzepten** eines ISMS werden die Umfänge und die Formulierungen von geforderten Nachweisen des ISMS umfassend dargelegt.

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.

Zielgruppe

- Angehende ISB / ITSiBe / CISO
- IT-Leitung
- IT-Administratoren
- Verantwortliche in der Informationssicherheit
- Verantwortliche in der Revision / IT-Revision
- Führungskräfte
- Projektleitung
- Unternehmensberater
- Wirtschaftsprüfer

Unseren **Seminarkatalog** sowie unsere **aktuellen Termine** finden Sie unter

www.DGI-AG.de

Gerne senden wir Ihnen unverbindlich **weiteres Informationsmaterial** zu.

Akademie der
DGI Deutsche Gesellschaft
für Informationssicherheit AG

Kurfürstendamm 57
D - 10707 Berlin

Telefon +49 30 31 51 73 89 - 10
Fax +49 30 31 51 73 89 - 20

E-Mail AKADEMIE@DGI-AG.de
Web www.DGI-AG.de



IT-Sicherheitsbeauftragter (ITSiBe) /
Chief Information Security Officer (CISO) (DGI®)
gemäß ISO 27001 und BSI IT-Grundschutz

Der IT-Sicherheitsbeauftragte / CISO

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 organisationspezifischen Informationssicherheitsmanagementsystems (ISMS) die **erfolgreiche Integration** der Planung, der Kontrolle sowie der Steuerung von **Prozessen** und ergänzenden **Dokumenten** sowie die **Dokumentation** eines **Sicherheitskonzepts** erforderlich.

Inhalt der Ausbildung

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 BSI IT-Grundschutz

- Rechtliche Anforderungen an die Informationssicherheit
- Datenschutz im Kontext der Informationssicherheit
- Fachbegriffe der Normen und der Informationssicherheit
- IT-Management und Informationssicherheit
- Die Informationssicherheitsstrategie
- Die Informationssicherheitsleitlinie
- 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 / CISO bei der Planung, Kontrolle und Steuerung des ISMS
- Befugnisse des ITSiBe / CISO
- Die Sicherheitsorganisation und Rollen im ISMS
- Verteilung der Verantwortlichkeiten des ISMS auf der Basis des „PDCA-Modells“
- Die 270xx-Normenreihe
- Zusammenwirken der ISO 27001 und ISO 27002

- Planung, Initiierung, Betrieb, Kontrolle und Aufrechterhaltung eines ISMS
- Wesentliche Schritte für die Einführung eines ISMS
- Ressourcen und Fähigkeiten zum Betrieb eines ISMS
- Risikolagen und Bedrohungsszenarien
- Integration des ISMS in bestehende Prozesse und Strukturen
- Integration des ISMS bei neuen Vorhaben und Projekten
- Die Inventarisierung und Erfassung des Informationsverbundes
- Die Schutzbedarfsfeststellung
- Das Informationssicherheitsrisikomanagement gemäß ISO 27005 / ISO 31000
- Die IT-Risikobehandlung und Maßnahmenumsetzung
- Die Erstellung eines IT-Sicherheitskonzeptes
- Umsetzung des Informationssicherheitsprozesses
- Best Practice des BSI IT-Grundschutz
- IT-Sicherheitszertifizierungen und Auditierung
- Zusammenwirken mit dem Business Continuity Management (BCM) gemäß ISO 22301
- Kritischer Austausch zu relevanten Fragestellungen (Übungen)

