Informationssicherheitsbeauftragte*r (IHK) - online

IHK ZENTRUM FÜR WEITERBILDUNG

Durch die zunehmende Digitalisierung und Globalisierung sind Unternehmen jeder Größe auf eine funktionierende digitale Infrastruktur angewiesen. Doch gerade in der heutigen Zeit sind Unternehmen einer stetig wachsenden Bedrohungslage und immer ausgefeilteren Angriffsszenarien ausgesetzt. Genau aus diesem Grund gewinnt Informationssicherheit immer mehr an Bedeutung: Sie steht nicht nur für die Sicherung sensibler Informationen oder den Schutz vor ständig neuen Bedrohungsszenarien, sondern gilt als existenzieller Wettbewerbsfaktor. Zudem stellt auch der Gesetzgeber hohe Anforderungen an die gesamte Informationssicherheit, die sich in den kommenden Monaten und Jahren weiter verstärken dürften. Ein wichtiger Schritt zum Schutz vor immer neuen Risiken und Gefahren ist die Aus- und Weiterbildung von Informationssicherheitsbeauftragten. Dieser Zertifikatslehrgang vermittelt das notwendige Fachwissen, um die entscheidenden Schutzmaßnahmen zu ergreifen.

Durch den Grundlagenteil wird sichergestellt, dass auch Mitarbeiterinnen und Mitarbeiter, die über keine vertieften IT-Kenntnisse verfügen, in der Lage sind, alle Inhalte des Seminars zu verstehen.

Ihr Ansprechpartner

Stephanie Bauer

Tel.: 07131 26414-41
Fax: 07131 26414-56
stephanie.bauer@ihk-weiterbildung.de

Informationssicherheitsbeauftragte/r und IT-Sicherheitsbeauftragte/r - wo liegt der Unterschied?

Während Informationssicherheitsbeauftragte für die unternehmensweite Informationssicherheit verantwortlich sind, sind IT-Sicherheitsbeauftragte nur für den Teilbereich der technischen Sicherheit der IT-Infrastruktur, -Systeme und -Anwendungen zuständig. Häufig werden beide Funktionen von derselben Person wahrgenommen. Im englischen Sprachgebrauch wird keine Unterscheidung getroffen (Chief Information Security Officer = CISO). In diesem Lehrgang wird das Wissen für angehende Informationssicherheitsbeauftragte vermittelt, welches das notwendige Wissen für IT-Sicherheitsbeauftragte beinhaltet.

Dieses Seminar richtet sich an:

Dieses Seminar richtet sich an angehende Informationssicherheitsbeauftragte, IT-Projektleiter*innen, IT-Administratorinnen und -Administratoren sowie sämtliche Mitarbeitende der IT oder anderen Abteilungen, die aktuelle oder zukünftig Informationssicherheit im Unternehmen organisieren und gewährleisten müssen.

Ihr Abschluss:

IHK-Zertifikat Informationssicherheitsbeauftragte*r (IHK)

02.06.2025–06.06.2025
online
Seminar-Nr.: 6513_251_02
Voraussichtliche Termine
02.06.2025, 03.06.2025, 04.06.2025, 05.06.2025, 06.06.2025

Dauer: ca. 40 UStd.
Zeiten: 08:30 - 16:30 Uhr

€ 1.590,–

Inhalt:

Modul 1 - Grundlagen der Informationssicherheit und regulatorische Rahmenbedingungen

- Teil 1: Einführung in die Informationssicherheit
  - Grundlegende Definitionen

    - Aktuelle Fallbeispiele
    - Ziele der Informationssicherheit
    - Informationssicherheitsmanagement
- Teil 2: Aufgabenübersicht
    - Informationssicherheitsbeauftragter
    - IT-Sicherheitsbeauftragter
    - Informationssicherheitsmanagement-Team
- Teil 3: Zuständigkeiten verschiedener Behörden
    - BSI
    - ENISA
    - Datenschutzaufsichtsbehörden
- Teil 4: Gesetzliche Grundlagen
    - Überblick
    - Kernbereiche des IT-Sicherheitsrechts
    - Randbereiche und aktuelle Entwicklungen (u.a. NIS-2, KI und Datenschutz)
- Teil 5: Verwaltungsanweisungen und Standards
- Teil 6: Relevante Vertragsfragen im Bereich IT / Informationssicherheit
    - IT-Outsourcing
    - Penetrationstests
    - Versicherungen
- Teil 7: Rechtsfolgen
    - Haftung von Leitungsebenen
    - Sanktionen

Modul 2 - Rollen und Zuständigkeiten und Informationssicherheitsmanagement

- Teil 1: Sinn und Zweck klarer Rollenverteilung
- Teil 2: Beschreibung verschiedener Rollen und Aufgabengebiete im Kontext der Informationssicherheit
    - Geschäftsleitung
    - Abteilungsleitungen
    - Verschiedene Bereichsbeauftragte (z.B. Informationssicherheitsbeauftragter, Datenschutzbeauftragter)
- Teil 3: Einführung zum Thema Informationssicherheitsmanagement
    - Definition von Managementsystemen
    - Hauptkomponenten eines ISMS
    - Ablauf und Mehrwert einer Zertifizierung
    - Überblick zu verschiedenen ISMS-Standards
- Teil 4: Aufbau und Pflege eines ISMS nach BSI IT-Grundschutz
    - Einführung und relevante Standards
    - Wahl der Vorgehensweise / Absicherungsmethodik
    - Vorgehensweise nach BSI (Standard-Absicherung)
    - Kontinuierliche Verbesserung
    - Musterdokumentation
- Teil 5: Aufbau und Pflege eines ISMS nach ISO/IEC 27001
    - Relevante Standards der ISO 27000er-Reihe
    - Umgang mit der ISO 27001
    - Prozessbeispiele
- Teil 6: Tools und Best-Practices bei der Einführung eines ISMS
    - Unterschiedliche Vorgehensweisen
    - Unterstützung durch ISMS-Tools in der Praxis

Modul 3 - Aktuelle Risiken für die Informationssicherheit und Schutzmaßnahmen

- Teil 1: Risikomanagement nach BSI-Standards 200-3
    - Vorbereitung
    - Überblick über elementare Gefährdungen
    - Vorgehensweise (insbesondere Risikobewertung und -behandlung)
- Teil 2: Business-Continuity-Management (BCMS) nach BSI-Standard 200-4
    - Einführung BCMS und präventive Absicherung
    - BCMS-Stufenmodell
    - Notfallplanung
    - Schulung und Sensibilisierung
    - Sonstige Maßnahmen und Tools für Risikofrüherkennung
    - Reaktion im Ernstfall - Bedeutung von Incident Response Teams

Modul 4 - Rollen und Zuständigkeiten und Informationssicherheitsmanagement

- Teil 1: Aktuelle Bedrohungsszenarien (Fallbeispiele)
    - Ransomware-Angriffe
    - Angriffe auf KRITIS, IT-Dienstleister und Co.
    - Social-Engineering - Der Mensch im Fokus von Angreifern
- Teil 2: Kategorisierung von Risiken
    - Webbasierte Risiken
    - Systembezogene Risiken
    - Anwendungsbezogene Risiken
    - Nutzerbezogene Risiken
- Teil 3: Einführung und Überblick zu Schutzmaßnahmen
    - Was sind Maßnahmen?
    - Dokumentationspflichten
    - Maßnahmenkategorien
- Teil 4: Strukturierte Vorgehensweise zur Umsetzung von Maßnahmen
    - BSI IT-Grundschutz-Methodik
    - Anwendung der Bausteine des IT-Grundschutz-Kompendiums
    - Vergleich zur ISO 27001 (Anhang A)
- Teil 5: Konkrete Beispielmaßnahmen
    - Organisatorische Schutzmaßnahmen
    - Technische Schutzmaßnahmen
    - Menschenbezogene Schutzmaßnahmen
    - Physische Schutzmaßnahmen

Der schriftliche Zertifikatstest findet online statt.

Anmeldung

Telefon: 07131 26414-41 • Fax: 07131 26414-56
E-Mail: stephanie.bauer@ihk-weiterbildung.de

IHK
ZENTRUM FÜR WEITERBILDUNG

IHK-Zentrum für Weiterbildung
Ferdinand-Braun-Straße 20
74074 Heilbronn

Anmeldung

Seminarnummer Beginn/Datum	Seminartitel	Teilnehmer (Titel, Vor- und Zuname)	Geburtsdatum Geburtsort	Funktion im Betrieb, Ausbildungsberuf (nur bei Azubi-Seminaren ausfüllen)

Postadresse:

Firma oder Name, Vorname

Straße/Hausnummer

PLZ/Ort

Mit welcher Softwareversion arbeiten Sie? (nur bei EDV-Seminaren ausfüllen)

Telefon

Mobil

E-Mail

Ansprechpartner/-in für Weiterbildung in unserem Unternehmen

Rechnungsadresse:

(bei abweichender Rechnungsadresse)

Firma oder Name, Vorname

Straße/Hausnummer

PLZ/Ort

Telefon/Fax

E-Mail

Bitte ankreuzen

- ☐ Ich habe die AGB und das Widerrufsrecht für Verbraucher auf der Website (www.ihk-weiterbildung.de/agb) gelesen und bin damit einverstanden.
- ☐ Ich willige in die Verarbeitung und Nutzung meiner personenbezogenen Daten gemäß der Datenschutzerklärung ein.
- ☐ Senden Sie mir 2× jährlich Ihr Weiterbildungsprogramm per Post.

Ort, Datum

Unterschrift