

# Informationssicherheitsbeauftragte\*r (IHK) - online

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-

### Diese Website verwendet Cookies

Wir verwenden Cookies, um Ihnen ein optimales Webseiten-Erlebnis zu bieten. Dazu zählen Cookies, die für den Betrieb der Seite und für die Steuerung unserer kommerziellen Unternehmensziele notwendig sind, sowie solche, die lediglich zu anonymen Statistikzwecken genutzt werden. Sie können selbst entscheiden, welche Kategorien Sie zulassen möchten. Bitte beachten Sie, dass auf Basis Ihrer Einstellungen womöglich nicht mehr alle Funktionalitäten der Seite zur Verfügung stehen. Weitere Informationen finden Sie in unseren Datenschutzhinweisen.

- Notwendig
  - Statistiken
  - Marketing
- Auswahl bestätigen Alle auswählen

#### Details

##### Notwendig (2)

##### Statistiken (2)

##### Marketing (2)

Notwendige Cookies helfen dabei, eine Webseite nutzbar zu machen, indem sie Grundfunktionen wie Seitennavigation und Zugriff auf sichere Bereiche der Webseite ermöglichen. Die Webseite kann ohne diese Cookies nicht richtig funktionieren.

Name	Anbieter	Zweck	Ablauf
wire	ihk-weiterbildung.de	Der Cookie ist für die sichere Anmeldung und die Erkennung von Spam oder Missbrauch der Webseite erforderlich.	Session
cmnstr	ihk-weiterbildung.de	Speichert den Zustimmungsstatus des Benutzers für Cookies.	1 Jahr

Statistik-Cookies helfen Webseiten-Besitzern zu verstehen, wie Besucher mit Webseiten interagieren, indem Informationen anonym gesammelt und gemeldet werden.

Name	Anbieter	Zweck	Ablauf
_ga_PF07PMP11H	Google	Wird verwendet, um Daten zu Google Analytics über das Gerät und das Verhalten des Besuchers zu senden. Erfasst den Besucher über Geräte und Marketingkanäle hinweg.	2 Jahre
_ga	Google	Registriert eine eindeutige ID, die verwendet wird, um statistische Daten dazu, wie der Besucher die Website nutzt, zu generieren.	2 Jahre

Wir verwenden Marketing-Cookies, um Besuchern auf Webseiten zu folgen und für sie relevante Anzeigen und Kampagnen auszuspielen.

Name	Anbieter	Zweck	Ablauf
_fbp	Facebook	Wird von Facebook genutzt, um eine Reihe von Werbeprodukten anzuzeigen, zum Beispiel Echtzeitgebote dritter Werbetreibender.	90 Tage
ln_or	LinkedIn	Wird von LinkedIn für zur Identifizierung des Browsers, Speicherung von Spracheinstellungen und für die Aussteuerung von Anzeigen verwendet.	1 Tag

Impressum

- 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  
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)
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

## 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

\_\_\_\_\_  
Ort, Datum

## 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](http://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.

\_\_\_\_\_  
Unterschrift