Informationssicherheitsbeauftragter / Chief Information Security Officer CERT/CISO

3 Lernmodule / 3 Referenten / 1 Gesamtzertifikat

IT-Sicherheitsbeauftragte(r) / Informationssicherheitsbeauftragte(r) nach ISO27001 & BSI IT-Grundschutz

Dieser 5-tägige CISO-Kurs behandelt die Grundlagen der organisatorischen (ISO27001 & BSI IT-Grundschutz) und technischen IT-Sicherheit (Basic Begrifflichkeiten) sowie die rechtliche Betrachtung und DSGVO.
Kurs in deutscher Sprache - Deutsche Schulungsunterlagen - Deutsche Prüfung

Die Position eines CISO wird in den Unternehmen oft unterschiedlich bezeichnet:

- Chief Information Security Officer (CISO)
- Information Security Officer (ISO)
- Chief Information Security Manager (CISM)
- IT-Sicherheitsbeauftragter (IT-SB oder IT SiBe)
- Informationssicherheitsbeauftragter (ISB)

Die Aufgaben, die diesen Rollen zugewiesen werden, können dazu in den diversen Unternehmensstrukturen voneinander abweichen.
Zertifikat "Chief Information Security Officer (CISO)"
Unser Experten-Zertifikat ermöglicht es Ihnen Ihre Kompetenz im Umfeld der Informationssicherheit eindeutig zu belegen.

Listenpreis
3.390,00 € exkl. MwSt
4.034,10 € inkl. MwSt

Dauer
5 Tage

Gebühr für Prüfungen/Examen
350,00 € exkl. MwSt / 416,50 € inkl. MwSt

Prüfungsversicherung
159,00 € exkl. MwSt / 189,21 € inkl. MwSt

Leistungen Präsenz
- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training
- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin


Manuela Krämer
Leitung Informationssicherheit

Kontakt/Fragen:
m.kraemer@cbt-training.de
Telefon: +49 (0)89-4576918-12

Inhalte
Seminare zur Ausbildung eines Informationssicherheitsbeauftragten gibt es einige, aber was sollte eine Basic Ausbildung an Inhalten bieten?

Wir haben über Jahre hinweg unseren Zertifizierungskurs auf stetig neue Anforderungen des CISO angepasst und erweitert.

Die Aufgaben und die Verantwortung des CISO werden immer umfangreicher. Unser langjähriges erfahrenes Referenten-Team, bestehend aus 3 Experten, begleitet die Teilnehmer praxisnah durch unseren 5-Tages-Kurs mit folgenden brisanten Themenbereichen:

1. Tag und 2. Tag Modul 1: Informationssicherheitsmanagement auf Basis von ISO 27001 und BSI IT-Grundschutz

Referent (Profil unter Dozent) ISMS-Management, ISO 27001 Lead Auditor, Qualitätsmanager

- **Einführung in die Informationssicherheit/IT-Sicherheit**
  - Grundwerte / Definition der Sicherheitsziele
  - Informationssicherheitsprozess
  - Rahmenwerk (IS-Framework)
  - Gesetzliche Vorgaben und Verpflichtungen
- **Aufgaben des Verantwortlichen für Informationssicherheit**
  - Anforderungprofil nach BSI Standard 200-2
  - IS-Management-Team und deren Aufgaben
  - Risikomanagement & Risikoanalyse nach ISO27005
- **Informationssicherheitsmanagement nach Normen und Standards ISO/IEC27001**
  - Rahmenwerke & Standards
  - ISO/IEC 27001:2022 (inkl. Erläuterung Änderungen von 2013 zu 2022)
  - ISO/IEC 2700x Normreihe
  - Plan Do Check Act Cycle (PDCA)
- **Einführung eines ISMS im Unternehmen**
  - Betrieb, Überwachung und Bewertung eines ISMS
  - Wartung und Verbesserung des ISMS
  - Grundlagen zur Implementierung
- **Informationssicherheitsmanagementsystem (ISMS) und Zertifizierung ISO/IEC 27001**
- **BSI IT-Grundschutz nach ISO 27001 und seine Anwendungen**
  - BSI-Standard 200-1 / 200-2 / 200-3 / 200-4
- **BSI Standards für IT-Sicherheit**
- **IT-Grundschutz-Kompendium des BSI**
  - Schichtenmodell / Bausteine / Dokumentstruktur / Umsetzungshinweise
  - Komponenten eines ISMS - Managemetnsystem für IS 200-1
  - Umsetzung Sicherheitsstretegie / SIcherheitskonzept
  - Aufgaben und Pflichten des Managements
  - Das ISMS des BSI (Sicherheitsprozess)
  - Lebenszyklus des Sicherheitskonzepts / Sicherheitskonzeption
  - Strukturanalyse
  - Schutzbedarf
  - IT-Grundschutz-Check
  - Risikoanalyse - Riskmanagement BSI Standard 200-3
  - Realisierung von Sicherheitsmaßnahmen

3. Tag und 4. Tag Modul 2: Cyber Security Grundlagen der IT-Sicherheit- und Informationssicherheit, aktuelle Bedrohungslage / Lösungen

Referent (Profil unter Dozent) Security Consultant

- Praxisrelevante Angriffsszenarien
  - Übersicht über praxisrelevante und verbreitete Angriffsszenarien
  - Erkennungsmöglichkeiten und Ersthilfemaßnahmen
  - Folgerungen für die eigene IT-Sicherheit
- Grundprinzipien der Cyber-Security
- Physische Sicherheit
  - Zutrittskontrollsysteme
  - Video-Überwachung
  - Bauliche Maßnahmen
- Technische Absicherungsmaßnahmen im Überblick
- Prinzip des geringsten Rechts
- Anwendungsbeispiele innerhalb des BSI Grundschutz

  - Interpretation eines Bausteins
  - Handlungsalternativen
  - Umsetzung
- Anwendungsbeispiele innerhalb der ISO Normen
  - Grundsätzliche Anforderungen
  - Folgerungen für die eigene Umsetzung
- Spezialfälle

5. Tag Modul 3: IT-Recht Kompakt für den IS-Beauftragten/ITSIBE bzw. Chief Information Security Officer
Dozent: Rechtsanwalt mit dem Tätigkeitsschwerpunkt IT-Recht und Datenschutz

- Überblick IT-Security: Rechtliche, organisatorische und technische Problemfelder
- IT-Compliance im Detail
- Stellung und Haftung des IT-SiBe/CISO im Unternehmen
- Einführung in den Datenschutz (DSGVO/BDSG)
- IT-Sicherheitsgesetz 2.0 / NIS-Richtlinie EU
- Private E-Mail/Internet Nutzung am Arbeitsplatz
- Content Scanning / Filtering
- Computerstrafrecht und Cybercrime
- Datenschutzkonforme Protokollierung im Unternehmen

Nach jedem Lernmodul erhalten Sie eine Zusammenfassung der Schulung, Besprechung der noch offenen Fragen mit anschließender optionalen Prüfung.

Nach dem Kurs sollte der Teilnehmer sich weiteres ISMS sowie auch Cyber Security Knowhow aneignen, um seine tägliche Herausforderungen meistern zu können.

Ziele

- Der Teilnehmer kennt nach dem Seminar das Vorgehen zur Initiierung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS) nach dem international anerkannten ISO/IEC 27001 Standard sowie die deutschen IT-Grundschutzstandards und das IT-Grundschutz-Kompendium des BSI Bundesamtes für Sicherheit in der Informationstechnik sowie die gesetzlichen Rahmenbedingungen.
- Dem Teilnehmer wird ermöglicht, die Position des IS-Beauftragten zu gestalten, sein Anliegen als Sicherheitsbeauftragter gegenüber der Unternehmensleitung, dem Management und den Mitarbeitern zu vertreten, das Unternehmen sicherheitstechnisch zu analysieren und Sicherheitsmaßnahmen zu ergreifen.
- Das Seminar behandelt neben den organisatorischen Aspekten der Informationssicherheit auch an 2 Tagen einen weitreichenden Überblick über aktuelle, technische Schutz- und Verteidigungseinrichtungen (IT-Sicherheit). Der Referent erläutert hierbei knapp die theoretischen Grundlagen verschiedener Sicherheitssysteme und bespricht ausführlich praktische Anwendungsfälle dieser Einrichtungen.
- Der 5. Tag steht im Brennpunkt des IT-Rechts mit EU-DSGVO und wird von einen Rechtsanwalt mit Tätigkeitsschwerpunkt IT-Recht und Datenschutz geschult.

- SPEZIELL FÜR ENERGIEVERSORGER:
  - Auf die individuellen Anforderungen des IT-Sicherheitskataloges und den Normanforderungen der DIN ISO/IEC 27001, den verbindlichen Maßnahmen des Anhangs A der DIN ISO/IEC 27001 und der DIN ISO/IEC TR 27019 (DIN SPEC 27019) im Bereich der Prozesssteuerung der Energieversorgung kann im Seminar eingegangen werden. - Teilnehmer sollten diesen Wunsch einfach äußern!

Zielgruppe

- Im IT-Sicherheitsgesetzes werden Kritis zur Implementierung eines ISMS und zur Benennung eines Ansprechpartners für Informations-/ IT-Sicherheit verpflichtet. Dieser muss nach ISO/IEC 27001 nicht nur einfach ernannt, sondern durch z.B Schulungen nachweislich auch kompetent sein. Nutzen Sie daher diesen CERT-KURS.

Mitarbeiter aus Unternehmen und Behörden die zum Beauftragten für ITS bzw. zum Security Information Officer ISO bzw. Chief Information Security Officer CISO, Sicherheitsbeauftragten für Informationssicherheit, IT-Sicherheitsbeauftragten bestellt wurden oder bestellt werden sollen.

Aber auch an interessierte Führungskräfte und Mitarbeiter des Sicherheitsmanagements, Leiter der Informationssicherheit, Systemadministratoren und IT-Manager.

Voraussetzungen

Es werden keine weiteren besonderen Vorkenntnisse benötigt. Grundverständnisse zu IS und IT sind vorteilhaft.

Prüfung/Zertifizierung

CERT CISO Chief Information Security Officer

Multiple-Choice Prüfungen, deutsch
Alle 3 Teilprüfungen werden als eine Gesamtprüfung gewertet.

Prüfung zum CBT CERT Zertifikat:

Die Prüfung erfolgt schriftlich als Multiple-Choice Prüfung. Die CBT CERT Prüfung wird direkt nach Kursende abgenommen. Sie gilt als bestanden, wenn mindestens 70% der Fragen richtig beantwortet wurden.

Nach Bestehen der Prüfung erhalten Sie ein personenbezogenes CBT CERT Zertifikat ,das Ihnen die erfolgreiche Kursteilnahme inklusive bestandener Prüfung bestätigt.

Hat ein Teilnehmer die CBT CERT Prüfung nicht bestanden, so kann er diese entweder direkt im Anschluss an die erste Prüfung oder während unserer Öffnungszeiten Online Live mit Prüfungsüberwachung (Kamerapflicht, MS-Teams) nach vorheriger schriftlicher Anmeldung (mind. 14 Tage vor Termin) gegen die genannte Prüfungsgebühr wiederholen. Die Prüfung kann höchstens 2-mal wiederholt werden. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Prüfungsversicherung zum CBT CERT:

Haben Sie zum Kurs und zur Prüfungsgebühr unsere Prüfungsversicherung bestellt, berechtigt diese zur einmaligen kostenfreien Prüfungswiederholung zu o.g. Bedingungen. Die Prüfungswiederholung muss innerhalb von 3 Monaten nach Kursbesuch erfolgt sein.

Ohne Prüfungsversicherung zahlen Sie bei Wiederholung die volle Prüfungsgebühr.

Gültigkeit CBT CERT ZERTIFIKAT:

Das CBT CERT Zertifikat ist 3 Jahre gültig und muss anschließend durch eine erneute Prüfung bei CBT Training & Consulting GmbH aktualisiert / verlängert werden.

Alle Prüfungsunterlagen werden 3 Jahre aufbewahrt.

Hinweise

Häufig verwendete Titel:

- IT-Sicherheitsbeauftragter ITSIBE, Chief Security Officer CSO, Chief Information Security Officer CISO, Information Security Manager CISM - je nach Art und Ausrichtung der Institution.

Anforderungsprofil ITSIBE / CISO:

- Hierzu finden Sie im BSI-Standard IT-Grundschutz Information. Die ganzheitliche Ausrichtung unseres Kurses gewährleistet die Berücksichtigung sowohl der technischen, juristischen als auch organisatorischen Aspekte!

HINWEIS:
Die Module können teilweise in der Reihenfolge aus Termingründen getauscht werden.
