

# IT-Security-Beauftragter (TÜV).

**Lernen Sie als IT-Sicherheitsbeauftragter in Modul 1 mehr über die Organisation einer optimalen Informationssicherheit.**



Seminar



38 Termine verfügbar



Zertifikat



Präsenz / Virtual Classroom



32 Unterrichtseinheiten



Garantietermine vorhanden

---

Seminarnummer: 31110

Stand: 05.02.2026. Alle aktuellen Informationen finden Sie unter <https://akademie.tuv.com/s/31110>

Die Sicherheit sensibler Daten, Informationen und Prozesse gewinnt immer mehr an Bedeutung. Ein optimales und zuverlässiges Informationssicherheits-Managementsystem ist dafür unerlässlich. Im Kurs lernen Sie als IT-Security-Beauftragter, wie Sie das Schutzniveau Ihrer Institution steigern und diese vor Gefährdungen bewahren. Der Schwerpunkt liegt dabei auf der Einführung eines ISMS nach ISO 27001.

## Aufbau:

Der Ablauf der Weiterbildung auf einen Blick:

### Live Training

Gruppenphase

Präsenz oder Virtual Classroom

### Serious Game

Spielerische Wissensvertiefung

### Fit for Test App

Unterstützende Prüfungsvorbereitung (optional)

Selbstlernphase

## **Prüfung**

PersCert-Prüfung am letzten Seminartag in Präsenz oder Online

## Nutzen

- Sie verfügen über aktuelles Wissen über die Anforderungen der relevanten Standards (wie ISO/IEC 27001 und IT-Grundschutz nach BSI) und deren Umsetzung.
- Sie wissen, welche Aspekte und Anforderungen der Informationssicherheit zu beachten sind.
- Sie können mit dem anerkannten Zertifikat Ihr erworbenes Fachwissen dokumentieren.

## Zielgruppe

- IT-Leiter
- verantwortliche Personen aus den Bereichen Informationssicherheit, Informationstechnologie, IT-Organisation, IT-Beratung, Revision und Risikomanagement.

## Voraussetzungen

Die Zulassungsvoraussetzungen zur Teilnahme an der von PersCert TÜV, der unabhängigen Personenzertifizierungsstelle von TÜV Rheinland, durchgeföhrten Prüfung, finden Sie auf [ID-Nr. 0000085846: IT-Security-Beauftragte:r \(TÜV\) - Certipedia](#).

Der Lehrgang wendet sich an Einsteiger in die Materie der Informationssicherheit und behandelt schwerpunktmaßig die rechtlichen Grundlagen, Normen und Vorschriften im Detail. Die Informationstechnologie / IT wird auf einer allgemeinen Ebene behandelt und nicht im Detail.

## Abschluss

### **Zertifikat**

Zur Feststellung Ihrer erworbenen Kompetenz wird eine Prüfung von PersCert TÜV, der unabhängigen Personenzertifizierungsstelle von TÜV Rheinland, durchgeföhrte.

Nach erfolgreichem Abschluss des Prüfungs- und Zertifizierungsverfahrens erhalten Sie von PersCert TÜV ein Zertifikat mit dem Abschlusstitel „IT-Security-Beauftragte:r (TÜV)“ als persönlichen Kompetenznachweis. Dokumente und Informationen (u.a. Zulassungsvoraussetzungen, Prüfungsinhalte

und Ablauf, Gültigkeit, Rezertifizierung, etc.) zum Zertifizierungsprogramm finden Sie auf [www.certipedia.com](http://www.certipedia.com) unter der Programm ID 85846.

Nutzen Sie zusätzlich nach erfolgter Zertifizierung die zahlreichen Möglichkeiten eines persönlichen TÜV Rheinland Prüfzeichens mit Ihrer individuellen ID als Werbesignet zu den unter [www.tuv.com/perscert](http://www.tuv.com/perscert) dargestellten Bedingungen. Stärken Sie mit Ihrem Zertifikat und dem damit verknüpften Prüfzeichen das Vertrauen bei Kunden und Interessenten.

## Inhalte des Seminars

### **Erster Seminartag**

Grundlagen der Informationssicherheit

- Aktueller Stellenwert der Informationssicherheit
- Grundlegende Begriffe
- Cyberkriminalität

Rechtlicher Rahmen der Informationssicherheit

- Überblick zu einschlägigen Gesetzen
- IT-Sicherheitsgesetz, NIS2
- Datenschutz

Relevante Standards

- ISO 2700x
- BSI IT-Grundsatz

### **Zweiter Seminartag**

Handhabung von Informationssicherheitsvorfällen

- Verantwortlichkeiten und Verfahren
- Mögliche Ursachen für Informationssicherheitsvorfälle

Informationssicherheitsmanagementsystem nach ISO 27001

- Managementsysteme und ihre Regelkreise
- Struktur eines ISMS nach ISO 27001
- Dokumentation des ISMS nach ISO 27001
- Möglichkeiten der toolbasierten Dokumentation

Kontext - Anwendungsbereich - Werte - Leitlinie

- Kontext der Organisation und interessierte Parteien
- ISMS-Scope / Anwendungsbereich

- Führung und Unterstützung

- Assets / Werte

## Organisation der Informationssicherheit

- Grundlagen
- Rollen im Informationssicherheitsprozess
- IT-Security-Beauftragter
- Haftung
- Kommunikation und Berichtswege im ISMS
- Kontakt zu Behörden und speziellen Interessengruppen
- Informationssicherheit im Projektmanagement

## Dritter Seminartag

### Technische Maßnahmen und Maßnahmenziele

- Access Management

- Netzwerksicherheit

■

- Technische Schutzmaßnahmen
- Cloud Security
- Remote Zugriff
- Systeme zur Angriffserkennung

■

- IT-Betrieb

■

- Dokumentierte Bedienabläufe und Änderungsmanagement
- Datensicherung und Backup
- Schadsoftware
- Logging
- Steuerung von Software im Betrieb
- Handhabung technischer Schwachstellen
- Umgang mit Mobilgeräten

■

- Schutz vor externen und umweltbedingten Bedrohungen
- Bedrohungen der Infrastruktur

### Security Awareness

- Sicherheitsbewusstsein im Unternehmen

- Security Awareness – Ein Konzept

- - Formale Gründe für ein Security Awareness Konzept
  - Hinweise für ein Security Awareness Konzept
  
- - Beispielhaftes Security Awareness Konzept
  - Umsetzungshinweise für Kampagnen
  - Beispiele für Sensibilisierungsmaßnahmen

Die ISO 27001

- Normkapitel ISO 27001
- Controls ISO 27001
- Neue Controls der ISO 27001:2022

## Vierter Seminartag

Grundlagen des Risikomanagements

Notfallmanagement und Business Continuity Management nach BSI 200-4

- Überblick und Begriffe
- Besonderheiten im BSI-Standard 200-4
- Initiierung des BCMS
- Konzeption und Planung des BCMS
- Aufbau und Befähigung der BAO
- Absicherung der Geschäftsprozesse
- Tests und Übungen
- Aufrechterhaltung und Verbesserung des BCMS

TÜV Zertifikatsprüfung

## Wichtige Hinweise

- Alle IT-Security-Zertifikate (TÜV) haben für neue Zertifizierungen ab dem 1.7.2018 eine Gültigkeit von 3 Jahren.  
Die Rezertifizierung kann erfolgen bei einem Nachweis über die fortgesetzte berufliche Tätigkeit im Fachgebiet und zusätzlicher Teilnahme an mindestens einer fachrelevanten Weiterbildung im Gültigkeitszeitraum des Zertifikats, im Mindestumfang von 8 UE. Der Nachweis kann z.B. durch Kopie von Teilnahmebescheinigung erfolgen. Details entnehmen Sie bitte dem jeweiligen Certipedia-Eintrag.
- Als zusätzliches Angebot erhalten Sie einen 8-wöchigen kostenfreien Vollzugriff auf die Online-Publikation „[IT-Servicemanagement digital ↗](#)“ – das Praxiswerk zu Compliance und Wirtschaftlichkeit in der IT zur Vertiefung Ihres Wissens..
- Dieses Seminar bieten wir mit einer digitalen Prüfungsvorbereitung „Fit for Test“ an. Ein Multiple Choice Test über die Lerninhalte zur optimalen Prüfungsvorbereitung. Die Nutzung ist kostenfrei.

Weitere Info unter: <https://akademie.tuv.com/lernformate/fit-for-test>. Den Zugang erhalten Sie am Beginn des Seminares.

- Zusätzlich erhalten Sie einen 3-wöchigen und kostenfreien Zugriff auf unser Information Security-Awareness-Game. Dieses "Serious Game" präsentiert eine hervorragende Möglichkeit, wie Unternehmen Mitarbeiter:innen hinsichtlich der Bedeutung von Informationssicherheit sensibilisieren und schulen können.

## Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter <https://akademie.tuv.com/s/31110> und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.