

## Ziel der Ausbildung

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich der Durchführung eines Audits gemäß ISO 19011, der Aufgabenbeschreibung des Lead Auditors ISO 27001 und des erforderlichen Fachwissens für die Auditierung eines ISMS.

Die Teilnehmer können nach Abschluss der Ausbildung die Durchführung eines ISMS-Audits planen sowie eine Bewertung des bestehenden ISMS vornehmen.

## Voraussetzungen

Der vorherige Besuch einer Ausbildung zum IT-Sicherheitsbeauftragten / Informationssicherheitsbeauftragten oder vertiefte Kenntnisse im Bereich der Informationssicherheit werden vorausgesetzt

## Zielgruppe

- Informationssicherheitsbeauftragte / IT-Sicherheitsbeauftragte
- Verantwortliche in der Informationssicherheit
- Verantwortliche im IT-Risikomanagement
- Verantwortliche in der IT-Compliance
- IT-Revisoren
- Unternehmensberater

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

[www.DGI-AG.de](http://www.DGI-AG.de)

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



## Lead Auditor ISO 27001 (DGI®)

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](mailto:AKADEMIE@DGI-AG.de)  
Web [www.DGI-AG.de](http://www.DGI-AG.de)

Foto Titelseite: ©tadamichi | stock.adobe.com  
Foto Innenteil: dock64 | Paul Reichert

## Der Lead Auditor ISO 27001

Die **Haupttätigkeit** eines Lead Auditors ISO 27001 besteht darin, die systematische **Beurteilung** des bestehenden **Informationssicherheitsniveaus** eines Unternehmens vorzunehmen sowie insbesondere die **Angemessenheit** der umgesetzten infrastrukturellen, technischen, organisatorischen und personellen **Maßnahmen** zu bewerten.

Weitere Aufgaben, die in die Zuständigkeit eines Lead Auditors ISO 27001 fallen, sind die **Entwicklung** und **Steuerung** des **Auditprogramms** sowie die **Erstellung** der erforderlichen **Audit-Checklisten** für die Bewertung des ISMS.

Der Lead Auditor ISO 27001 muss die erforderlichen **Audit-Methoden**, wie Stichprobenprüfung, Dokumentenprüfung, Interviewführung oder Begehung von Standorten, **anwenden** können. Er benötigt die Kompetenzen, um die an ein Unternehmen gestellten standort- und branchenspezifischen **Anforderungen** fachgerecht einzubeziehen und die Konformität der Maßnahmenumsetzung sowie die Einhaltung der beabsichtigten Maßnahmenziele festzustellen.

Des Weiteren ist die **Festlegung** von **Kriterien** für die **Bewertung** der **Feststellungen** im Rahmen der Durchführung des **ISMS Audits** sowie für die Erstellung eines **ISMS-Auditberichts** erforderlich.

## Inhalt der Ausbildung

Erwerben Sie die spezifischen Kenntnisse des Lead Auditor ISO 27001 für die Auditierung eines Informationssicherheitsmanagementsystems (ISMS)

- Planung, Zielsetzung und Durchführung eines Audits
- Bestimmung des Anwendungs-bereichs eines Audits (Scope)
- Bestimmung eines Informationsverbundes
- Internes und externes Audit
- Anforderungen an ein Audit und den Auditor
- Fachbegriffe aus Normen
- Fachbegriffe eines Audits
- Auditierung von Konformitäten gegen Rechtsvorschriften, Standards und Normen
- Prüfkriterien gemäß ISO 19011
- Erstellung eines Auditprogramms
- Rollen und Zuständigkeiten im Auditprozess
- Kommunikation im Auditprozess
- Umgang mit Auditrisiken
- Audit-Methoden zur Überprüfung eines Sicherheitskonzepts
- Prüfung der Prozesse und Dokumentationen eines ISMS
- Audit-Checkliste gemäß ISO 27001 und BSI IT-Grundschatz
- Exemplarische Prüfpunkte eines ISMS-Audits
- Prüfung der Aufbau- und Ablauforganisation
- Prüfung der technischen und organisatorischen Maßnahmen
- Beobachtung von Arbeitsabläufen
- Dokumentensichtung und Dokumentenprüfung
- Erfüllung von Nachweispflichten
- Stichprobenprüfung und statistische Analysen
- Vor-Ort-Prüfung
- Interviewteilnehmer
- Interviewführung
- Konformitäten und Abweichungen
- Feststellungen eines ISMS-Audits
- Behandlung von Feststellungen
- Entwicklung, Umsetzung und Nachverfolgung von Korrekturmaßnahmen
- Festlegung von Maßnahmen
- Bewertung der Ergebnisse
- Dokumentation von Feststellungen
- Regelmäßige Überprüfung von Maßnahmen und Revision
- Kontinuierliche Verbesserung
- Inhalte, Gliederung und Erstellung eines ISMS-Auditberichts
- Nachbereitung und Auswertung eines Audits
- Abschlussgespräch zum Audit
- Integration anderer Managementsysteme wie ISO 9001 oder ISO 22301

