



# Seminarkatalog 2024

**Ausbildungen mit Personenzertifikat**  
**Seminare**  
**Workshops**

**Informationssicherheit**

**Business Continuity Management**

**IT-Risikomanagement**

**IT-Sicherheit**

**ICS Security**

**Cybersicherheit**

**Datenschutz**



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)

Zugunsten der besseren Lesbarkeit wurde im Text auf die gleichzeitige Verwendung weiblicher und männlicher Personengruppen (Mitarbeiter, Mitarbeiterin bzw. Mitarbeiter/in) verzichtet und die männliche Nominalform angeführt. Mit dieser Vereinfachung des sprachlichen Ausdrucks soll die Gleichberechtigung der Geschlechter nicht beeinträchtigt werden.

Stand: Dezember 2023

Irrtümer, Druckfehler und Preisänderungen vorbehalten.

© DGI AG 2023



## VORWORT

### WISSEN UND KOMPETENZ

Die ständige Weiterentwicklung der Informationsverarbeitung fordert eine permanente Auseinandersetzung mit den sich ständig verändernden Risiko- und Gefährdungslagen sowie der Verbesserung umgesetzter Sicherheitskonzepte. So muss das Thema Informationssicherheit, insbesondere vor dem Hintergrund wachsender Globalisierung, Vernetzung und Mobilität sowie immer komplexeren Systemen der Informationsverarbeitung, als ein zentraler strategischer Faktor für den Fortbestand und die Wettbewerbsfähigkeit der eigenen Organisation angesehen werden.

Die Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG bietet seit Jahren erfolgreich Ausbildungen mit Personenzertifikat, Seminare und Workshops in allen korrelierenden Bereichen der Informationssicherheit an, um einen erfolgreichen Wissensaufbau und die Stärkung der persönlichen Kompetenzen der Teilnehmer durch eine angemessene Qualifizierung sicherzustellen.

Unsere Bildungsangebote orientieren sich an den Anforderungen unserer Kunden aktuelle und praxisbezogene Inhalte vermittelt zu bekommen. Die kontinuierliche Weiterentwicklung unserer Bildungsangebote stellt sicher, dass die aktuellen fachlichen Anforderungen, insbesondere aus nationalen und internationalen Standards, sowie die individuellen Bedürfnisse der Teilnehmer, insbesondere nach Praxisnähe und einem intensiven Interessens- und Wissensaustausch, einbezogen werden können.

In unserem öffentlich zugänglichen Zertifikatsregister können Sie zudem Ihre erworbenen Kompetenzen den relevanten Stakeholdern gegenüber darstellen.

### Berlin, Kurfürstendamm...

Unser Ziel ist Ihr Lernerfolg - so schaffen wir an unserem Standort in Berlin ein lernunterstützendes und harmonisches Gesamtklima, um Ihren Aufenthalt zu einem nachhaltigen Erlebnis werden zu lassen - ob durch einen kostenlosen Kinobesuch im legendären Zoo Palast, durch unsere hochwertige und reichhaltige Verkostung oder durch die Inspiration, die Sie durch unsere liebevoll gestalteten Räumlichkeiten erfahren.

### ...Live Online...

Wenn Sie uns, aus gleich welchen Gründen, nicht vor Ort in unseren Räumlichkeiten besuchen können, bieten wir nahezu alle Veranstaltungen zeitgleich Live Online an. Je nach Gruppengröße erfolgt die Durchführung der Veranstaltung sodann als Online- oder Hybridveranstaltung.

### ...oder individuell wo und wie es Ihnen behagt

Wenn Sie Interesse an etwas Speziellem oder einer Inhouse-Veranstaltung haben, setzen wir gerne gemeinsam festgelegte Weiterbildungsziele für die Kompetenzentwicklung Ihrer Mitarbeiter um.

Wir freuen uns auf Sie und senden die besten Grüße aus der Hauptstadt.

Ihr



Ronny Neid  
- Vorstand -

# INHALT

## AUSBILDUNGEN MIT PERSONENZERTIFIKAT DGI®

IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO)	8
Lead Auditor ISO 27001	9
BSI IT-Grundschutz-Praktiker	10
BSI IT-Grundschutz-Berater	11
BSI Vorfall-Praktiker	12
IT Risk Manager	13
Business Continuity Manager	14
ICS Security Manager	15
Kryptographie Security Expert	16
Datenschutzbeauftragter	17
Datenschutz-Auditor	18
Datenschutzbeauftragter im Gesundheitswesen	19

## SEMINARE DGI®

Die Umsetzung der BAIT angemessen planen und konzipieren	22
IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit	23
Informationssicherheit für Betreiber von Telekommunikationsinfrastrukturen und -anlagen	24
Datenschutzrechtliche Aufgaben und Rechte bei Betriebsratstätigkeit	25
Datenschutz im Personalwesen	26
Datenschutz im Finanz- und Versicherungswesen	27

## WORKSHOPS

Die Durchführung und Dokumentation einer IT-Risikoanalyse	30
Die Durchführung und Dokumentation einer Datenschutz- Folgenabschätzung	31
Die Durchführung und Dokumentation einer Business Impact Analyse	32
Die Durchführung einer Dokumenten- und Vertragsprüfung im Kontext der Informationssicherheit und des Datenschutzes	33

## INFORMATIONEN

Veranstaltungsentwicklung und Qualitätssicherung	38
Dozenten	39
Lernumfeld und Seminarraum	40
Inhouse-Veranstaltung	42
Personenzertifizierung	43
Chronologische Übersicht aller Veranstaltungen 2024	44
Persönliche Notizen	50



**AUSBILDUNGEN MIT  
PERSONENZERTIFIKAT DGI®**

- IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO)
- Lead Auditor ISO 27001
- BSI IT-Grundschutz-Praktiker
- BSI IT-Grundschutz-Berater
- BSI Vorfall-Praktiker
- IT Risk Manager
- Business Continuity Manager
- ICS Security Manager
- Kryptographie Security Expert
- Datenschutzbeauftragter
- Datenschutz-Auditor
- Datenschutzbeauftragter im Gesundheitswesen



# IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO) (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Planung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 und BSI IT-Grundschutz



Die Haupttätigkeit eines IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) besteht darin, die Geschäftsführung bei der Wahrnehmung ihrer Pflichten zur Sicherstellung eines angemessenen Informationssicherheitsniveaus zu unterstützen und den spezifischen Schutzbedarf der Unternehmenswerte bei der Ausführung der Geschäfts- und Produktionsprozesse zu identifizieren.

Weitere Aufgaben, die in die Zuständigkeit eines ITSiBe / CISO fallen, sind die Abstimmung und Koordination der Informationssicherheitsstrategie, die Ableitung der Ziele zur Informationssicherheit, das Erkennen der unternehmensspezifischen Risikolagen und Bedrohungsszenarien sowie die Kontrolle und Steuerung der nachhaltigen Umsetzung von angemessenen und wirksamen Sicherungsmaßnahmen.

Der ITSiBe / CISO muss den IT-gestützten Geschäftsbetrieb in Einklang mit den Vorgaben der Governance, der Compliance und des ordnungsgemäßen IT-Betriebs bringen, die Überprüfung eingetretener Sicherheitsvorfälle und Schadensereignisse initiieren und verbessern sowie insbesondere die Wahrung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität sicherstellen. Des Weiteren ist für den Aufbau eines organisationsspezifischen Informationssicherheitsmanagementsystems (ISMS) die erfolgreiche Integration der Planung, der Kontrolle sowie der Steuerung von Prozessen und ergänzenden Dokumenten sowie die Dokumentation eines Sicherheitskonzepts erforderlich.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von relevanten Begriffen aus dem Bereich der Informationssicherheit, der Aufgabenbeschreibung des ITSiBe / CISO sowie des erforderlichen Fachwissens für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS). In Abgrenzung zu der Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®) wird in dieser Ausbildung vertiefend auf die Ausgestaltung eines organisationsspezifischen ISMS gemäß ISO 27001 und ISO 27002 eingegangen. Unter Zuhilfenahme von zahlreichen Leseproben zu relevanten Sicherheitskonzepten eines ISMS werden die Umfänge und die Formulierungen von geforderten Nachweisen des ISMS umfassend dargelegt.

## INHALTE (Auszug)

- Die Informationssicherheitsstrategie
- Ziele der Informationssicherheit
- IT-Sicherheitsgesetz und KRITIS
- Aufgaben des ITSiBe wie Planung, Kontrolle und Steuerung des ISMS
- Die Sicherheitsorganisation und Rollen im ISMS
- Die Normenreihe ISO 270xx
- Planung, Initiierung, Betrieb, Kontrolle und Aufrechterhaltung eines ISMS
- Die Erstellung eines IT-Sicherheitskonzeptes
- Umsetzung des Informationssicherheitsprozesses
- Best Practice des BSI IT-Grundschutzes

## TERMINE 2024

Berlin

08. - 11. Januar  
12. - 15. Februar  
18. - 21. März  
22. - 25. April  
27. - 30. Mai  
24. - 27. Juni  
15. - 18. Juli  
19. - 22. August  
07. - 10. Oktober  
11. - 14. November  
09. - 12. Dezember

## TERMINE 2024

Online

08. - 11. Januar  
12. - 15. Februar  
18. - 21. März  
22. - 25. April  
27. - 30. Mai  
24. - 27. Juni  
15. - 18. Juli  
19. - 22. August  
07. - 10. Oktober  
11. - 14. November  
09. - 12. Dezember

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

2.050,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.950,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

220,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Lead Auditor ISO 27001 (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Auditierung eines Informationssicherheitsmanagementsystems (ISMS)



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 zur Verfügung stehenden 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.

## INHALTE (Auszug)

- Planung, Zielsetzung und Durchführung eines Audits
- Anforderungen an ein Audit und den Auditor
- Auditprinzipien gemäß ISO 1911
- Rollen und Zuständigkeiten im Auditprozess
- Audit-Methoden zur Überprüfung eines Sicherheitskonzepts
- Audit-Checkliste gemäß ISO 27001 und BSI IT-Grundschutz
- Exemplarische Prüfpunkte eines ISMS-Audits
- Konformitäten und Abweichungen
- Feststellungen eines ISMS-Audits
- Inhalte, Gliederung und Erstellung eines ISMS-Auditberichts

## TERMINE 2024

Berlin

19. - 23. Februar

13. - 17. Mai

22. - 26. Juli

16. - 20. September

18. - 22. November

## TERMINE 2024

Online

19. - 23. Februar

13. - 17. Mai

22. - 26. Juli

16. - 20. September

18. - 22. November

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

2.400,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

2.300,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

300,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZIEL DER AUSBILDUNG

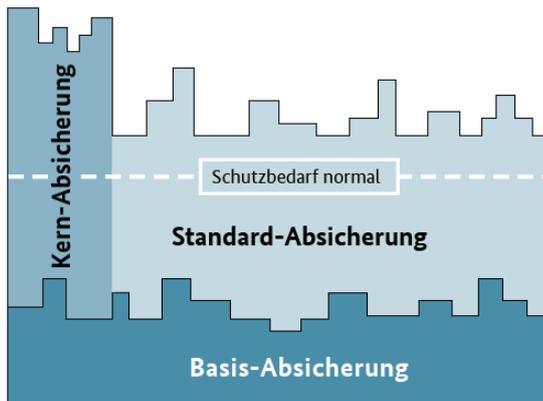
Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich der Durchführung eines Audits gemäß ISO 19011, der Aufgabenbeschreibung des Lead Auditors ISO 27001 und des erforderlichen Fachwissens für die Auditierung eines ISMS. Die Teilnehmer können nach Abschluss der Ausbildung die Durchführung eines ISMS-Audits planen sowie eine Bewertung des bestehenden ISMS vornehmen.

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# BSI IT-Grundschutz-Praktiker (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Planung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß der Vorgehensweise des BSI IT-Grundschutzes



Unsere Ausbildung zum BSI IT-Grundschutz-Praktiker erfüllt das Curriculum sowie die Qualifizierungsanforderungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) und versetzt Sie in die Lage die Aufgaben eines IT-Sicherheitsbeauftragten (ITSiBe) oder Informationssicherheitsbeauftragten (ISB) zu übernehmen.

Sie erlernen die Leitung Ihrer Organisation bei der Wahrnehmung der Pflichten zur Sicherstellung eines angemessenen Informationssicherheitsniveaus zu unterstützen, angemessene Maßnahmen für Ihr Sicherheitskonzept zu bestimmen sowie den spezifischen Schutzbedarf Ihrer Informationen, Anwendungen und IT-Systeme zu identifizieren.

Vertiefende Kenntnisse, die Sie im Rahmen unserer Ausbildung zum BSI IT-Grundschutz-Praktiker erlangen, sind die Umsetzung der Initiierung, Entwicklung, Lenkung und Dokumentation des Sicherheitsprozesses, die Umsetzung der erforderlichen Sicherheitskonzeption sowie der Aufrechterhaltung und Verbesserung der Informationssicherheit.

In Ihrer Funktion als ITSiBe oder ISB steuern Sie die Einhaltung der Ziele zur Informationssicherheit durch die Betrachtung von Gefährdungslagen, die Überprüfung von Sicherheitsvorfällen sowie deren Schadensereignissen und fördern das Erkennen der Risikolagen und Bedrohungsszenarien in der eigenen Organisation.

Des Weiteren erwerben Sie das Know-how für den Aufbau eines organisationsspezifischen ISMS gemäß BSI IT-Grundschutz, die erfolgreiche Integration der Planung, der Kontrolle sowie der Steuerung von Prozessen und ergänzenden Dokumenten sowie die Dokumentation einer Sicherheitskonzeption gemäß BSI-Standard 200-2.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt unserer Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich der Informationssicherheit sowie des erforderlichen Fachwissens für die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines ISMS gemäß BSI IT-Grundschutz bis hin zur erforderlichen Zertifizierungsreife.

## INHALTE (Auszug)

- Initiierung und Organisation des Sicherheitsprozesses
- Informationssicherheitsstrategie und Informationssicherheitsleitlinie
- Die Sicherheitsorganisation und Verantwortlichkeiten im ISMS
- Das BSI IT-Grundschutz-Kompendium
- Die BSI-Standards 200-1, 200-2, 200-3 und 100-4 (200-4)
- Dokumentation im Sicherheitsprozess
- Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis-, Standard-, Kernabsicherung
- Umsetzung der Sicherheitskonzeption
- Grundlagen des IT-Risikomanagements
- Zertifizierung auf der Basis von IT-Grundschutz

## TERMINE 2024

Berlin

15. - 18. Januar  
11. - 14. März  
15. - 18. April  
03. - 06. Juni  
01. - 04. Juli  
12. - 15. August  
16. - 19. September  
28. - 31. Oktober  
02. - 05. Dezember

## TERMINE 2024

Online

15. - 18. Januar  
11. - 14. März  
15. - 18. April  
03. - 06. Juni  
01. - 04. Juli  
12. - 15. August  
16. - 19. September  
28. - 31. Oktober  
02. - 05. Dezember

Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.

## VERANSTALTUNGSPREIS

2.250,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

2.150,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

250,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# BSI IT-Grundschutz-Berater (DGI®)

Erwerben Sie die spezifischen Kenntnisse zur Unterstützung bei der Planung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß des BSI IT-Grundschutzes bis zur Zertifizierungsreife



Unsere Ausbildung zum BSI IT-Grundschutz-Berater erfüllt das Curriculum sowie die Qualifizierungsanforderungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) und versetzt Sie in die Lage die Initiierung, die Planung, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) gemäß den Anforderungen des BSI bis zur Zertifizierungsreife hin zu unterstützen.

Sie erlernen durch einen hohen praktischen Anteil der Wissensvermittlung insbesondere die Entwicklung, Erstellung und Lenkung der erforderlichen Dokumentationen und Prozesse, die Behörden und Unternehmen für den Nachweis einer Zertifizierung gemäß ISO 27001 auf Basis des BSI IT-Grundschutzes benötigen sowie ein Audit auf Basis von BSI IT-Grundschutz vorzubereiten.

Vertiefende Kenntnisse, die Sie im Rahmen unserer Ausbildung zum BSI IT-Grundschutz-Berater erlangen, sind die Entwicklung und Umsetzung einer angemessenen Informationssicherheitsstrategie für Ihre Organisation, die Vorbereitung und Durchführung eines Audits sowie die Umsetzung angemessener Maßnahmen des Business Continuity Managements.

## INHALTE (Auszug)

- Normen und Standards der Informationssicherheit
- BSI IT-Grundschutz-Vorgehensweise
- Leitfragen zur BSI IT-Grundschutz-Absicherung
- BSI IT-Grundschutz-Kompendium
- BSI IT-Grundschutz-Check
- Risikoanalyse
- Aufrechterhaltung und kontinuierliche Verbesserung
- BSI IT-Grundschutz-Profile
- Vorbereitung auf ein Audit
- Notfallmanagement

## TERMINE 2024

Berlin

05. - 07. Februar

06. - 08. Mai

09. - 11. September

16. - 18. Dezember

## TERMINE 2024

Online

05. - 07. Februar

06. - 08. Mai

09. - 11. September

16. - 18. Dezember

Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.

## VERANSTALTUNGSPREIS

1.850,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.750,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKAT

Das Zertifikat kann nur über das BSI erworben werden.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt unserer Ausbildung liegt auf der Vermittlung erforderlichen Know-hows, um Organisationen bei der praktischen Umsetzung eines ISMS gemäß ISO 27001 auf Basis des BSI IT-Grundschutzes beraten zu können. Als Teilnehmer unserer durch das BSI anerkannten Ausbildung erwerben Sie die Berechtigung die Prüfung zur Erlangung des Personenzertifikats IT-Grundschutz-Berater beim BSI abzulegen. Weitere Informationen finden Sie auf der Webseite des BSI.

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# BSI Vorfall-Praktiker (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Planung und Etablierung eines systematischen Vorfallmanagements für IT- und Informationssicherheitsvorfälle gemäß der Vorgehensweise des BSI



Die Schulung zum BSI Vorfall-Praktiker erfüllt das Curriculum sowie die Qualifizierungsanforderungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) und versetzt Sie in die Lage die Aufgaben eines Vorfallmanagers der Informationssicherheit und der IT-Sicherheit zu übernehmen.

Sie erlernen die Leitung Ihrer Organisation bei der Wahrnehmung der Pflichten zur Sicherstellung eines angemessenen Informationssicherheitsniveaus zu unterstützen, angemessene Maßnahmen für Ihr Vorfallmanagement zu bestimmen sowie den spezifischen Ablauf des Vorfallmanagements in Ihrer Organisation zu planen.

Vertiefende Kenntnisse, die Sie im Rahmen unserer Ausbildung zum BSI Vorfall-Praktiker erlangen, sind die Relevanz und die Funktionsweise des Cyber-Sicherheitsnetzwerks, die Sofortmaßnahmen bei einem Vorfall, die Einordnung und Systematisierung von Gefährdungen und Angriffsformen, den Ablauf des Vorfallmanagements, die Behandlung von IT-Sicherheitsvorfällen, die Remote-Unterstützung, die Vorfallbearbeitung bei IT-Systemen "abseits der üblichen Büroumgebung" und die präventiven Maßnahmen zur Vermeidung künftiger Vorfälle.

Des Weiteren erwerben Sie das Know-how für den Aufbau eines organisationsspezifischen Vorfallmanagements gemäß den Empfehlungen des BSI sowie für die erfolgreiche Integration der Planung, der Kontrolle sowie der Steuerung von Prozessen und ergänzenden Dokumentationen des Vorfallmanagements.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung zum BSI Vorfall-Praktiker liegt auf der Vermittlung von Methoden und Vorgehensweisen in dem Bereich des Vorfallmanagements der Informationssicherheit und der IT-Sicherheit sowie des erforderlichen Fachwissens für die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines Vorfallmanagements gemäß den Empfehlungen des BSI.

## INHALTE (Auszug)

- Das Cyber-Sicherheitsnetzwerk
- Die Meldung eines Vorfalls
- Die Gefährdungen und Angriffsformen
- Das Standard-Vorgehen
- Die Behandlung von IT-Sicherheitsvorfällen
- Die Remote-Unterstützung
- Die Vorfallbearbeitung bei IT-Systemen „abseits der üblichen Büroumgebung“
- Die präventiven Maßnahmen zur Vermeidung künftiger Vorfälle

## TERMINE 2024

Berlin

22. - 24. Januar

22. - 24. Mai

02. - 04. September

16. - 18. Dezember

## TERMINE 2024

Online

22. - 24. Januar

22. - 24. Mai

02. - 04. September

16. - 18. Dezember

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.350,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.250,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

600,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# IT Risk Manager (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Planung und Etablierung eines IT-Risikomanagementsystems gemäß ISO 31000, ISO 27005 und BSI IT-Grundschutz



Die Haupttätigkeit eines IT Risk Managers besteht darin, die IT-Risiken eines Unternehmens anhand der spezifischen Bedrohungslage zu identifizieren, realistische Risikoszenarien zu entwickeln und die Abschätzung der Schadensauswirkungen auf den Geschäftsbetrieb vorzunehmen.

Weitere Aufgaben, die in die Zuständigkeit eines IT Risk Managers fallen, sind insbesondere die Abstimmung und Koordination der IT-Risikostrategie, die Festlegung von Kriterien der Risikobewertung und der Risikoakzeptanz sowie die Planung angemessener Maßnahmen der Risikobehandlung zur Unterstützung der Unternehmensziele.

Der IT Risk Manager muss, um die Einhaltung der gesetzlich vorgeschriebenen Risikofrüherkennung zu gewährleisten, ein aktives risikoorientiertes Vorgehen in allen Geschäftsabläufen etablieren sowie die Planung und Umsetzung der Sicherungsmaßnahmen in den Bereichen Informationssicherheit und Business Continuity kontrollieren und steuern.

Des Weiteren ist für den Aufbau eines organisationspezifischen Risikomanagementsystems (RMS) die erfolgreiche Integration der Planung, der Kontrolle und der Steuerung von Prozessen und ergänzenden Dokumenten für den IT-gestützten Geschäftsbetrieb sowie die Dokumentation eines IT-Risikomanagementhandbuchs erforderlich.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich des IT-Risikomanagements, der Aufgabenbeschreibung eines IT Risk Managers und des erforderlichen Fachwissens für die Etablierung eines RMS gemäß ISO 31000, ISO 27005 sowie des BSI IT-Grundschutz. Die Teilnehmer können nach Abschluss der Ausbildung die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines RMS zur Umsetzung bringen.

## INHALTE (Auszug)

- Die IT-Risikostrategie
- Die Aufgaben des „IT Risk Managers“ im RMS
- Die IT-Risikomanagementorganisation und Verantwortlichkeiten im RMS
- Die ISO 31000
- Die ISO 27005
- Der BSI-Standard „200-3 Risikoanalyse“
- Der IT-Risikomanagementprozess
- Die Risikointegration in den Geschäftsbetrieb
- Die risikoorientierte Steuerung von Geschäftsabläufen
- Abhängigkeiten und Wechselwirkungen des IT-gestützten Geschäftsbetriebs erkennen

## TERMINE 2024

Berlin

05. - 07. Februar

08. - 10. April

10. - 12. Juni

12. - 14. August

14. - 16. Oktober

09. - 12. Dezember

## TERMINE 2024

Online

05. - 07. Februar

08. - 10. April

10. - 12. Juni

12. - 14. August

14. - 16. Oktober

09. - 12. Dezember

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.850,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.750,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

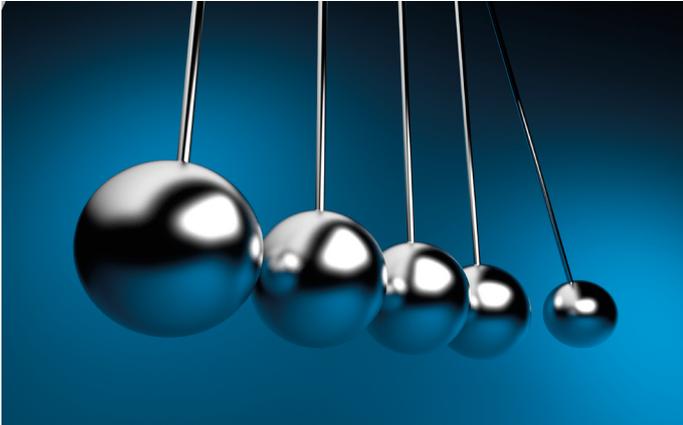
240,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Business Continuity Manager (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Planung und Etablierung eines Business Continuity Managementsystems gemäß ISO 22301, ISO 27031 und des BSI IT-Grundschutzes



Die Haupttätigkeit eines Business Continuity Managers besteht darin, die Widerstandsfähigkeit der Organisation zu stärken, um bei zeitkritischen Sicherheitsvorfällen die vereinbarungsgemäße Wiederherstellung der Geschäftstätigkeit sicherstellen und negative Auswirkungen für ihr Unternehmen abwenden zu können.

Weitere Aufgaben, die in die Zuständigkeit eines Business Continuity Managers fallen, sind die Abstimmung und Koordination der Business Continuity Strategie, insbesondere die Festlegung von Wiederanlauf- und Wiederherstellungsparametern, von Kontinuitätsstrategien sowie die Durchführung von Business Impact Analysen (BIA).

Der Business Continuity Manager sollte Maßnahmen zur Notfallvorsorge umsetzen, um den Eintritt von möglichen Schadensereignissen abzuwenden sowie Maßnahmen zur Umsetzung bringen, die für den Fall eines Schadenseintritts eine angemessene Notfallbewältigung ermöglichen.

Des Weiteren ist eine erfolgreiche Planung, Kontrolle und Steuerung von Notfallprozessen sowie die Dokumentation eines IT-Notfallkonzepts und eines IT-Notfallhandbuchs, inklusive Sofort-, Wiederanlauf-, Wiederherstellungs- und Geschäftsfortführungsplänen, essenziell für die Etablierung eines organisationspezifischen Business Continuity Management Systems (BCMS).

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich des Business Continuity Managements (BCM), der Aufgabenbeschreibung des Business Continuity Managers und des erforderlichen Fachwissens für die Etablierung eines BCMS gemäß ISO 22301, ISO 27031 sowie des BSI IT-Grundschutzes. Die Teilnehmer können nach Abschluss der Ausbildung die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines normkonformen BCMS, bis hin zur Zertifizierungsreife Ihres Unternehmens, zur Umsetzung bringen.

## INHALTE (Auszug)

- Die Strategie zum BCM
- Das IT-Sicherheitsgesetz und KRITIS
- Aufgaben des Business Continuity Managers wie Planung, Kontrolle und Steuerung des BCMS
- Die IT-Notfallorganisation und Verantwortlichkeiten im BCM
- Die Normenfamilie ISO 223xx
- Die ISO 27031 - IT Readiness for Business Continuity (IRBC)
- Der BSI-Standard „200-4 Business Continuity Management“
- Das IT-Notfallvorsorgekonzept
- Das IT-Notfallkonzept
- Das IT-Notfallhandbuch

## TERMINE 2024

Berlin

29. - 31. Januar  
25. - 27. März  
27. - 29. Mai  
29. - 31. Juli  
23. - 25. September  
25. - 27. November

## TERMINE 2024

Online

29. - 31. Januar  
25. - 27. März  
27. - 29. Mai  
29. - 31. Juli  
23. - 25. September  
25. - 27. November

Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.

## VERANSTALTUNGSPREIS

1.750,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.650,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

220,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# ICS Security Manager (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Planung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) für industrielle Automatisierungssysteme (IACS) gemäß IEC 62443, ISO 27001 und BSI IT-Grundschutz



Die Haupttätigkeit des "ICS (Industrial Control System) Security Manager" besteht darin, die Leitung der Organisation in der Wahrnehmung ihrer Pflichten zur Sicherstellung eines angemessenen Informationssicherheitsniveaus, bei dem Betrieb von IACS, zu unterstützen, sowie die angemessenen Security Level und Protection Level zu bestimmen.

Die stark zunehmende Vernetzung von Prozesssteuerungssystemen mit IT Netzen führt zu zusätzlichen, spezifischen Risiko- und Bedrohungsszenarien, insbesondere für die Betreiber von IACS. Bei der Entwicklung, der Integration sowie dem Betrieb von IACS müssen insbesondere geltende Normen und Rechtsvorschriften beachtet werden, um eine risikoadäquate Entwicklung der organisationsspezifischen Sicherheitsstrategie sowie die Umsetzung eines angemessenen ganzheitlichen Sicherheitskonzeptes sicherzustellen.

Bedrohungen wie Sabotage, Spionage oder gezielte Angriffe auf Daten und Systeme sowie geistiges Eigentum und Know-how fordern ein proaktives Sicherheitsdenken der verantwortlichen Personen sowie einen bewussten Umgang mit dem Thema Betriebs- und Informationssicherheit. Die zu berücksichtigenden Sicherheitsfunktionen, beim Design der Hard- und Softwarekomponenten von ICS und IACS, auf Betriebsplattformen und in den hochgradig vernetzten Infrastrukturen, erfordern oftmals ein komplexes internes Prozessmanagement, sichere Systemarchitekturen sowie anlagen-spezifische Schutzmaßnahmen.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen und Methoden zur Planung und Umsetzung der Informationssicherheit in IT-gestützten Steuerungs- und Automatisierungsanlagen. Die Teilnehmer können nach Abschluss der Ausbildung das Zusammenwirken von IT Sicherheit und Anlagensicherheit, für einen sicheren Betrieb von ICS-Umgebungen, erkennen und bewerten. Unter Einbeziehung der Anforderungen an ein ISMS sowie durch die Einbindung des Business Continuity Managements können die Teilnehmer die angemessenen Maßnahmen zur Etablierung des geforderten Sicherheitsniveaus planen und zur Umsetzung bringen.

## INHALTE (Auszug)

- Die IEC 62443-Normenreihe für industrielle Kommunikationsnetze
- Anforderungen an Hersteller, Betreiber und Integratoren
- Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
- Anforderungen an die Fähigkeiten des Integrators
- Anforderungen an Sicherheitsmaßnahmen bei der Erbringung von Dienstleistungen an IACS
- Das IT-Sicherheitsgesetz und KRITIS
- Informationssicherheit und IT-Sicherheitskonzepte für ICS-Umgebungen
- Der IT-Grundschutz des BSI
- Aufbau eines ISMS und BCMS
- Risikomanagement beim Betrieb von ICS-Systemen

## TERMINE 2024

Berlin  
22. - 24. Januar  
17. - 19. Juni  
21. - 23. Oktober

## TERMINE 2024

Online  
22. - 24. Januar  
17. - 19. Juni  
21. - 23. Oktober

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.850,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber  
1.750,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

240,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Kryptographie Security Expert (DGI®)

Erwerben Sie die Kenntnisse und Fähigkeiten zur Anwendung kryptographischer Verfahren und Verschlüsselungstechniken im Kontext der IT-Sicherheit



Sicherheitsmaßnahmen können nur dann wirksam sein, wenn deren Bestimmung und Umsetzung eine ganzheitliche Betrachtung, einschließlich der Betrachtung der Perspektive potenzieller Angreifer, zugrunde liegt.

Eine Vielzahl von Sicherheitsmaßnahmen berücksichtigt die Anwendung kryptographischer Verfahren, wie die Nutzung digitaler Zertifikate und Signaturen, den Aufbau von Public-Key-Infrastrukturen (PKI), den verschlüsselten Datenaustausch in Netzwerken via Ethernet- oder IP-Verschlüsselung oder auf der Anwendungsschicht via S/MIME. Die sinnhafte Einführung und Nutzung solcher Verfahren und Komponenten setzt ein strukturiertes Vorgehen in der Bedrohungsanalyse, unter Berücksichtigung aktueller Angriffsmethoden und Vorgehensweisen potenzieller Angreifer, voraus. Des Weiteren muss die ordnungsgemäße Anwendung kryptografischer Verfahren umgesetzt und fehlerhafte Implementierungen und Konfigurationen von Sicherheitskomponenten verhindert werden. Ein angemessenes Sicherheitsniveau der Nutzung kryptographischer Verfahren wird erreicht, wenn das Zusammenwirken aller Faktoren bei der Einführung und Verwendung bewusst gesteuert wird.

Die Auseinandersetzung mit der Nutzung und Anwendung kryptographischer Verfahren unterstützt zusätzlich den Wissensaufbau im Bereich der Informationssicherheit, insbesondere des Datenschutzes sowie der IT-Sicherheit.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung ist die Vermittlung der für die praktische Anwendung kryptographischer Verfahren erforderlichen Fachkenntnisse, der aktuellen Verschlüsselungstechniken, der Anwendung von Sicherheitszertifikaten und digitalen Signaturen sowie des Aufbaus von Public-Key-Infrastrukturen (PKI). Die Teilnehmer erwerben Kenntnisse über aktuelle Bedrohungs- und Risikolagen bei der Nutzung kryptographischer Verfahren, wie S/MIME, SSL oder X.509-Zertifikaten und die Umsetzung von Maßnahmen zur Sicherstellung der Schutzziele einer Organisation.

## INHALTE (Auszug)

- Grundlegende Operationen in der Kryptographie
- Kryptographische Hashverfahren
- Symmetrische Verschlüsselungsalgorithmen
- Asymmetrische Verfahren
- Schlüsselaustauschverfahren
- Zufallszahlen
- PKI-Infrastrukturen
- Ermittlung und Definition von IT-Sicherheitsanforderungen
- Netzwerksicherheit - Diskussion aktueller Verfahren auf OSI Layer-2 und Layer-3
- Praktische Übungen

## TERMINE 2024

Berlin

15. - 17. April

09. - 11. September

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.850,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.750,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

240,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Datenschutzbeauftragter (DGI®)

Erwerben Sie das spezifische Fachwissen für die Benennung als Datenschutzbeauftragter, wie von der DSGVO sowie dem BDSG gefordert



Die Haupttätigkeit eines Datenschutzbeauftragten (DSB) besteht darin, die Einhaltung von datenschutzrechtlichen Anforderungen, insbesondere reguliert durch die EU-Datenschutz-Grundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG), bei dem für die Verarbeitung Verantwortlichen zu überwachen.

Zu diesem Zweck muss der DSB ein wirkungsvolles Datenschutzmanagement entwickeln, implementieren und betreiben. Im Rahmen des Datenschutzmanagements muss der DSB umfassende Prüf- und Überwachungsmechanismen etablieren und kontinuierlich weiterentwickeln, um etwa die Angemessenheit der technischen und organisatorischen Maßnahmen zur Wahrung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit bei der Verarbeitung von personenbezogenen Daten (pb Daten) zu bewerten und um die Führungskräfte des Verantwortlichen fundiert beraten zu können.

Die erforderliche Kompetenz eines DSB sollte datenschutzrechtliches Wissen sowie ein grundlegendes technisches Know-how umfassen. Darüber hinaus sollte ein DSB seine Aufgaben effizient und strukturiert erledigen, um die Ressourcen des eigenen Unternehmens und der eigenen Datenschutzorganisation zu schonen und die Akzeptanz des Datenschutzmanagements auf einem hohen Niveau zu etablieren.

Der Aufbau unserer Ausbildung bietet angehenden DSB eine sehr praxisnahe Orientierung, um ein strukturiertes und wirkungsvolles Datenschutzmanagement aufzubauen und zu managen. Durch den Erfahrungsaustausch mit sämtlichen Teilnehmern werden zudem datenschutzspezifische Konzepte und Vorgehensweisen besprochen sowie Aspekte der praktischen Umsetzung Ihres Datenschutzmanagements durch unsere Dozenten aufgezeigt.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich des Datenschutzes sowie der Informationssicherheit, der Aufgabenbeschreibung des Datenschutzbeauftragten und des erforderlichen Fachwissens zur Erfüllung der gestellten Anforderungen aus der DSGVO sowie dem BDSG. Die Teilnehmer können nach Abschluss der Ausbildung die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines Datenschutzmanagementsystems zur Umsetzung bringen.

## INHALTE (Auszug)

- Die Anforderungen aus der DSGVO sowie dem BDSG
- Der Aufbau und die Umsetzung eines Datenschutzmanagementsystems
- Die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten
- Die Benennung, Stellung und Aufgaben des Datenschutzbeauftragten
- Der Aufbau der Datenschutzorganisation
- Die Rechte der betroffenen Person
- Die Datenverarbeitung im Auftrag - Rechte, Pflichten und Konsequenzen
- Die Durchführung einer Datenschutz-Folgenabschätzung (DSFA)
- Die Umsetzung der Sicherheit der Verarbeitung
- Das Verzeichnis von Verarbeitungstätigkeiten
- Die Informations-, Melde- und Rechenschaftspflichten

## TERMINE 2024

Berlin

15. - 17. Januar  
18. - 20. März  
03. - 05. Juni  
05. - 07. August  
21. - 23. Oktober  
02. - 04. Dezember

## TERMINE 2024

Online

15. - 17. Januar  
18. - 20. März  
03. - 05. Juni  
05. - 07. August  
21. - 23. Oktober  
02. - 04. Dezember

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.600,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.500,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

200,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Datenschutz-Auditor (DGI®)

Erwerben Sie die spezifischen Kenntnisse für die Auditierung eines Datenschutzmanagementsystems (DSMS)



Die Haupttätigkeit eines Datenschutz-Auditors besteht darin, die systematische Beurteilung des bestehenden Datenschutzniveaus eines Unternehmens vorzunehmen sowie insbesondere die Angemessenheit der umgesetzten technischen und organisatorischen Maßnahmen zu bewerten.

Weitere Aufgaben, die in die Zuständigkeit eines Datenschutz-Auditors fallen, sind die Entwicklung und Steuerung des Auditprogramms sowie die Erstellung der erforderlichen Audit-Checklisten für die Durchführung von Stichprobenprüfungen und Interviews.

Der Datenschutz-Auditor muss die Audit-Methoden für die Durchführung einer Dokumentenprüfung und für die Begehung von Standorten anwenden können, um die an ein Unternehmen gestellten standort- und branchenspezifischen Anforderungen des Datenschutzes einzubeziehen und die Konformität der Maßnahmenumsetzung zu bewerten.

Des Weiteren ist die Festlegung von Kriterien für die Bewertung der Feststellungen des Datenschutz-Audits sowie für die Erstellung eines Datenschutz-Auditberichts erforderlich, um eine kontinuierliche Aufrechterhaltung des Betriebes des eigenen Datenschutzmanagementsystems (DSMS) sowie die fortlaufende Verbesserung sicherstellen zu können.

## INHALTE (Auszug)

- Die Planung, Zielsetzung und Durchführung eines Datenschutz-Audits
- Die Anforderungen an interne und externe Audits
- Die Anforderungen an den Datenschutz-Auditor
- Die Entwicklung von Prüfkriterien eines Audits gemäß ISO 19011
- Die Entwicklung eines Audit-Programms
- Die Rollen und Zuständigkeiten im Audit-Prozess
- Die Dokumentation eines Datenschutz-Audits
- Die Audit-Methoden zur Überprüfung eines DSMS
- Exemplarische Prüfpunkte eines Datenschutz-Audits
- Die Feststellungen eines Datenschutz-Audits
- Die Feststellung und Bewertung von Konformitäten und Abweichungen eines DSMS
- Die Gliederung und die Erstellung eines Datenschutz-Audit-Berichts

## TERMINE 2024

Berlin

26. - 28. Februar

06. - 08. Mai

26. - 28. August

04. - 06. November

## TERMINE 2024

Online

26. - 28. Februar

06. - 08. Mai

26. - 28. August

04. - 06. November

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.850,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.750,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

240,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## 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 Datenschutz-Auditors und des erforderlichen Fachwissens für die Auditierung eines DSMS. Die Teilnehmer können nach Abschluss der Ausbildung die Durchführung eines Datenschutz-Audits planen sowie eine Bewertung des bestehenden DSMS vornehmen.

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Datenschutzbeauftragter im Gesundheitswesen (DGI®)

Erwerben Sie das spezifische Fachwissen für die Benennung als Datenschutzbeauftragter im Gesundheitswesen, wie von der DSGVO und dem SGB gefordert



Die Haupttätigkeit eines Datenschutzbeauftragten im Gesundheits- und Sozialwesen besteht darin, den Umgang mit Patientendaten zu bewerten und zu kontrollieren sowie die Prozesse der Verarbeitung von personenbezogenen Daten rechtskonform zu steuern.

Weitere Aufgaben, die in die Zuständigkeit eines Datenschutzbeauftragten im Gesundheits- und Sozialwesen fallen, sind insbesondere die Eruierung und das Verständnis spezifischer Branchenanforderungen für die eigene Organisation, um angemessene Maßnahmen zur Wahrung der Vertraulichkeit, der Integrität, der Authentizität und der Verfügbarkeit von Patientendaten zur Umsetzung zu bringen.

Beim Umgang mit Patientendaten muss der Datenschutzbeauftragte im Gesundheits- und Sozialwesen neben den Anforderungen aus der EU-Datenschutz-Grundverordnung (DSGVO) sowie insbesondere aus dem Sozialgesetzbuch (SGB) zusätzlich spezifische Gesetze und Vorschriften des Gesundheitswesens, Landesgesetze, die Musterberufsordnung der Ärzte (MBO-Ä) sowie die gesetzlich verankerte Schweigepflicht beachten.

Des Weiteren sind für den Aufbau und die Etablierung eines organisationsspezifischen Datenschutzmanagementsystems die erfolgreiche Integration der Planung, der Kontrolle und der Steuerung von Prozessen und ergänzenden Dokumenten sowie die Dokumentation eines Datenschutzkonzepts erforderlich.

## ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung des datenschutzspezifischen Fachwissens für den Bereich des Gesundheits- und Sozialwesens. Insbesondere die Einhaltung der regulierenden Rechtsvorschriften sowie die Sicherstellung der Vertraulichkeit, der Integrität, der Authentizität und der Verfügbarkeit von personenbezogenen Daten im Patientenverhältnis werden strukturiert vermittelt. Die Teilnehmer können nach Abschluss der Ausbildung die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines Datenschutzmanagementsystems im Bereich des Gesundheits- und Sozialwesens zur Umsetzung bringen.

## INHALTE (Auszug)

- DSGVO, SGB, BDSG, MBO-Ä und Schweigepflicht
- Die datenschutzspezifischen Gesetze und Vorschriften des Gesundheitswesens
- Die Verantwortlichkeiten und Anforderungen beim Umgang mit Gesundheits- und Sozialdaten
- Der Datenschutz in Krankenhäusern, Medizinischen Versorgungszentren, Arztpraxen, Rettungsdiensten, Alters- oder Pflegeheimen
- Die Einwilligung des Patienten
- Die Erhebung und Speicherung für Zwecke der Behandlung
- Die Weitergabe der Patientendaten innerhalb der Einrichtung
- Die Auftragsverarbeitung und Schweigepflichtentbindung
- Die Informationsansprüche der Krankenkassen und des Medizinischen Dienstes
- Die Auskunfts- und Einsichtsrechte der betroffenen Person
- Die Schweigepflicht - befugtes und unbefugtes Offenbaren gemäß § 203 StGB

## TERMINE 2024

Berlin

12. - 13. Februar

13. - 14. Mai

23. - 24. September

25. - 26. November

## TERMINE 2024

Online

12. - 13. Februar

13. - 14. Mai

23. - 24. September

25. - 26. November

Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.

## VERANSTALTUNGSPREIS

1.150,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.050,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZERTIFIKATSPREIS

200,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# SEMINARE DGI®



- 
- Die Umsetzung der BAIT angemessen planen und konzipieren
  - IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit
  - Informationssicherheit für Betreiber von Telekommunikationsinfrastrukturen und -anlagen
  - Datenschutzrechtliche Aufgaben und Rechte bei Betriebsratstätigkeit
  - Datenschutz im Personalwesen
  - Datenschutz im Finanz- und Versicherungswesen

# Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®)

Erwerben Sie die spezifischen Kenntnisse zur Umsetzung der „Bankenaufsichtliche Anforderung an die IT (BAIT)“



Die nachweisliche Umsetzung der BAIT ist für Kreditinstitute und Finanzdienstleistungsinstitute sowie für deren IT-Dienstleister von existenzieller Bedeutung.

Die BAIT konkretisiert die aktuellen Einwirkungen auf einen sicheren IT-Betrieb und sieht signifikante Verschärfungen bei der Sanktionierung von Verstößen seitens der relevanten Unternehmen vor. Überdies muss davon ausgegangen werden, dass künftige Überprüfungen und Audits von aufsichtsrechtlicher Seite sowie von Wirtschaftsprüfern weniger Spielraum hinsichtlich der Reife der Maßnahmen für die Umsetzung der Anforderungen der BAIT zulassen.

Der unternehmensspezifischen Umsetzung von Maßnahmen für einen ordnungsgemäßen, sicheren und konformen Betrieb der IT muss vor diesem Hintergrund eine hohe Bedeutung beigemessen werden.

Eine dedizierte Auseinandersetzung mit der BAIT muss dazu führen, dass erforderliche Projektierungen des IT-Betriebs und explizit die Entwicklung angemessener Maßnahmen der Informationssicherheit zielgerichtet umgesetzt werden. Darüber hinaus sollten alle relevanten Stakeholder für die Erfüllung der Anforderungen aus der BAIT ausreichend informiert und sensibilisiert werden.

Darüber hinaus ist dieses Seminar ebenso für die relevanten Stakeholder für die Umsetzung der VAIT, KAIT und ZAIT geeignet.

## SEMINARZIEL

Der Schwerpunkt des Seminars liegt in der Vermittlung der Anforderungen aus der BAIT. Insbesondere werden die einzelnen Handlungsbereiche der BAIT vertiefend erläutert und die angemessene Umsetzung der resultierenden Maßnahmen aus den Handlungsbereichen aufgezeigt. Die umfangreichen Arbeitsunterlagen zum Seminar enthalten ein Musterkonzept für den Nachweis der Umsetzung der Maßnahmen aus den Handlungsbereichen der BAIT.

## INHALTE (Auszug)

- Die MaRisk
- Informationsrisikomanagement
- Informationssicherheitsmanagement
- Operative Informationssicherheit
- Identitäts- und Rechtemanagement
- IT-Projekte und Anwendungsentwicklung
- IT-Betrieb
- Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
- IT-Notfallmanagement
- Kritische Infrastrukturen

## TERMINE 2024

Berlin  
29. - 30. Januar  
10. - 11. April  
29. - 30. Juli  
13. - 14. November

## TERMINE 2024

Online  
29. - 30. Januar  
10. - 11. April  
29. - 30. Juli  
13. - 14. November

Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.

## VERANSTALTUNGSPREIS

1.350,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.250,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit (DGI®)

Erlernen Sie die Grundlagen der Informationstechnologie (IT) im Kontext der Einhaltung von datenschutzrechtlichen Anforderungen an Ihre Organisation



Die in den letzten Jahren vermehrt Einzug gehaltene Digitalisierung von Geschäftsprozessen und die damit einhergehende IT-gestützte Datenverarbeitung führt zu einer intensiven Auseinandersetzung mit den Maßnahmen zur IT-Sicherheit sowie des Datenschutzes.

So müssen insbesondere der Datenschutzbeauftragte und sämtliche Personen, die für die Einhaltung von Anforderungen an die IT-Sicherheit verantwortlich sind, eine zunehmend hohe Kenntnis der in der eigenen Organisation verwendeten technischen Komponenten und IT-gestützten Anwendungen sowie deren Funktionsweisen und Aufgaben bei der Verarbeitung digitaler Daten besitzen.

Zudem müssen IT-sicherheitsrelevante und datenschutzrechtlich gesondert zu berücksichtigende Bereiche, anhand der Signifikanz der automatisierten Verarbeitung von geschäftsrelevanten und personenbezogenen Daten, bewertet werden können.

Somit ist der Aufbau von persönlichem Wissen und die Vertiefung des Know-hows der verantwortlichen Personen, für die Sicherstellung eines ordnungsgemäßen, sicheren und konformen Betriebs der IT, eine Schlüsselqualifikation, um die Bewertung des organisationsspezifischen Sicherheitsniveaus vornehmen zu können und angemessene Maßnahmen der Informationssicherheit umzusetzen.

## SEMINARZIEL

Der Schwerpunkt des Seminars liegt in der Vermittlung von Basiswissen aus dem Bereich der Informationstechnologie. Insbesondere werden Grundlagen geschaffen, um die Zusammenhänge zwischen technischen Komponenten und deren Auswirkungen auf datenschutzrechtliche Anforderungen und die IT-Sicherheit verstehen und beurteilen zu können.

## INHALTE (Auszug)

- Netzwerkkomponenten (Server, Clients, Hardware, mobile Geräte)
- Netzwerke (Netzerdienste, Topologien, Protokolle)
- Anwendungen (Software, Maildienste)
- Infrastruktur (Gebäude- und Raumstruktur)
- Schutzkonzepte (Passwortkonventionen, Passwortkonzept, Berechtigungskonzept, Backupkonzept, Archivkonzept)
- Angriffe und Schutzmaßnahmen (Hacking, Penetration Testing, Malware, Netzwerkanalyse, Virtual Private Network, Public Key Infrastructure)
- Kryptographie in der praktischen Anwendung
- Neue Entwicklungen (z.B. Cloud Computing, Social Media)

## TERMINE 2024

Berlin  
31. Januar - 01. Februar  
08. - 09. April  
31. Juli - 01. August  
11. - 12. November

## TERMINE 2024

Online  
31. Januar - 01. Februar  
08. - 09. April  
31. Juli - 01. August  
11. - 12. November

*Alle aufgeführten Termine werden gegebenenfalls als Hybrid-Veranstaltung durchgeführt.*

## VERANSTALTUNGSPREIS

1.190,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

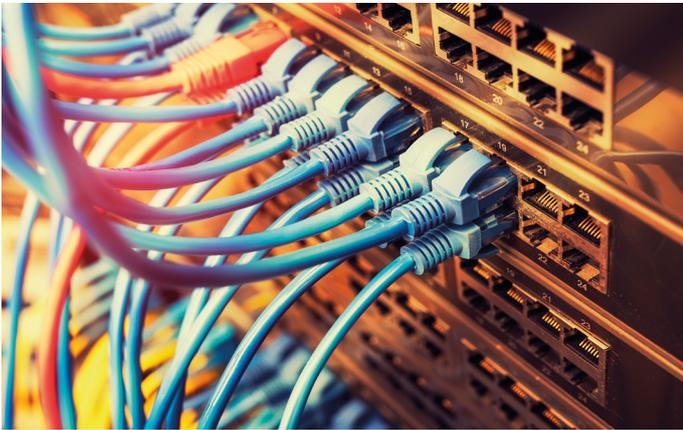
1.090,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Informationssicherheit für Betreiber von Telekommunikationsinfrastrukturen und -anlagen (DGI®)

Erwerben Sie die notwendigen Kenntnisse eines TK-Anbieters / TK-Betreibers zum rechtskonformen Aufbau und Betrieb einer TK-Infrastruktur



Der Betrieb von Telekommunikationsinfrastrukturen sowie von telekommunikationsgestützten Geschäftsprozessen unterliegt engen sektorspezifischen Regulierungen, insbesondere zur Sicherstellung der datenschutzrechtlichen Anforderungen bei der Erhebung und Verarbeitung personenbezogener Daten, wie Standort-, Inhalts- und Verbindungsdaten. Des Weiteren ist die enge Verzahnung der TK mit der Informationstechnik und den daraus resultierenden vielfältigen Anwendungsbereichen eine Herausforderung zur angemessenen Umsetzung der geforderten Maßnahmen zur Informationssicherheit. Die Einwirkungen des Telekommunikation-Telematien-Datenschutzgesetzes (TTDSG) und die Wahrung des Fernmeldegeheimnisses stellen an die Betreiber von Telekommunikationsinfrastrukturen für öffentliche und nicht öffentliche Telekommunikationsdienstleistungen gesonderte Anforderungen. Der explizit im TTDSG festgeschriebene Kundenschutz sowie der Schutz der eigenen Beschäftigten beim Betrieb von TK-Anlagen fordern spezifische Maßnahmen zur Sicherstellung der Rechte der betroffenen Personen.

Die Eruierung der eigenen Bedrohungsszenarien und das Abwenden von Sicherheitsvorfällen beim TK-Betrieb sind im Rahmen des Risikomanagements gesondert zu betrachten und können die Wahrung der organisationsspezifischen Sorgfalts- und Verkehrssicherungspflichten unterstützen, um Haftungsansprüche Dritter oder der eigenen Beschäftigten sowie finanzielle Schäden für die eigene Organisation oder einen Image- oder Reputationsschaden risikoorientiert zu steuern.

## SEMINARZIEL

Der Schwerpunkt des Seminars liegt in der Vermittlung der rechtlichen wie technischen Anforderungen, sowie der notwendigen Kenntnisse zum Aufbau eines angemessenen Sicherheitskonzepts und der Umsetzung notwendiger Sicherheitsmaßnahmen, die einen rechtskonformen TK-Betrieb sicherstellen und persönliche wie organisationseigene Haftungsansprüche abwenden können.

## INHALTE (Auszug)

- KRITIS und TK-Betrieb
- BSI IT-Grundschutz und Maßnahmen für TK-Anlagenbetreiber
- Öffentlicher und nicht-öffentlicher TK-Betrieb
- Die Stellung der BNetzA
- Risikomanagement beim Betrieb von TK
- Sicherheitskonzepte für TK-Betreiber öffentlicher Netze
- Sicherheitskonzepte für TK-Anlagenbetreiber
- Überwachungs- und Kontrollmöglichkeiten beim Betrieb von TK-Anlagen
- Rechtskonformer Umgang mit Standortdaten sowie Inhalts- und Verbindungsdaten

## TERMINE 2024

auf Anfrage

## VERANSTALTUNGSPREIS

1.190,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.090,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Datenschutzrechtliche Aufgaben und Rechte bei Betriebsratstätigkeit (DGI®)

Setzen Sie Aufgaben und Rechte bei der Verarbeitung von personenbezogenen Daten der Arbeitnehmer um



Das Persönlichkeitsrecht der informationellen Selbstbestimmung von Arbeitnehmern ist gemäß Betriebsverfassungsgesetz (BetrVG) zu schützen, was die Einhaltung der datenschutzspezifischen Pflichten durch Ihre Organisation nach sich zieht.

Die Mitbestimmungs- und Mitwirkungsrechte des Betriebs- und Personalrats sind insbesondere bei der Verarbeitung von personenbezogenen Daten der Arbeitnehmer seitens der Organisation zu wahren.

Der Betriebs- und Personalrat hat die Einhaltung der Pflichten aus dem Datenschutzrecht zu kontrollieren und auf deren Einhaltung hinzuwirken.

Die Konstruktivität der Zusammenarbeit des Betriebs- und Personalrats mit dem Datenschutzbeauftragten sowie dem IT-Sicherheitsbeauftragten nimmt bei der Umsetzung angemessener Maßnahmen zur Einhaltung des Datenschutzes eine gewichtige Rolle ein.

Die an Ihre Organisation gestellten datenschutzrechtlichen Anforderungen müssen zudem im Wirkungskreis des Betriebs- und Personalrats selbst eingehalten werden.

Die Umsetzung erforderlicher Maßnahmen zur Wahrung der Rechte der Arbeitnehmer, wie von der EU-Datenschutz-Grundverordnung (DSGVO) sowie dem Bundesdatenschutzgesetz (BDSG) gefordert, setzt eine hohe Kenntnis des Datenschutzrechts der Betriebs- und Personalratsmitglieder voraus.

## SEMINARZIEL

Der Schwerpunkt des Seminars liegt auf der Vermittlung von datenschutzrechtlichem Grundlagenwissen, um Sie als Mitglied des Betriebsrats auf Ihr Mandat vorzubereiten. Ziel des Seminars ist es, den Teilnehmern ein vertiefendes Verständnis für den rechtssicheren Umgang bei der Verarbeitung von Arbeitnehmerdaten und insbesondere der Zusammenarbeit mit dem Datenschutzbeauftragten zu vermitteln.

## INHALTE (Auszug)

- Grundlagen des Datenschutzrechts gemäß DSGVO, BDSG, BetrVG, Allgemeinem Gleichbehandlungsgesetz (AGG) und Sozialgesetzbuch (SGB)
- Mitbestimmungs- und Mitwirkungsrechte bei der Planung, der Einrichtung oder der Änderung von IT-gestützter Verarbeitung von personenbezogenen Daten
- Durchsetzung der Rechte des Betriebsrats im Datenschutzmanagement
- Selbständige Verarbeitung von Arbeitnehmerdaten durch den Betriebsrat
- Auskunfts- und Einsichtsrechte
- Schnittpunkte und Zusammenarbeit mit dem Datenschutzbeauftragten
- Die Wahrung der Rechte der Arbeitnehmer bei der Verarbeitung personenbezogener Daten

## TERMINE 2024

auf Anfrage

## VERANSTALTUNGSPREIS

1.150,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.050,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Datenschutz im Personalwesen (DGI®)

Den rechtskonformen Umgang mit Beschäftigtendaten im Personalwesen umsetzen und aufrechterhalten



Der Personalbereich ist in öffentlichen und nicht-öffentlichen Organisationen einer Vielzahl von Aufgaben und gesetzlichen Anforderungen ausgesetzt.

Der Einhaltung datenschutzrechtlicher Vorgaben zur Sicherstellung des informationellen Selbstbestimmungsrechts Ihrer Beschäftigten wird zunehmend eine stärkere Bedeutung beigemessen. So kann der Umgang mit Ihren Beschäftigtendaten relevante Auswirkungen auf Ihr Image und Ihre Reputation begründen.

In Abgrenzung zu Seminaren zum Beschäftigtendatenschutz, ist dieses Seminar insbesondere dazu angelegt die Begründung, Durchführung und Beendigung von Beschäftigungsverhältnissen aus Sicht der Personalverwaltung und deren rechtskonformen Umgang mit personenbezogenen Daten zu erläutern.

## SEMINARZIEL

Das Seminar bietet allen Beschäftigten im Personalbereich einen grundlegenden Überblick über die geltenden datenschutzrechtlichen Grundlagen hinsichtlich des Umgangs mit personenbezogenen Daten, die im Zusammenhang mit dem Beschäftigungsverhältnis erhoben, verarbeitet und genutzt werden. Personalverantwortliche Personen erhalten Informationen, wie die personenbezogenen Daten von der Bewerbungsphase bis hin zur Pensionszahlung rechtskonform erhoben, verarbeitet und genutzt werden können. Konkrete Praxisempfehlungen zur Prozesssteuerung und Dokumentensteuerung bieten einen pragmatischen Lösungsansatz zur Umsetzung in Ihrer Organisation.

## INHALTE (Auszug)

- Beschäftigtendatenschutz
- Rechtmäßiger Umgang mit Beschäftigtendaten
- Allgemeines Gleichbehandlungsgesetz (AGG)
- Rechtmäßige konzerninterne Weitergabe
- Rechtmäßiger Umgang mit Bilddaten der Beschäftigten
- Zulässigkeit der Erhebung und Verarbeitung
- Übermittlung und Weitergabe von Beschäftigtendaten an Dritte
- Elektronische Personalakte / Papierakte
- Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses
- Einwilligung im Beschäftigtenverhältnis

## TERMINE 2024

auf Anfrage

## VERANSTALTUNGSPREIS

1.150,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.050,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Datenschutz im Finanz- und Versicherungswesen (DGI®)

Erwerben Sie die erforderliche Fachkunde für die Verarbeitung personenbezogener Daten im Finanz- und Versicherungswesen



Die Einhaltung datenschutzrechtlicher Vorgaben gewinnt durch die zunehmende Verarbeitung von Informationen durch IT-gestützte Systeme und Prozesse für das gesamte Finanz- und Versicherungswesen stetig an Bedeutung.

Im Rahmen der finanz- und versicherungsspezifischen Aufgabenstellungen verarbeiten Beschäftigte von Finanz- und Versicherungsgesellschaften, -maklern, -vermittlern und Assekuradeuren personenbezogene Daten, unter anderem von Interessenten, Kunden, Beschäftigten, Lieferanten sowie Produkt- und Kooperationspartnern.

Dies erfordert zwingend die Umsetzung von technischen und organisatorischen Maßnahmen, um einen angemessenen Schutz der Persönlichkeitsrechte zu gewährleisten.

Insbesondere der Einhaltung des gesetzlich geforderten Datenschutzniveaus kommt bei sämtlichen Organisationen des Finanz- und Versicherungswesens eine übergeordnete Bedeutung zu, wie sie insbesondere aus der DSGVO, dem BDSG, dem Kreditwesengesetz, dem Geldwäschegesetz, dem Versicherungsaufsichtsgesetz oder dem Versicherungsvertragsgesetz gefordert wird.

## SEMINARZIEL

In diesem Seminar erlernen Sie die Grundlagen für den rechtskonformen Umgang mit personenbezogenen Daten im Finanz- und Versicherungswesen. Nach Abschluss dieses Seminars können Sie die gesetzlich geforderten Maßnahmen zur Sicherstellung der informationellen Selbstbestimmung bestimmen und die Umsetzung eines angemessenen Datenschutzmanagementsystems initiieren, planen und steuern sowie das Zusammenwirken von Risiken und Gefährdungen bei der Erhebung und Verarbeitung personenbezogener Daten bewerten.

## INHALTE (Auszug)

- Verantwortlichkeiten für die Einhaltung des Datenschutzes
- Übermittlung von Gesundheitsdaten an Versicherer
- Die Einwilligungserfordernisse für die Erhebung und Verarbeitung von Kunden- und Interessentendaten - Betroffene
- Die Verarbeitung und Nutzung für Zwecke der Vertragsbearbeitung
- Weitergabe und Übermittlung von Kunden- und Interessentendaten
- Auskunfts- und Einsichtsrechte der Betroffenen
- Übermittlung an Inkasso
- Berufsgruppenspezifische Anforderungen an Vertrieb und Verwaltung
- Besonderheiten der Datenverarbeitung wie GDV-Datensätze
- Aufbewahrungsfristen und Löschpflichten (rechtskonforme Archivierung)

## TERMINE 2024

auf Anfrage

## VERANSTALTUNGSPREIS

1.150,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

1.050,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Weitere Informationen zur Veranstaltung  
finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



A photograph of a modern meeting room. In the foreground, a round, light-colored table with a wooden edge is set with two white papers, each with a black pen. There are also two clear glasses and a tray with several water bottles. Two black chairs with chrome frames are positioned around the table. The wall behind the table is covered in a perforated acoustic panel. A framed picture of an orange object hangs on the wall. The floor is covered in a grey carpet. The overall atmosphere is professional and clean.

# WORKSHOPS DGI®

- Workshop für die Durchführung und Dokumentation einer IT-Risikoanalyse
- Workshop für die Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung
- Workshop für die Durchführung und Dokumentation einer Business Impact Analyse
- Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung im Kontext der Informationssicherheit und des Datenschutzes



# Workshop für die Durchführung und Dokumentation einer IT-Risikoanalyse (DGI®)

Erlernen und optimieren Sie das praktische Vorgehen für die Durchführung einer IT-Risikoanalyse



Die Pflicht für die Durchführung von Informationssicherheitsrisikoanalysen unter Einbeziehung des relevanten IT-Risikoumfeldes (IT-Risikoanalysen) resultiert insbesondere aus den Anforderungen zahlreicher Normen und Standards, die für die Gewährleistung des sicheren und konformen IT-Betriebs sowie für die ordnungsgemäße Durchführung von IT-gestützten Geschäftsprozessen zu beachten sind.

Die in den Normen und Standards festgelegten Modelle, Methoden und Vorgehensweisen für die Durchführung einer IT-Risikoanalyse zeugen zumeist von sehr theoretischer Natur und liefern nur unzureichende Ansätze für ein praktikables, effizientes und effektives IT-Risikomanagement.

Im Rahmen dieses Workshops erlernen Sie die Handhabung eines modellhaften Ablaufs, um eine IT-Risikoanalyse, insbesondere unter Berücksichtigung der Ihnen zur Verfügung stehenden zeitlichen Ressourcen sowie einer angemessen transparenten Nachvollziehbarkeit für Dritte, durchführen zu können.

Wir vermitteln Ihnen, unter Einbeziehung eines Tools, zu berücksichtigende Zusammenhänge und wechselseitige Abhängigkeiten von einwirkenden Risikofaktoren, wie etwa den Bedrohungen, Schwachstellen und wahrscheinlichen Auswirkungen.

Anhand von zwei konkreten Anwendungsbeispielen lernen Sie das Vorgehen kennen, um die Bewertung einzelner Risikolagen vornehmen und nachweislich begründen zu können.

Darüber hinaus werden die Optionen für die Aufrechterhaltung und die fortlaufende Verbesserung der Durchführung einer IT-Risikoanalyse sowie für die Dokumentation und Kommunikation dargestellt.

Die aktive Moderation von Diskussionen und der Erfahrungsaustausch der Teilnehmer untereinander runden diesen Workshop ab.

## INHALTE (Auszug)

- Die ISO 31000 - Das Risikomanagement
- Die ISO 27005 - Das Informationssicherheitsrisikomanagement
- Der BSI Standard 200-3
- Die IT-Risikoanalyse auf der Basis von BSI IT-Grundschutz
- Der Begriff „Risiko“
- Die relevanten Bedrohungen
- Die relevanten Schwachstellen
- Die wahrscheinlichen Auswirkungen
- Der Risikoeigner
- Der Risikomanager
- Die Informationsgeber
- Die Risikodokumentation
- Die Risikokommunikation
- Durchführung einer beispielhaften IT-Risikoanalyse für die „Einführung einer cloudbasierten Softwareanwendung“
- Durchführung einer beispielhaften IT-Risikoanalyse für den „Umzug eines Rechenzentrumsstandortes“

## TERMINE 2024

Berlin  
08. Februar  
13. Juni  
15. August  
12. Dezember

## TERMINE 2024

Online  
08. Februar  
13. Juni  
15. August  
12. Dezember

## VERANSTALTUNGSPREIS

650,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

550,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZIEL DES WORKSHOPS

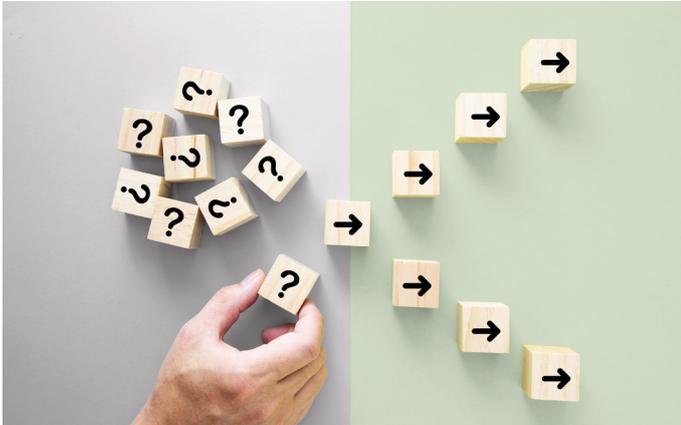
Der Schwerpunkt des Workshops liegt auf der praxisorientierten Vermittlung der Durchführung einer IT-Risikoanalyse unter Betrachtung konkreter Anwendungsbeispiele.

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Workshop für die Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung (DGI®)

Erlernen und optimieren Sie das praktische Vorgehen für die Durchführung einer Datenschutz-Folgenabschätzung



Die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) wird gemäß Artikel 35 DSGVO grundsätzlich gefordert, wenn eine Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Dies könnte auf zahlreiche Verarbeitungen zutreffen und zu einer hohen Anzahl an durchzuführenden DSFA führen.

Die dahingehend verbreiteten Modelle, Methoden und Vorgehensweisen für die Durchführung einer DSFA zeugen zumeist von sehr theoretischer Natur und liefern nur unzureichende Ansätze für ein praktikables, effizientes und effektives Management einer DSFA.

Im Rahmen dieses Workshops erlernen Sie die Handhabung eines modellhaften Ablaufs, um eine DSFA, insbesondere unter Berücksichtigung der Ihnen zur Verfügung stehenden zeitlichen Ressourcen sowie einer angemessen transparenten Nachvollziehbarkeit für Dritte, durchführen zu können.

Wir vermitteln Ihnen, unter Einbeziehung eines Tools, zu berücksichtigende Zusammenhänge und wechselseitige Abhängigkeiten von einwirkenden Risikofaktoren für betroffene Personen, wie etwa den Bedrohungen, Schwachstellen und wahrscheinlichen Auswirkungen.

Anhand von zwei konkreten Anwendungsbeispielen lernen Sie das Vorgehen kennen, um die Bewertung einzelner Risikolagen für betroffene Personen vornehmen und nachweislich begründen zu können.

Darüber hinaus werden die Optionen für die Aufrechterhaltung und die fortlaufende Verbesserung der Durchführung einer DSFA sowie für die Dokumentation und Kommunikation dargelegt.

Die aktive Moderation von Diskussionen und der Erfahrungsaustausch der Teilnehmer untereinander runden diesen Workshop ab.

## INHALTE (Auszug)

- Die ISO 29134 - Leitlinien für die Datenschutz-Folgenabschätzung
- Der Begriff „Datenschutz-Folgenabschätzung“
- Die relevanten Bedrohungen
- Die relevanten Schwachstellen
- Die wahrscheinlichen Auswirkungen
- Der DSFA-Ablauf
- Die DSFA-Dokumentation
- Die DSFA-Kommunikation
- Durchführung einer beispielhaften DSFA für die „Einführung einer cloudbasierten Softwareanwendung“
- Durchführung einer beispielhaften DSFA für die „Datenschutzgerechte Ausgestaltung des Arbeitens im Home Office“

## TERMINE 2024

Berlin  
18. Januar  
21. März  
06. Juni  
08. August  
05. Dezember

## TERMINE 2024

Online  
18. Januar  
21. März  
06. Juni  
08. August  
05. Dezember

## VERANSTALTUNGSPREIS

650,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

550,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZIEL DES WORKSHOPS

Der Schwerpunkt des Workshops liegt auf der praxisorientierten Vermittlung der Durchführung einer Datenschutz-Folgenabschätzung unter Betrachtung konkreter Anwendungsbeispiele.

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Workshop für die Durchführung und Dokumentation einer Business Impact Analyse (DGI®)

Erlernen und optimieren Sie das praktische Vorgehen für die Durchführung einer Business Impact Analyse



Die Pflicht für die Durchführung von Business Impact Analysen (BIA) resultiert insbesondere aus den Anforderungen zahlreicher Normen und Standards, die für die Aufrechterhaltung der Betriebsfähigkeit der IT und für die zeitgerechte Erbringung von IT-gestützten Geschäftsprozessen zu beachten sind.

Die in den Normen und Standards festgelegten Modelle, Methoden und Vorgehensweisen für die Durchführung einer BIA zeugen zumeist von sehr theoretischer Natur und liefern nur unzureichende Ansätze für ein praktikables, effizientes und effektives Management der Projektierung einer BIA.

Im Rahmen dieses Workshops erlernen Sie die Handhabung eines modellhaften Ablaufs, um eine BIA, insbesondere unter Berücksichtigung der Ihnen zur Verfügung stehenden zeitlichen Ressourcen sowie einer angemessen transparenten Nachvollziehbarkeit für Dritte, durchführen zu können.

Wir vermitteln Ihnen, unter Einbeziehung eines Tools, zu berücksichtigende Zusammenhänge und wechselseitige Abhängigkeiten von zu betrachtenden Prozessen sowie von relevanten Risikofaktoren, wie etwa den Bedrohungen, Schwachstellen und wahrscheinlichen Auswirkungen.

Anhand von zwei konkreten Anwendungsbeispielen lernen Sie das Vorgehen kennen, um die Bewertung einzelner Risikolagen vornehmen und nachweislich begründen zu können.

Darüber hinaus werden die Optionen für die Aufrechterhaltung und die fortlaufende Verbesserung der Durchführung einer BIA sowie für die Dokumentation und Kommunikation dargelegt.

Die aktive Moderation von Diskussionen und der Erfahrungsaustausch der Teilnehmer untereinander runden diesen Workshop ab.

## INHALTE (Auszug)

- Die ISO 22313 - Business Continuity Management System
- Der BSI Standard 200-4 - Business Continuity Management
- Der Begriff „Business Impact Analyse“
- Der typische Aufbau von IT-gestützten Geschäftsprozessen
- Der BIA-Ablauf
- Die relevanten Bedrohungen
- Die relevanten Schwachstellen
- Die wahrscheinlichen Auswirkungen
- Die BIA-Dokumentation
- Die BIA-Kommunikation
- Durchführung einer beispielhaften BIA für den „Geschäftsprozess - Abrechnung und Zahlung von Gehältern und zugehörigen Abgaben“
- Durchführung einer beispielhaften BIA für den „Geschäftsprozess - Betrieb eines Webshops“

## TERMINE 2024

Berlin  
01. Februar  
30. Mai  
26. September  
28. November

## TERMINE 2024

Online  
01. Februar  
30. Mai  
26. September  
28. November

## VERANSTALTUNGSPREIS

650,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

550,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZIEL DES WORKSHOPS

Der Schwerpunkt des Workshops liegt auf der praxisorientierten Vermittlung der Durchführung einer Business Impact Analyse unter Betrachtung konkreter Anwendungsbeispiele.

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).



# Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung im Kontext der Informationssicherheit und des Datenschutzes (DGI®)

Erlernen und optimieren Sie das praktische Vorgehen für die Durchführung einer Dokumenten- bzw. Vertragsprüfung



Die Durchführung einer Dokumentenprüfung bzw. einer Vertragsprüfung stellt die generellen rechtlichen Anforderungen eines ordentlichen Kaufmanns gemäß dem Bürgerlichen Gesetzbuch (BGB), im Hinblick auf die Einhaltung der Sorgfaltspflichten, sicher und mindert zudem mögliche Risiken für die eigene Organisation und gegebenenfalls Dritte.

Im Rahmen dieses Workshops erlernen Sie die Handhabung eines modellhaften Ablaufs, um eine Dokumentenprüfung oder eine Vertragsprüfung, insbesondere unter Berücksichtigung der Ihnen zur Verfügung stehenden zeitlichen Ressourcen sowie einer angemessen transparenten Nachvollziehbarkeit für Dritte, durchführen zu können.

Wir vermitteln Ihnen, unter Einbeziehung eines Tools, zu berücksichtigende Zusammenhänge und wechselseitige Abhängigkeiten von einwirkenden Risikofaktoren für die Lenkung und Steuerung von Dokumenten und Verträgen sowie von möglichen wahrscheinlichen Auswirkungen infolge von Schwachstellen in Dokumenten und Verträgen.

Anhand von konkreten Anwendungsbeispielen lernen Sie das Vorgehen kennen, um die Bewertung einzelner Schwachstellen mit Auswirkung für die Lenkung und Steuerung von Dokumenten und Verträgen sowie für die Beachtung und Einhaltung von Rechten und Pflichten aus Dokumenten und Verträgen vornehmen und nachweislich begründen zu können.

Die aktive Moderation von Diskussionen und der Erfahrungsaustausch der Teilnehmer untereinander runden diesen Workshop ab.

## INHALTE (Auszug)

- Die „Dokumentierte Information“ - Anforderungen aus gängigen ISO-Normen
- Die Dokumentenlenkung und -steuerung
- Die Kriterien für die Dokumentenprüfung
- Die Vertragslenkung und -steuerung
- Die Kriterien für die Vertragsprüfung
- Die typischen Schwachstellen von Dokumenten und Verträgen
- Die wahrscheinlichen Auswirkungen
- Der Ablauf einer Dokumentenprüfung bzw. Vertragsprüfung
- Die Dokumentation einer Dokumentenprüfung bzw. Vertragsprüfung
- Die Kommunikation einer Dokumentenprüfung bzw. Vertragsprüfung
- Durchführung einer beispielhaften Dokumentenprüfung für eine „IT-Sicherheitsregelung“
- Durchführung einer beispielhaften Vertragsprüfung für einen „Auftragsverarbeitungsvertrag“

## TERMINE 2024

Berlin  
19. Januar  
22. März  
07. Juni  
09. August  
06. Dezember

## TERMINE 2024

Online  
19. Januar  
22. März  
07. Juni  
09. August  
06. Dezember

## VERANSTALTUNGSPREIS

650,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

Für Mitglieder von Verbänden und KRITIS-Betreiber

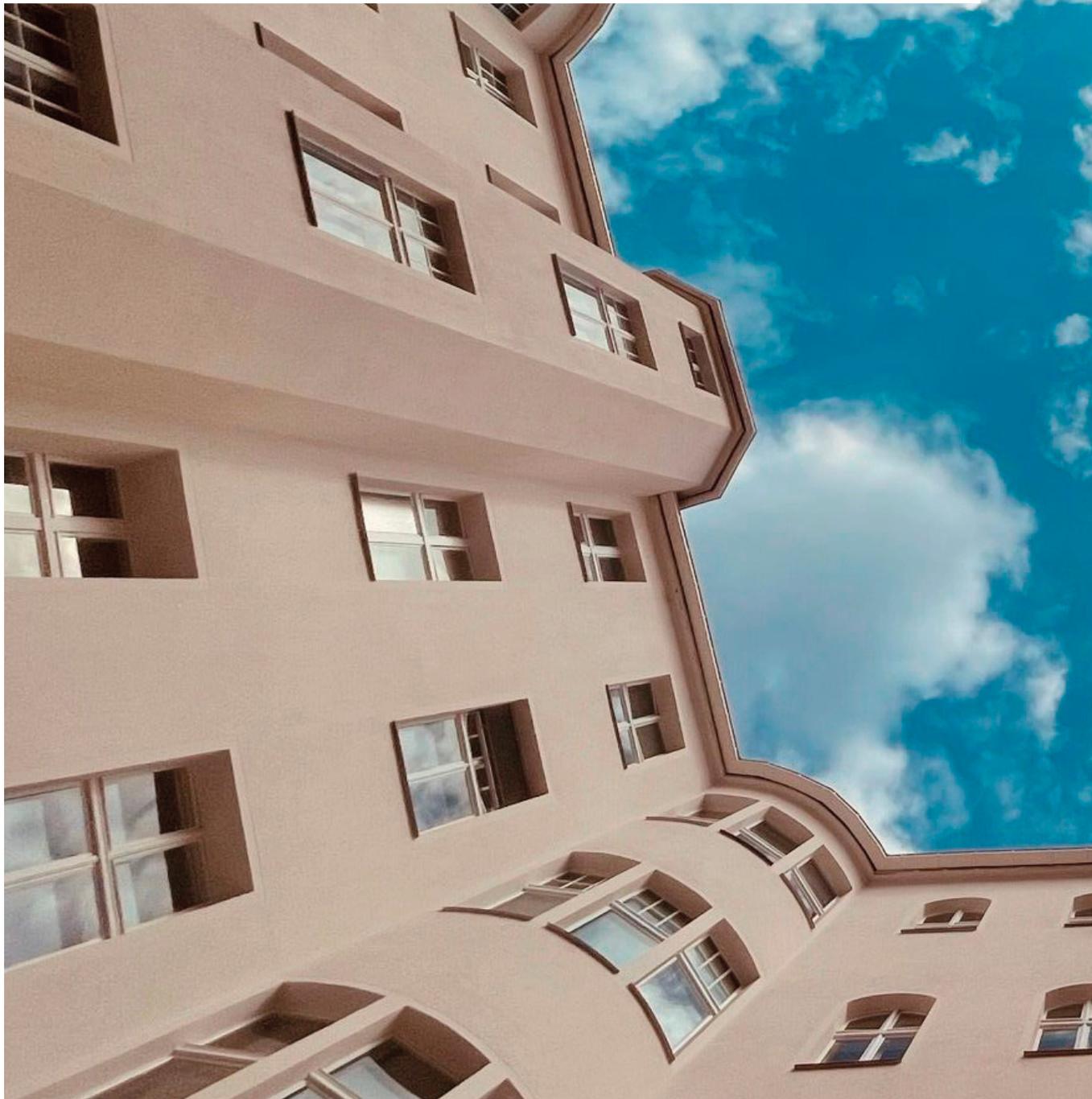
550,00 EUR - zuzüglich aktueller gesetzlicher Umsatzsteuer

## ZIEL DES WORKSHOPS

Der Schwerpunkt des Workshops liegt auf der praxisorientierten Vermittlung der Durchführung einer Dokumentenprüfung bzw. einer Vertragsprüfung unter Betrachtung konkreter Anwendungsbeispiele.

Weitere Informationen zur Veranstaltung finden Sie unter [www.DGI-AG.de](http://www.DGI-AG.de).







The background of the page is a blurred office scene. On the left, there is a wooden pen holder containing several pens, one of which has a bright green cap. In the center and right, a white binder with a silver ring is visible, resting on a desk. The binder is open, showing several pages. The overall lighting is soft and natural, typical of an office environment.

# INFORMATIONEN

- Veranstaltungsentwicklung und Qualitätssicherung
- Dozenten
- Lernumfeld und Seminarraum
- Inhouse-Veranstaltung
- Personenzertifizierung
- Chronologische Übersicht aller Veranstaltungen 2024
- Persönliche Notizen



# VERANSTALTUNGSENTWICKLUNG UND QUALITÄTSSICHERUNG

Die Akademie der DGI AG ist seit über 10 Jahren der qualifizierte und zuverlässige Geschäftspartner für öffentliche und nicht-öffentliche Kunden, wenn es um Ausbildungen, Seminare und Workshops in den Themengebieten der Informationssicherheit, des Datenschutzes, des IT-Risikomanagements sowie des Business Continuity Managements geht.

Um die Erwartungshaltung und die Anforderungen unserer Teilnehmerinnen und Teilnehmer an die besonders hohe Qualität unserer Ausbildungen, Seminare und Workshops fortlaufend in einer strukturierten und systematischen Art und Weise zu erfüllen, betreiben wir seit vielen Jahren ein zertifiziertes Qualitätsmanagementsystem (QMS) gemäß DIN ISO 9001.

Das zertifizierte QMS der Akademie der DGI AG erstreckt sich über sämtliche Phasen der Entwicklung, der Planung, dem Vertrieb, der Umsetzung sowie der Überwachung und der Verbesserung unserer Ausbildungen, Seminare und Workshops.

Die Verbesserung unserer Veranstaltungen erfolgt dabei kontinuierlich und zeitnah, auf der Basis einer Bewertung von Anlässen, die eine entsprechende Weiterentwicklung erfordern. Derlei Anlässe für die kontinuierliche Verbesserung unserer Ausbildungen, Seminare und Workshops können sich ergeben durch Veränderungen bei den themen- oder durchführungsspezifischen rechtlichen oder technischen Rahmenbedingungen, durch Vorschläge und Wünsche unserer Teilnehmerinnen und Teilnehmer sowie durch unser stetiges Bestreben, die objektiv betrachtet höchstmögliche Kundenzufriedenheit zu erreichen.

Die Ergebnisse unserer hohen Qualitätsbestrebungen können unsere Teilnehmerinnen und Teilnehmer bei der Vorbereitung, der Durchführung sowie der Nachbereitung unserer Ausbildungen, Seminare und Workshops höchstpersönlich erleben. Aus Sicht der Leitung der Akademie der DGI AG soll die Zufriedenheit unserer Teilnehmerinnen und Teilnehmer dabei in einem bestmöglichen Maß unabhängig davon sein, welche Dozentin oder welcher Dozent die Veranstaltung durchgeführt hat.



## DOZENTEN



**Ronny Neid**

*Vorstand | COO*

*DGI Deutsche Gesellschaft für  
Informationssicherheit AG*

Herr Neid ist Diplom-Betriebswirt und verantwortet als COO das operative Geschäft des Unternehmens. Herr Neid steuert Kundenprojekte in den Bereichen Informationssicherheit, Risikomanagement und Business Continuity Management.

Herr Neid ist der fachlich verantwortliche Ansprechpartner der Akademie der DGI AG für die Entwicklung von Ausbildungen mit Personenzertifikat, Seminaren und Workshops sowie für die Erstellung dazugehöriger Prüfungen, einschließlich Prüfungsfragen.

„Die Auswahl von geeigneten Dozentinnen und Dozenten für die Durchführung von Ausbildungen, Seminaren und Workshops der Akademie der DGI AG ist von entscheidender Relevanz für die objektiv betrachtete bestmögliche Kundenzufriedenheit nach einer Teilnahme an unseren Veranstaltungen.

Aus diesem Grund erfolgt die Auswahl unserer Dozentinnen und Dozenten stets unter der Maßgabe der persönlichen Qualifikation und Sachkunde, der individuellen Vortragskompetenz sowie der aktiven Mitwirkung bei der Weiterentwicklung unserer Veranstaltungsangebote.

Unseren Dozentinnen und Dozenten steht stets ein fachlich verantwortlicher Ansprechpartner in der Akademie der DGI AG zur Verfügung, um jedem Einsatz die Ergebnisse und Erkenntnisse der jeweiligen Veranstaltung zu erörtern und in die kontinuierliche Verbesserung einfließen zu lassen.“

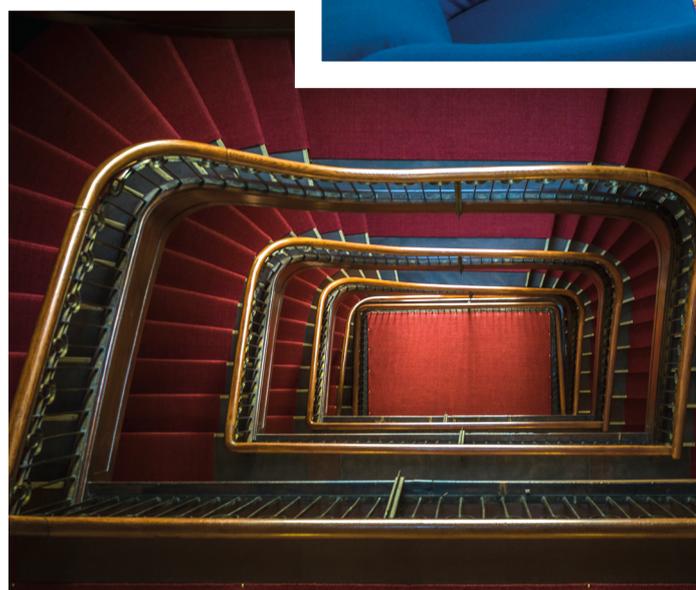
## LERNUMFELD UND SEMINARRAUM

Berlin, Charlottenburg, Kurfürstendamm.

In einer der wohl bekanntesten Gegenden Berlins befindet sich unser Firmensitz. Im obersten Stockwerk der Hausnummer 57 befinden sich unsere Seminarräume „Roberta“ und „Luise“.

Das Lernumfeld sowie die Veranstaltungen unseres Hauses selbst sind geprägt von Ansätzen der Nachhaltigkeit und Ganzheitlichkeit. Wir sind stets bestrebt dieses im gesamten Bereich der Veranstaltungsdurchführung gezielt durchzusetzen. So schaffen wir Räume eines lernunterstützenden und harmonischen Gesamtklimas, legen viel Wert auf eine vitaminreiche und hochwertige Pausenverkostung, ein reichhaltiges und hochwertiges Mittagsmenü sowie eine vielfältige Auswahl an Getränken und Obst während der gesamten Zeit der Veranstaltungsdurchführung.

Neben dem hohen Anteil an praxisbezogenen Themen bestechen die Ausbildungen mit Personenzertifikat sowie die Seminare der Akademie der DGI AG vor allem durch eine geringe Anzahl von Gruppenteilnehmern, die es dem Dozenten erlaubt sich jedem Teilnehmer intensiv zu widmen. Ob fachliche Fragen, Anregungen oder eigene Erfahrungen, die Teilnehmer sind stets dazu eingeladen sich aktiv zu beteiligen.





# INHOUSE-VERANSTALTUNG

## Individuell für Ihr Unternehmen

Mit der Durchführung unserer Ausbildungen mit Personenzertifikat und unserer Seminare in den Bereichen Informationssicherheit, Business Continuity Management, IT-Risikomanagement, IT-Sicherheit, ICS Security oder Datenschutz unterstützen wir Sie beim Aufbau erforderlichen Wissens sowie der kontinuierlichen Aufrechterhaltung des Know-hows Ihrer Mitarbeiter.

Unsere jahrelange Erfahrung aus der Beratung von Unternehmen sowie aus der Aus- und Weiterbildung setzen wir für Ihr Unternehmen gewinnbringend bei der erfolgreichen Entwicklung der fachlichen wie persönlichen Kompetenzen Ihrer Mitarbeiter ein.

Neben unseren Ausbildungen mit Personenzertifikat und unseren Seminare bieten wir Ihnen ergänzend begleitende Beratungsleistungen oder die Vertiefung des erworbenen Wissens Ihrer Mitarbeiter in unternehmensspezifischen Workshops.

Wir verstehen uns als wichtiges Bindeglied, um das erforderliche Wissen an Ihre Mitarbeiter zu vermitteln und die an Ihr Unternehmen gestellten Anforderungen an einen ordnungsgemäßen, sicheren und konformen Geschäftsbetrieb der IT-Prozesse Ihres Unternehmens sicherzustellen, risikoadäquate Maßnahmen zu erkennen und diese durch ein gezieltes Management zur Umsetzung zu bringen.

Sämtliche Ausbildungen und Seminare können für Ihr Unternehmen nach vorheriger Absprache hinreichend individualisiert werden, um die gewünschten Kenntnisse Ihrer Mitarbeiter aufzubauen und die erforderlichen Ziele des persönlichen Kompetenzaufbaus sicherzustellen.

Die Vorteile einer Inhouse-Veranstaltung für Ihr Unternehmen sind insbesondere

## Analyse und Festlegung Ihrer individuellen Weiterbildungsziele

- Eingehende Abstimmung der Weiterbildungsziele mit Ihren spezifischen Vorgaben
- Gesonderte Berücksichtigung der Vorkenntnisse Ihrer Mitarbeiter

## Maßgeschneiderte individuelle Weiterbildungsinhalte

- Zielgruppenspezifische Entwicklung von Weiterbildungsinhalten
- Individuelle Entwicklung von Veranstaltungunterlagen und Arbeitshilfen für Ihre Mitarbeiter
- Organisationsspezifische Entwicklung von Praxisbeispielen und Übungen

## Effektivität und Kosteneffizienz

- Durchführung der Inhouse-Veranstaltung an einem von Ihnen gewünschten Standort
- Wegfall der Belastung durch Reisezeiten für Ihre Mitarbeiter
- Kosteneffiziente Qualifikation Ihrer Mitarbeiter
- Einsparung von Reise- und Übernachtungskosten für Ihr Unternehmen

Bei Interesse an einer Inhouse-Veranstaltung erstellen wir Ihnen gerne ein individuelles Angebot.

# PERSONENZERTIFIZIERUNG

## Ihre persönliche Qualifikation

Eine Personenzertifizierung in den Bereichen Informationssicherheit, BSI IT-Grundschutz, Business Continuity Management, IT-Risikomanagement, ICS Security oder Datenschutz bietet Ihnen den Vorteil, das erworbene Fachwissen durch eine unabhängige Stelle bestätigen zu lassen und das erworbene Fachwissen qualifiziert nachweisen zu können.

Mit einer Personenzertifizierung der DGI Deutsche Gesellschaft für Informationssicherheit AG erwerben Sie einen Nachweis, dass Sie das Wissen und Know-how in dem Fachbereich der abgeschlossenen Ausbildung erfolgreich erworben haben.

Ihre erworbenen Kompetenzen und Qualifikationen durch den Besuch unserer Ausbildungen können Sie optional durch das Ablegen einer Zertifikatsprüfung unabhängig feststellen lassen. Mit dem erfolgreichen Abschluss der Prüfung wird Ihre Qualifikation durch ein personalisiertes Zertifikat bestätigt.

Ergänzend besteht für Sie die Möglichkeit, nach der Ausstellung Ihres Personenzertifikats DGI® ein personalisiertes Siegel für Ihre eigenen werblichen Zwecke zu erwerben.

Ihr personalisiertes Zertifikat sowie Ihr personalisiertes Siegel können Sie zusätzlich in englischer Sprache erwerben.

## Die Außendarstellung Ihrer persönlichen Qualifikation

Ihre nachgewiesene Qualifikation kann Anforderungen an die erforderliche Fachkunde eines IT-Sicherheitsbeauftragten oder betrieblichen Datenschutzbeauftragten erfüllen.

Zudem kann die transparente Außendarstellung Ihrer Qualifikation durch ein Personenzertifikat oder ein personalisiertes Siegel Ihrem Unternehmen Markt- und Wettbewerbsvorteile sichern.

Nach einer erfolgreich abgeschlossenen Ausbildung mit einem Personenzertifikat DGI® können Ihre persönlichen Angaben zur Personenzertifizierung in unserem öffentlichen Zertifikatsregister hinterlegt werden.

## Ihr personalisiertes Siegel



## Ihr Personenzertifikat DGI®



# CHRONOLOGISCHE ÜBERSICHT ALLER VERANSTALTUNGEN 2024

## BERLIN / ONLINE JANUAR

08. - 11. Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
15. - 17. Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG
15. - 18. Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
18. Workshop für die Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung (DGI®)
19. Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung im Kontext der Informationssicherheit und des Datenschutzes (DGI®)
22. - 24. Ausbildung zum ICS Security Manager (DGI®) gemäß IEC 62443, ISO 27001 und BSI IT-Grundschutz
22. - 24. Ausbildung zum BSI Vorfall-Praktiker (DGI®)
29. - 30. Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®)
29. - 31. Ausbildung zum Business Continuity Manager (DGI®)
31. - 01. IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit (DGI®)

## BERLIN / ONLINE FEBRUAR

01. Workshop für die Durchführung und Dokumentation einer Business Impact Analyse (DGI®)
05. - 07. Ausbildung zum BSI IT-Grundschutz-Berater (DGI®)
05. - 07. Ausbildung zum IT Risk Manager (DGI®)
08. Workshop für die Durchführung und Dokumentation einer IT-Risikoanalyse (DGI®)
12. - 13. Ausbildung zum Datenschutzbeauftragten im Gesundheitswesen (DGI®)
12. - 15. Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz

**BERLIN / ONLINE      FEBRUAR**

19. - 23.                    Ausbildung zum Lead Auditor ISO 27001 (DGI®)
26. - 28.                    Ausbildung zum Datenschutz-Auditor (DGI®)

**BERLIN / ONLINE      MÄRZ**

11. - 14.                    Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
18. - 20.                    Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG
18. - 21.                    Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
21.                            Workshop für die Durchführung und Dokumentation einer  
Datenschutz-Folgenabschätzung (DGI®)
22.                            Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung  
im Kontext der Informationssicherheit und des Datenschutzes (DGI®)
25. - 27.                    Ausbildung zum Business Continuity Manager (DGI®)

**BERLIN / ONLINE      APRIL**

08. - 09.                    IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit (DGI®)
08. - 10.                    Ausbildung zum IT Risk Manger (DGI®)
10. - 11.                    Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®)
15. - 18.                    Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
22. - 25.                    Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz

# CHRONOLOGISCHE ÜBERSICHT ALLER VERANSTALTUNGEN 2024

## **BERLIN / ONLINE      MAI**

- 06. - 08.      Ausbildung zum Datenschutz-Auditor (DGI®)
- 06. - 08.      Ausbildung zum BSI IT-Grundschutz-Berater (DGI®)
- 13. - 14.      Ausbildung zum Datenschutzbeauftragten im Gesundheitswesen (DGI®)
- 13. - 17.      Ausbildung zum Lead Auditor ISO 27001 (DGI®)
- 22. - 24.      Ausbildung zum BSI Vorfall-Praktiker (DGI®)
- 27. - 29.      Ausbildung zum Business Continuity Manager (DGI®)
- 27. - 30.      Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
- 30.            Workshop für die Durchführung und Dokumentation einer Business Impact Analyse (DGI®)

## **BERLIN / ONLINE      JUNI**

- 03. - 05.      Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG
- 03. - 06.      Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
- 06.            Workshop für die Durchführung und Dokumentation einer  
Datenschutz-Folgenabschätzung (DGI®)
- 07.            Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung  
im Kontext der Informationssicherheit und des Datenschutzes (DGI®)
- 10. - 12.      Ausbildung zum IT Risk Manger (DGI®)
- 13.            Workshop für die Durchführung und Dokumentation einer IT-Risikoanalyse (DGI®)
- 17. - 19.      Ausbildung zum ICS Security Manager (DGI®)
- 24. - 27.      Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz

**BERLIN / ONLINE      JULI**

01. - 04.                    Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
15. - 18.                    Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
22. - 26.                    Ausbildung zum Lead Auditor ISO 27001 (DGI®)
29. - 30.                    Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®)
29. - 31.                    Ausbildung zum Business Continuity Manager (DGI®)
31. - 01. I                    T-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit (DGI®)

**BERLIN / ONLINE      AUGUST**

05. - 07.                    Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG
08.                            Workshop für die Durchführung und Dokumentation einer  
Datenschutz-Folgenabschätzung (DGI®)
09.                            Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung  
im Kontext der Informationssicherheit und des Datenschutzes (DGI®)
12. - 14.                    Ausbildung zum IT Risk Manger (DGI®)
12. - 15.                    Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
15.                            Workshop für die Durchführung und Dokumentation einer IT-Risikoanalyse (DGI®)
19. - 22.                    Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
26. - 28.                    Ausbildung zum Datenschutz-Auditor (DGI®)

# CHRONOLOGISCHE ÜBERSICHT ALLER VERANSTALTUNGEN 2024

## BERLIN / ONLINE      SEPTEMBER

- 02. - 04.      Ausbildung zum BSI Vorfall-Praktiker (DGI®)
- 09. - 11.      Ausbildung zum BSI IT-Grundschutz-Berater (DGI®)
- 16. - 19.      Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
- 16. - 20.      Ausbildung zum Lead Auditor ISO 27001 (DGI®)
- 23. - 24.      Ausbildung zum Datenschutzbeauftragten im Gesundheitswesen (DGI®)
- 23. - 25.      Ausbildung zum Business Continuity Manager (DGI®)
- 26.      Workshop für die Durchführung und Dokumentation einer Business Impact Analyse (DGI®)

## BERLIN / ONLINE      OKTOBER

- 07. - 10.      Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
- 14. - 15.      Ausbildung zum IT Risk Manger (DGI®)
- 21. - 23.      Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG
- 21. - 23.      Ausbildung zum ICS Security Manager (DGI®)
- 28. - 31.      Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)

## BERLIN / ONLINE      NOVEMBER

- 04. - 06.      Ausbildung zum Datenschutz-Auditor (DGI®)
- 11. - 12.      IT-Grundlagen aus Sicht des Datenschutzes und der IT-Sicherheit (DGI®)

**BERLIN / ONLINE      NOVEMBER**

11. - 14.      Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
13. - 14.      Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®)
18. - 22.      Ausbildung zum Lead Auditor ISO 27001 (DGI®)
25. - 26.      Ausbildung zum Datenschutzbeauftragten im Gesundheitswesen (DGI®)
25. - 27.      Ausbildung zum Business Continuity Manager (DGI®)
28.            Workshop für die Durchführung und Dokumentation einer Business Impact Analyse (DGI®)

**BERLIN / ONLINE      DEZEMBER**

02. - 04.      Ausbildung zum Datenschutzbeauftragten (DGI®) gemäß DSGVO und BDSG
02. - 05.      Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)
06.            Workshop für die Durchführung und Dokumentation einer  
Datenschutz-Folgenabschätzung (DGI®)
07.            Workshop für die Durchführung einer Dokumenten- und Vertragsprüfung  
im Kontext der Informationssicherheit und des Datenschutzes (DGI®)
09. - 11.      Ausbildung zum IT Risk Manager (DGI®)
09. - 12.      Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) /  
Chief Information Security Officer (CISO) (DGI®) gemäß ISO 27001 und BSI IT-Grundschutz
12.            Workshop für die Durchführung und Dokumentation einer IT-Risikoanalyse (DGI®)
16. - 18.      Ausbildung zum BSI IT-Grundschutz-Berater (DGI®)
16. - 18.      Ausbildung zum BSI Vorfall-Praktiker (DGI®)



Satz und Layout: Chris Wiemer  
Druck: Copy-Terra

Bildnachweise:

dock64 | Paul Reichert  
JR Productions UG | Paul Reichert  
©AkuAku | stock.adobe.com  
©Alexander | stock.adobe.com  
©chee siong teh - stock.adobe.com  
©Destina | stock.adobe.com  
©EtiAmmos | stock.adobe.com  
©Funtap | stock.adobe.com  
©Golden Sikorka | stock.adobe.com  
©ilkercelek | stock.adobe.com  
©lenetsnikolai | stock.adobe.com  
©Maksim Kabakou | stock.adobe.com  
©MH | stock.adobe.com  
©Nmedia | stock.adobe.com  
©peterschreiber.media | stock.adobe.com  
©Stockwerk-Fotodesign - stock.adobe.com  
©sucharn | stock.adobe.com  
©tadamichi | stock.adobe.com  
©utah51 | stock.adobe.com  
©xiaoliangge | stock.adobe.com



AKADEMIE der

**DGI**<sup>®</sup> Deutsche Gesellschaft für  
Informationssicherheit AG

Kurfürstendamm 57 · D - 10707 Berlin

T +49 30 31 51 73 89 - 10 · F +49 30 31 51 73 89 - 20

AKADEMIE@DGI-AG.de · www.DGI-AG.de