



TRAINING 2-2026

Lehrgänge, Kurse, Schulungen, Workshops und Events

INFORMATIONSSICHERHEIT · DATENSCHUTZ · CYBER- UND IT SECURITY
RISIKOMANAGEMENT · BCM · KRISENMANAGEMENT
KI-SICHERHEIT · PERSONENSICHERHEIT · PHYSISCHE SICHERHEIT

Jetzt anmelden unter
www.infosec.ch/dis



EXKLUSIVKURS DIGITALE SOUVERÄNITÄT

Strategien für mehr Kontrolle im digitalen Zeitalter

Kursleitung: Pascal Stöckli, Projektleiter Digitale Souveränität am Institut Public Sector Transformation (IPST) der Berner Fachhochschule BFH und Mitgründer des Netzwerks Souveräne Digitale Schweiz (SDS)

Hotel Sedartis, Thalwil
23. Juni 2026, 09.00 – 16.30 Uhr

«ZEIT FÜR DAS NÄCHSTE KOMPETENZ-UPDATE»

Liebe Leserinnen und Leser

Neue technologische Entwicklungen, neue Anforderungen und neue Perspektiven machen lebenslanges Lernen wichtiger denn je. Wann war das letzte Update Ihrer Kompetenzen?



In der digitalen Welt sind Updates an der Tagesordnung und gerade im Hinblick auf das Thema Sicherheit enorm wichtig. Wer mit veränderten Anforderungen und Rahmenbedingungen Schritt halten will, muss aber nicht nur in Sachen Software am Ball bleiben, sondern besonders, wenn es um die eigenen Sicherheitskompetenzen geht.

Als perfekte Updates bieten sich hierbei unsere Aus- und Weiterbildungen an, die praxisbewährtes Wissen vermitteln und neue Perspektiven eröffnen:

Zum Beispiel die Lehrgänge für **Datenschutzbeauftragte (DSB)** (Seite 9), für **Informations- und IT-Sicherheitsbeauftragte (IT-SIBE)** (Seite 19) oder für **ISO 27001 Lead Auditoren** (Seite 39).

Falls Personal- oder Zeitressourcen für ein Update zu knapp sind, bringen wir unser Fachwissen gerne auch zu Ihnen ins Haus: Im Rahmen eines **Mandats** übernimmt beispielsweise ein **externer DSB** (Seite 12) Ihre Datenschutzaufgaben oder es unterstützt Sie ein **externer Chief Information Security Officer (CISO)** (Seite 38) bei Ihren Informationssicherheitsaufgaben.

Sie sehen, wir machen Ihnen ein Kompetenz-Update einfach. So einfach, dass es keinen Grund gibt, noch länger damit zuzuwarten.

In diesem Sinne auf bald.

Freundliche Grüsse
Ihr Reto Zbinden

Rechtsanwalt, CEO
reto.zbinden@infosec.ch

LEHRGÄNGE UND KURSE

Fundiertes und praxisorientiertes Fachwissen.

Besuchen Sie unsere zertifizierten und anerkannten Schulungen.

DATENSCHUTZ

Datenschutzberater (DSB)

Seite 9

Einführung in Aufgaben und Verantwortlichkeiten (DSG, DSGVO Basic)

🕒 5 Tage

📅 Startdaten: 04.05.2026 | 29.06.2026 | 07.09.2026 | 19.10.2026*

Datenschutz Grundlagen

Seite 13

Vom Datenschutz-Grünschnabel zum Datenschutz-Fuchs

🕒 1 Tag

📅 Startdaten: 11.05.2026* | 28.10.2026

Medizin und Datenschutz: Patientendaten sicher managen **NEU**

Seite 15

Datenschutzkurs für Fachpersonen aus dem Gesundheitswesen

🕒 1 Tag

📅 Startdaten: 09.06.2026* | 03.09.2026

Schweizer Datenschutzgesetz

infosec.ch/ds10

Einführung in das Datenschutzrecht in der Schweiz

🕒 2 Tage

📅 Startdaten: 18.06.2026* | 14.09.2026* | 05.11.2026

DSGVO-Intensiv

infosec.ch/ds02

Intensivschulung zur EU-Datenschutz-Grundverordnung (DSGVO Advanced)

🕒 3 Tage

📅 Startdaten: 20.05.2026* | 23.09.2026

COMPLIANCE

EU Data Compliance (Durchgeführt in Deutsch oder Englisch) **NEU**

Seite 17

Für den fachlichen Vorsprung im digitalen Regulierungsumfeld

🕒 5 Tage

📅 Startdaten: 10.08.2026* (EN) | 16.11.2026 (DE)*

EVENTS

MEET SWISS INFOSEC!

infosec.ch/msi

Aktuelle Tendenzen für Informationssicherheit, Datenschutz, IT-Sicherheit

🕒 4 h

📅 Datum: 25.01.2027

LEHRGÄNGE UND KURSE

Fundiertes und praxisorientiertes Fachwissen.

Besuchen Sie unsere zertifizierten und anerkannten Schulungen.

INFORMATIONSSICHERHEIT

Informationssicherheitsgesetz des Bundes

Seite 18

Das Informationssicherheitsgesetz des Bundes betrifft (fast) alle

🕒 4 Tage

📅 Startdaten: 26.05.2026 | 01.09.2026 | 01.12.2026*

Informations- und IT-Sicherheitsbeauftragter (IT-SIBE)

Seite 19

Praxiswissen über Aufgaben, Kompetenzen und Verantwortlichkeiten

🕒 5 Tage

📅 Startdaten: 08.06.2026 | 17.08.2026* | 14.12.2026

AI Manager Security & Privacy

Seite 22

Know-how zu Sicherheits- und Rechtsfragen von KI/AI-Systemen und -Services

🕒 5 Tage

📅 Startdaten: 04.05.2026* | 21.09.2026 | 09.11.2026*

Corporate Security Officer (CSO)

Seite 23

Die umfassende 360°-Sicht der Integralen Sicherheit kennenlernen

🕒 5 Tage

📅 Startdaten: 15.06.2026 | 23.11.2026*

Security Awareness Manager

NEU

Seite 24

Know-how zur Erstellung eines Security Awareness-Konzepts

🕒 3 Tage

📅 Startdaten: 15.06.2026* | 26.10.2026

Elektronische Archivierung

[infosec.ch/is04](https://www.infosec.ch/is04)

Kompetenz in rechtlichen, konzeptionellen und technischen Grundlagen erlangen

🕒 1 Tag

📅 Startdaten: 27.05.2026* | 20.10.2026

BUSINESS CONTINUITY MANAGEMENT, KRISENMANAGEMENT

Business Continuity Manager (BCM), Krisenmanager (KM)

Seite 25

Ausnahmesituationen in der Unternehmung meistern

🕒 5 Tage

📅 Startdaten: 24.08.2026* | 16.11.2026

PERSONENSICHERHEIT

Evakuierung

Seite 28

Grundlagen zur Umsetzung von Evakuationsinstruktionen

🕒 1 Tag

📅 Startdaten: 12.05.2026* | 08.09.2026

* Digitale Durchführung s. S. 7

LEHRGÄNGE UND KURSE

Fundiertes und praxisorientiertes Fachwissen.

Besuchen Sie unsere zertifizierten und anerkannten Schulungen.

CYBER- UND IT SECURITY

Cloud- und IT Security-Manager

Seite 29

Sichere und konforme Bereitstellung von IT Services on-premise oder in der Cloud  5 Tage

 Startdaten: 22.06.2026 | 14.09.2026 | 09.11.2026

Microsoft Cloud Security & Compliance Specialist

NEU

Seite 31

Security und Compliance in der Microsoft Cloud meistern  3 Tage

 Startdaten: 08.06.2026* | 05.10.2026 | 16.11.2026*

Prüfungsvorbereitung CISSP

Seite 33

CISSP-Zertifizierung dank seriöser Prüfungsvorbereitung  5 Tage

 Startdaten: 29.06.2026 | 14.09.2026 | 23.11.2026

Ethical Hacking (Digital)

Seite 34


Angriffe auf Netzwerk-, System- und Applikationsebene, inkl. Webapplikationen  5 Tage

 Startdatum: 19.10.2026*

Secure Coding (Digital)

Seite 35

Grundwissen bzgl. Sicherheit beim Entwickeln und Ausrollen von Software  4 Tage

 Startdatum: 27.10.2026*

RISIKOMANAGEMENT

Risikomanager

Seite 37

Risiken abschätzen und mögliche Schäden vermindern  4 Tage


 Startdaten: 06.05.2026 | 19.10.2026

EXKLUSIVKURSE

Digitale Souveränität

infosec.ch/dis

Strategien für mehr Kontrolle im digitalen Zeitalter  1 Tag

 Datum: 23.06.2026

Profiling

infosec.ch/prof

Menschen lesen und Täuschungen erkennen - mit Techniken aus der Praxis  1 Tag

 Datum: 13.10.2026

* Digitale Durchführung s. S. 7

ISO-SCHULUNGEN

Fundiertes und praxisorientiertes Fachwissen.

Besuchen Sie unsere zertifizierten und anerkannten ISO-Schulungen.

ISO 27001 / 27002 / 42001

ISO 27001 Lead Auditor	Seite 39
<i>ISMS nach ISO 27001 auditieren, mit Prüfungsabschluss</i>	🕒 5 Tage
📅 Startdaten: 04.05.2026 10.08.2026 23.11.2026	
ISO 27001 Manager	Seite 41
<i>Grundlagen und Prozesse der Informationssicherheit nach ISO 27001</i>	🕒 3 Tage
📅 Startdaten: 01.06.2026 28.09.2026* 09.12.2026	
Einführung ISO 27001, ISO 27002	infosec.ch/io03
<i>Grundlagen der Normen und Standards im Bereich Informationssicherheit</i>	🕒 1 Tag
📅 Startdaten: 18.08.2026 10.11.2026*	
ISO 42001 Lead Auditor NEU	Seite 43
<i>Einführung ins Auditing bezüglich der ISO-Norm 42001, inkl. Zertifizierung</i>	🕒 5 Tage
📅 Startdatum: 07.09.2026	

TIPP!

SWISS INFOSEC WEBINARE - KOMPAKT UND PRAXISNAH

Wissen aus erster Hand – zu aktuellen Security- und Compliance-Themen

Nehmen Sie sich etwas Zeit und profitieren Sie von wertvollem Fachwissen unserer Sicherheitsexpertinnen und -experten. Unsere Webinare sind kostenlos und bieten praxisnahe Einblicke, Tipps und Antworten auf Ihre Fragen – bequem und direkt online. www.infosec.ch/webinare

* Digitale Durchführung s. S. 7

WORKSHOPS & FIRMENSCHULUNGEN

Expertenwissen digital oder bei Ihnen vor Ort.

Unser Fachwissen massgeschneidert auf Ihr Unternehmen und Ihre Bedürfnisse.

DATENSCHUTZ

- | | |
|--|-----------|
| Workshop zum Schweizer Datenschutzgesetz | Seite 45 |
| <i>Datenschutzlücken? Unsere Experten liefern Antworten und Empfehlungen</i> | 🕒 1/2 Tag |
| Workshop Medizin und Datenschutz NEU | Seite 46 |
| <i>Für einen aktuellen und praxisorientierten Umgang mit Gesundheitsdaten.</i> | 🕒 1/2 Tag |

INFORMATIONSSICHERHEIT, CYBER- UND IT SECURITY

- | | |
|---|---|
| Workshop Information Governance | Seite 47 |
| <i>Wo steht Ihr Unternehmen bezüglich Information Governance?</i> | 🕒 1/2 Tag |
| Workshop zum Informationssicherheitsgesetz (ISG) des Bundes | infosec.ch/is12 |
| <i>Überblick über die Anforderungen, die das ISG an Sie stellt</i> | 🕒 1 Tag |
| Firmenschulung TISAX | infosec.ch/is15 |
| <i>Standard für Informationssicherheit in der Automobilindustrie</i> | 🕒 1 Tag |
| Workshop Cybervorfall: Vorbereitung und Incident Response NEU | Seite 48 |
| <i>Praxisnaher Überblick über den Umgang mit Cybervorfällen</i> | 🕒 1/2 Tag |
| Workshop IT Security und Datenschutz | Seite 49 |
| <i>Technik und Datenschutz vereint an einem halben Tag</i> | 🕒 1/2 Tag |
| Workshop KI-Sicherheit NEU | Seite 50 |
| <i>Fragen klären im Zusammenhang mit KI und Sicherheit/Datenschutz</i> | 🕒 1/2 Tag |
| IT Security Workshop NEU | Seite 51 |
| <i>Analyse Ihrer Fähigkeiten zur Abwehr von Cyberangriffen</i> | 🕒 1/2 Tag |
| Workshop Standortbestimmung IKT-Minimalstandard Gas NEU | Seite 52 |
| <i>Wo steht Ihr Unternehmen bezüglich IKT-Minimalstandard Gas?</i> | 🕒 1/2 Tag |

BUSINESS CONTINUITY MANAGEMENT, KRISENMANAGEMENT

- | | |
|---|---|
| Firmenschulung Stresstest zur Krisenbewältigung | infosec.ch/bc02 |
| <i>Richten Sie Ihr Augenmerk auf die wirklichen Bedrohungen</i> | 🕒 4 h |

WORKSHOPS & FIRMENSCHULUNGEN

Expertenwissen digital oder bei Ihnen vor Ort.

Unser Fachwissen massgeschneidert auf Ihr Unternehmen und Ihre Bedürfnisse.

Firmenschulung Krisen erfolgreich meistern

[infosec.ch/bc03](https://www.infosec.ch/bc03)

20-Stunden-Übung für Ihren Krisenstab

🕒 2 Tage

Workshop Krisenresilienz

[infosec.ch/bc04](https://www.infosec.ch/bc04)

Sind Sie auf die nächste Krise gut vorbereitet?

🕒 1/2 Tag

PERSONENSICHERHEIT

Firmenschulung Evakuationen sicher durchführen

[infosec.ch/pi04](https://www.infosec.ch/pi04)

Beweisen Sie Ihre Stärke in einer Notsituation

🕒 1 Tag

ALLGEMEINE HINWEISE

ANFRAGEN UND BUCHUNGEN

Für alle Lehrgänge, Kurse und Schulungen können Sie sich online über das Anmeldeformular beim Kurs, per E-Mail oder telefonisch anmelden. Kontakt: +41 41 984 12 12 oder infosec@infosec.ch

Alle Daten und Kurse finden Sie auch online in unserer Kursübersicht: www.infosec.ch/kurse

Es gelten für sämtliche in dieser Broschüre publizierten Angebote die AGB der Swiss Infosec AG.

Die AGB entnehmen Sie bitte unserer Webseite: www.infosec.ch/agb

VERGÜNSTIGUNG AB 3 PERSONEN DESSELBEN UNTERNEHMENS

Ab 3 Personen desselben Unternehmens gewähren wir bei Swiss Infosec-eigenen Lehrgängen und Kursen einen Rabatt von 10% auf den Gesamtbuchungspreis.

FIRMENSCHULUNGEN INDIVIDUELL NACH IHREN BEDÜRFNISSEN

Alle unsere Lehrgänge, Kurse, Workshops und Schulungen können auch als **firmeninterne Schulungen bei Ihnen vor Ort oder digital** durchgeführt werden. Gerne berücksichtigen wir dabei Ihre individuellen Bedürfnisse und Gegebenheiten. www.infosec.ch/inhouse

Kontaktieren Sie uns mit Ihren Wünschen unter +41 41 984 12 12 oder infosec@infosec.ch

*DIGITALE DURCHFÜHRUNG

Der Kurs wird ausschliesslich digital über Microsoft Teams durchgeführt. Teilnehmenden, die keine Möglichkeit haben, der Veranstaltung digital beizuwohnen, stellen wir die erforderliche Infrastruktur in unseren Schulungsräumen zur Verfügung.



Erfahrung – Verlässlichkeit – Stärke

1 Team – 2 Unternehmen – 3 Gemeinsamkeiten

Die Swiss Infosec AG und ihre Schwester Swiss GRC AG bilden ein agiles Team unterschiedlicher und ausgewiesener Fachleute, die in ihren Tätigkeitsfeldern ihre **Stärken und Erfahrungen** voll zum Tragen bringen. Gemeinsam erreichen wir kurze Reaktionszeiten auf Anfragen von Interessenten und Kunden. *Zeitgerechte, zielführende und präzise Antworten.*

Mit unseren erfahrenen und teils langjährigen über 130 Mitarbeitenden schaffen wir ein Klima von **Respekt und Wertschätzung**, das auch unsere Kunden spüren. Diese Qualität leben und fördern wir bewusst auch an Mitarbeiteranlässen. *Probleme werden gemeinsam gelöst und Erfolge gemeinsam gefeiert.*

Wir wollen unsere Marktposition als führendes Schweizer Beratungsunternehmen und Ausbildungsinstitut im Bereich der Integralen Sicherheit, insbesondere in **Informationssicherheit, Datenschutz und IT-Sicherheit**, weiter ausbauen und stärken. Unsere Kunden schätzen und kennen uns als ihren flexiblen, kompetenten und praxisorientierten Beratungspartner. *Die Zufriedenheit unserer Kunden steht im Zentrum unseres Handelns.*

Ihre Problemlösung beginnt mit einem Kontakt zu uns:

+41 41 984 12 12, infosec@infosec.ch

www.infosec.ch


Ihre Swiss Infosec AG



Datenschutzberater (DSB)

Für Datenschutzberater (Schweizerisches Datenschutzgesetz)

 5 Tage

 max. 12 Personen

DAS DATENSCHUTZGESETZ DER SCHWEIZ

In diesem Lehrgang werden Sie umfassend in die Aufgaben des «Datenschutzberaters» gemäss Art. 10 des Schweizerischen Datenschutzgesetzes (DSG) eingeführt. Sie lernen die gesetzlichen Anforderungen an diese Funktion kennen und können innerhalb Ihres Unternehmens die von Datenschutzfragen betroffenen Stellen fachkompetent unterstützen.

ZIELE

Sie lernen praxisorientiert die rechtlichen, organisatorischen und informationstechnischen Grundlagen und Anforderungen des Datenschutzes kennen und erhalten Hintergrundinformationen und Hilfestellungen, die für die firmeninterne Umsetzung und Einhaltung des Datenschutzes nützlich und relevant sind.

Sie werden dabei umfassend in die gesetzlich festgelegten Aufgaben, Kompetenzen und Verantwortlichkeiten des Datenschutzberaters eingeführt und erlangen die Fähigkeit, die Aufgaben eines Datenchtutzberaters kompetent und erfolgreich zu erfüllen.

Des Weiteren werden Sie befähigt, die Aspekte des Datenschutzes unternehmensintern gesetzeskonform zu vertreten. Sie werden im Bereich Datenschutz zu kompetenten

Gesprächspartnern für HR-Verantwortliche, IT-Mitarbeitende, Projektleiter und die Linie.

Nach dem Besuch dieses Lehrgangs verfügen Sie über die gewünschte Qualifikation für die Ausübung der Funktion des Datenschutzberaters gemäss Artikel 10 DSG.

Datenschutzberater (DSB)

Für Datenschutzberater (Schweizerisches Datenschutzgesetz)

🕒 5 Tage

👥 max. 12 Personen

INHALT

- Grundlagen des Datenschutzes, Datenschutz in der Schweiz und der EU (EU-Datenschutz-Grundverordnung DSGVO)
- Das Datenschutzgesetz, die Datenschutzverordnung (DSV)
- Aufbau eines Datenschutzmanagementsystems: Datenschutzpolitik, Datenschutzkonzept, Zugriffsschutzkonzepte, Berechtigungs- und Rollenkonzepte
- Interne Überwachung: E-Mail- und Internetüberwachung, Grenzen der Überwachung
- Zugriff und Protokollierung: E-Mail, Internet, persönliche Ordner, mobile Systeme
- Inventarisierung und Klassifizierung der Datensammlungen, Dokumentation der Datenverarbeitungen im Unternehmen, Bearbeitungsreglemente
- Bearbeitung von Daten, Datentransfer ins Ausland, Rechtsansprüche der Betroffenen, Vorgehen bei einem Auskunftsbeglehen, Pflichten der Datenbearbeiter, Haftungsrisiken, Datenschutzaufsicht, Interessenkollisionen im Datenschutz
- Datenschutzerfordernissen in Outsourcing-Verhältnissen
- Datenschutzeraspekte: Cloud Computing, BYOD, Social Media, Big Data
- Technischer Datenschutz/Systemdatenschutz wie Transport-, Zugangs-, Personendatenträger-, Bekanntgabe-, Speicher-, Benutzer-, Zugriffs- und Eingabekontrolle
- Verschlüsselung, Authentisierung, interne Protokollierungen
- Berücksichtigung von Datenschutzeraspekten in Projekten
- Anforderungen an die reversionssichere Protokollierung
- Archivierung vs. Datenschutz
- Quellen zum Datenschutz



ZIELGRUPPE


Personalverantwortliche, IT-Projektleiter, betriebliche Datenschutzberater und -beauftragte, Datenschutzverantwortliche, Revisoren, Sicherheitsverantwortliche, Compliance Officer oder generell Personen, die sich mit Fragen des Datenschutzes zu befassen haben.



Datenschutzberater (DSB)

Für Datenschutzberater (Schweizerisches Datenschutzgesetz)

 5 Tage

 max. 12 Personen

TERMINE/ORTE

04.05.2026 - 08.05.2026 Sursee
29.06.2026 - 03.07.2026 Sursee
07.09.2026 - 11.09.2026 Thalwil
19.10.2026 - 23.10.2026 Digital*
30.11.2026 - 04.12.2026 Sursee

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/ds01



Nach dem Besuch dieses Lehrganges verfügen Sie über die gewünschte Qualifikation für die Ausübung der Funktion des «Datenschutzberaters» gemäss Art. 10 DSG. (bisher: Betrieblicher Datenschutzverantwortlicher gem. Art. 12a Abs. 2 VDSG)

«Interessanter Lehrgang mit geballtem Wissen auf einem verständlichen und angenehmen Niveau. Die aktive Diskussion und konkrete Fallbeispiele ermöglichen einen grossen Praxisbezug.»

*Michael Heinzl, Head of Data Protection,
Liebherr Machines Bulle SA*

«Der Lehrgang ist super! Die einzelnen Thementage sind sehr gut aufgeteilt und die Experten geben viele Inputs und Beispiele aus der Praxis. Die Teilnehmergruppe war spitze und das Lernen hat Spass gemacht.»

*Angela Mattmann, Datenschutzbeauftragte,
IWP AG*

«Der Lehrgang war sehr hilfreich und es wurde auf alle Fragen eingegangen. Auch die Unterlagen waren eine grosse Hilfe und sind perfekt zum Nachschlagen.»

*Alexandra Bender, Verantwortliche
Qualitätsmanagement, Elco AG*

Informationspflicht

Einwilligung

Newsletter

Auskunftsrecht

**Rechtmässigkeit von
Datenbearbeitungen**



Werbeversände

Archivierung

Klassifizierung

Kundendaten

**Besonders
schützenswerte
Personendaten**

Mandat: Externer Datenschutzbeauftragter (DSB) / Data Protection Officer (DPO)

Beratung, Schulung und Services: Datenschutzwissen nach DSG und EU-DSGVO

Als externe Datenschutzbeauftragte übernehmen wir Ihre Datenschutzaufgaben auf Mandatsbasis und sorgen für angemessene Datenschutzlösungen, die die Vorgaben der entsprechenden Gesetze (DSG und/oder DSGVO/GDPR) rechtskonform umsetzen. Unsere Spezialistinnen und Spezialisten machen Datenschutz in Ihrem Unternehmen sichtbar, sind Ansprechpartner für die Geschäftsleitung und übernehmen auf Wunsch auch die Schulung und Sensibilisierung Ihrer Mitarbeitenden.

Wir kennen alle Hürden und Fallstricke und beantworten Ihre Fragen schnell und präzise. Wann setzen Sie auf unsere Expertise?

Kontaktieren Sie uns für ein persönliches und unverbindliches Erstgespräch:
infosec@infosec.ch, Telefon +41 41 984 12 12

www.infosec.ch/dsb

www.infosec.ch/mandat-dsb (PDF)


www.infosec.ch/datenschutz



Datenschutz Grundlagen

Vom Datenschutz-Grünschnabel zum Datenschutz-Fuchs

 1 Tag

 max. 12 Personen

UNSICHER IM UMGANG MIT PERSONENDATEN UND RECHTLICHEN VORSCHRIFTEN?

Dieser Kurs beantwortet Fragen wie z.B. wie eine Datenschutzerklärung zu erstellen ist oder was zu beachten ist beim Newsletter-Versand, bei der Bearbeitung von Mitarbeiterdaten im Personaldossier oder beim Prüfen der Datenschutzvereinbarung des europäischen Geschäftspartners. Teilnehmende erhalten Hilfestellungen für die Umsetzung des Datenschutzes nach DSGVO oder der DSGVO.

INHALT

- Anwendungsbereich und Prinzipien der Datenschutzgesetzgebung
- Methodik zum Aufbau eines datenschutzkonformen Umgangs mit Personendaten im Unternehmen
- Umgang mit Newsletter- und Werbeversand
- Rechtskonforme Erstellung einer Datenschutzerklärung
- Datenschutz und HR: Beantwortung der wichtigsten Fragen im Zusammenhang mit dem Personaldossier (Aufbewahrung und Einsicht von Dokumenten wie Arztzeugnisse, Einwilligung in die Veröffentlichung von Mitarbeiterfotos, Überwachung des E-Mail-Verkehrs etc.)
- Hilfestellung beim Erstellen von Löschprozessen und Umgang mit Anfragen von betroffenen Personen

ZIELGRUPPE

Personalverantwortliche, Marketing und Kommunikation, IT und generell Personen, die sich mit Fragen des Datenschutzes zu befassen haben.

TERMINE/ORTE

11.05.2026 Digital*
28.10.2026 Sursee

Weitere Daten und Buchung: infosec.ch/ds04

KOSTEN

CHF 1050.– (exkl. MwSt.)

FIRMENSCHULUNG

Diese Ausbildung kann auch als firmeninterne Schulung bei Ihnen vor Ort durchgeführt werden.

Datenschutz

ISMS

IT-Sicherheit

Archivierung

Information Governance

Krisenmanagement

Physische Sicherheit**Business Continuity Management**

Awareness

Personensicherheit

Cybersecurity

Data Center Security

KI-Governance**Informationssicherheit****Mandate by Swiss Infosec AG**

Interdisziplinäres Fachwissen für mehr Unternehmenssicherheit nach Best Practice

Termindruck, fehlende Ressourcen, eine lange Pendenzenliste. Gute Gründe, weshalb der Einsatz eines externen Spezialisten oder einer externen Spezialistin der Swiss Infosec AG Sinn machen kann.

Wir beraten, unterstützen und schulen Sie in allen Fragen rund um Integrale Sicherheit und stehen Ihnen auf Wunsch stundenweise oder auf Mandatsbasis als starke Stütze zur Seite! Mit grosser Erfahrung in interdisziplinärem Teamwork gehen unsere Fachspezialisten und Fachspezialistinnen auf Ihre individuellen Anliegen ein, z.B. als:

- Externer Datenschutzbeauftragter (DSB) / Data Protection Officer (DPO)
- Chief Information Security Officer (CISO)
- Cybersecurity Officer (CSO) / IT Security Officer (ISO)
- Externer KI-Governance Manager
- Business Continuity Manager
- Awareness Manager as a Service
- Weitere Möglichkeiten s. unter www.infosec.ch/mandate


Wann setzen Sie auf das Best Practice-Know-how der Swiss Infosec AG?


Kontaktieren Sie uns für ein persönliches und unverbindliches Erstgespräch.
+41 41 984 12 12, infosec@infosec.ch



NEU! Medizin und Datenschutz: Patientendaten sicher managen

Datenschutzkurs für Fachpersonen aus dem Gesundheitswesen

 1 Tag

 max. 12 Personen

HEALTH & PRIVACY-KURS: DATENSCHUTZKOMPETENZEN FÜR GESUNDHEITSPROFIS

Nach diesem Kurs kennen Sie die Vorgaben zur Weitergabe von Patientendaten und wissen, wann und wofür Sie die Einwilligung der PatientInnen einholen müssen. Zudem verstehen Sie die datenschutzrelevanten Aspekte moderner Technologien wie KI-Tools und Cloud-Lösungen und sind in der Lage, diese rechtssicher im Arbeitsalltag einzusetzen.

INHALT

- Anwendbares Recht (Schweizerisches DSG oder kantonale Datenschutzgesetze, spezialgesetzliche Bestimmungen zum Gesundheitswesen)
- Einwilligung der PatientInnen und Informationspflichten
- Sicherer Umgang mit Patientendaten (Zugriffsberechtigungen, Umgang mit Besuchern, etc.)
- Weitergabe von Patientendaten (Überweisungen, Besprechungen im Konsil, Daten aus Smart Devices, Verwendung zu Studienzwecken, Meldungen an Behörden, usw.)
- Auslagerung der Datenspeicherung in Cloud-Lösungen
- Verwendung von Künstlicher Intelligenz (Personalplanung, Voice-to-Text, Generative KI zur Diagnosestellung oder zum Verfassen von Berichten, etc.)

ZIELGRUPPE

Medizinisches Personal, Pflege, Administration, Compliance und IT-Verantwortliche aus Spitälern, Arztpraxen, Pflegeeinrichtungen, Forschung und der MedTech-Branche, Themeninteressierte.

TEILNAHMEVORAUSSETZUNG

Erste Erfahrungen und Grundlagenwissen im Datenschutz.

TERMINE/ORTE

09.06.2026 Digital*
03.09.2026 Sursee

Weitere Daten und Buchung: infosec.ch/ds13

KOSTEN

CHF 1050.– (exkl. MwSt.)



Vertretermandate nach den gesetzlichen Vorgaben der Schweiz und der EU

Wir stehen Ihnen als externe gesetzlich anerkannte Vertreter in einem Mandatsverhältnis zur Verfügung. Unsere Spezialistinnen und Spezialisten sorgen in der Rolle des externen Vertreters dafür, dass Anforderungen und Anfragen seitens Behörden koordiniert, fristgerecht und in Ihrem Interesse bearbeitet werden.

Profitieren Sie von unserer Beratung flexibel und ad hoc – genau dann, wenn Sie sie brauchen.

Unsere Vertretermandate:

- Externer Vertreter nach DSG
- Externer Vertreter nach DSGVO
- UK-Verteter nach UK GDPR
- Externer EU-Vertreter nach NIS-2
- Externer UK-Vertreter nach UK NIS
- Externer EU-Vertreter nach Data Act
- Externer EU-Vertreter nach Digital Services Act (DSA)
- Externer Vertreter für GPAI-Anbieter
- Externer Vertreter von Anbietern von Hochrisiko-KI-Systemen
- u.v.m.

Kontaktieren Sie uns für ein persönliches und unverbindliches Erstgespräch.

+41 41 984 12 12, infosec@infosec.ch

www.infosec.ch/vertretermandate



NEU! EU Data Compliance (DE oder EN)

Verschaffen Sie sich im digitalen Regulierungsumfeld einen fachlichen Vorsprung

🕒 5 Tage

👥 max. 20 Personen

WIE WIRKEN SICH AKTUELLE EU-RECHTSAKTE AUF IHRE ORGANISATION AUS?

AI Act, NIS-2, DSA, DORA & Co.: Dieser Lehrgang vermittelt fundiertes Wissen zu den EU-Rechtsakten rund um Data Compliance – und zeigt, wie auch Organisationen ausserhalb der EU Risiken früh erkennen, rechtssicher handeln und Chancen strategisch nutzen können.

INHALT

- Überblick über die digitale Agenda der EU (Absichten, Ziele, Governance)
- Inhalte, Anwendungsbereiche und Auswirkungen folgender EU-Rechtsakte:
 - AI Act, Cyber Resilience Act (CRA), DSGVO, Digital Services Act (DSA), Digital Markets Act (DMA), Data Governance Act (DGA), Data Act, Digital Operational Resilience Act (DORA), NIS-2
 - Ausblick: Digital Fairness Act/Digital Networks Act

Weitere Infos und Buchung: infosec.ch/co01

ZIELGRUPPE

Fach- und Führungskräfte sowie Berufspraktikerinnen und -praktiker, die mit regulatorischen, rechtlichen oder technischen Aspekten der Datenverarbeitung und digitalen Compliance im EU-Kontext betraut sind.

TEILNAHMEVORAUSSETZUNG

- Grundkenntnisse im Datenschutz (z. B. DSGVO) oder Informationssicherheitsmanagement
- Berufserfahrung in den Bereichen Recht, Compliance, IT, Datenschutz, digitale Geschäftsmodelle oder regulierte Branchen (z. B. Finanzmarkt, Gesundheitswesen)
- Bereitschaft, sich mit rechtlichen Texten und regulatorischen Anforderungen auseinanderzusetzen

TERMINE/ORTE

10.08.2026 - 14.08.2026 Digital* (EN)

16.11.2026 - 20.11.2026 Digital* (DE)

KOSTEN

CHF 4950.– (exkl. MwSt.)



Informationssicherheitsgesetz

Das Informationssicherheitsgesetz des Bundes betrifft (fast) alle

🕒 4 Tage

👥 max. 12 Personen

«GOOD PRACTICE» FÜR DIE UMSETZUNG DER VORGABEN DES ISG

Das Informationssicherheitsgesetz des Bundes (ISG) enthält anspruchsvolle gesetzliche Vorgaben für Bundesbehörden, kantonale Behörden und privatrechtliche Unternehmen, die den Bund bei der Wahrnehmung seiner Aufgaben unterstützen. In diesem Lehrgang lernen Sie die rechtlichen, organisatorischen und technischen Grundlagen kennen, die Ihr Unternehmen, Ihre Organisation oder Behörde benötigt, um die Anforderungen des ISG auf effiziente und praktikable Weise zu erfüllen.

INHALT

- Cyber- und andere Gefahren für Informationen und IT-Infrastrukturen
- Die nationale Cyberstrategie des Bundes
- Das Informationssicherheitsgesetz des Bundes: Ziele, Geltungsbereich, Massnahmen
- «Good practice» in der Informations- und IT-Sicherheit: Standard ISO/IEC 27001/27002
- Umsetzung in der Praxis
- Informationssicherheit und Datenschutz
- Weitere Inhalte online: infosec.ch/is11

ZIELGRUPPE

Sicherheitsverantwortliche, Zuständige für Legal und Compliance, Projektleiter sowie Vertreter von Behörden, Betreibern von kritischen Infrastrukturen oder externen Dienstleistern des Bundes.

TERMINE/ORTE

26.05.2026 - 29.05.2026 Sursee
01.09.2026 - 04.09.2026 Thalwil
01.12.2026 - 04.12.2026 Digital*

KOSTEN

CHF 4150.– (exkl. MwSt.)

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.

FIRMENSCHULUNG

Diese Schulung kann auch als firmeninterne Schulung bei Ihnen vor Ort, abgestimmt auf Ihre Bedürfnisse, durchgeführt werden.

Informations- und IT-Sicherheitsbeauftragter (IT-SIBE)

Lehrgang für Information und IT Security Officer

🕒 5 Tage

👥 max. 12 Personen

GEBALLTES WISSEN AUS JAHRELANGER ERFAHRUNG

Wir führen Sie seit über 30 Jahren erfolgreich und umfassend in die Grundlagen der Informations- und IT-Sicherheit ein. Dabei legen wir grossen Wert auf Best Practices wie beispielsweise ISO 27001/27002 beim Aufbau und Betrieb eines Informationssicherheitsmanagementsystems ISMS. Unsere integrale Sichtweise auf organisatorische, technische, physische, personelle und rechtliche Aspekte der Sicherheit eröffnet Ihnen einen zukunftsweisenden 360°-Blick auf die Informationssicherheit von heute.

ZIEL

Nach dem Lehrgang können Sie das erworbene Wissen in den Bereichen Informationssicherheit und IT-Sicherheit in Ihren Aufgaben und Verantwortlichkeiten als Informations- und IT-Sicherheitsbeauftragte optimal einsetzen.

Fallbeispiele aus der Praxis sowie Checklisten, Musterdokumente und Formulare befähigen Sie, die interne Informations- und IT-Sicherheit zu analysieren, zu organisieren und umzusetzen.

Sie sind sich Ihrer wichtigen Funktion als Schnittstelle zwischen Geschäftsführung und Mitarbeitenden bewusst und tragen Ihren Teil zum Schutz des Unternehmens bei.



Informations- und IT-Sicherheitsbeauftragter (IT-SIBE)

Lehrgang für Information und IT Security Officer

🕒 5 Tage

👥 max. 12 Personen

INHALT

- Die Rolle der Unternehmensführung in Sicherheit, Sicherheitskultur, Sicherheitspolitik, Sicherheitsorganisation
- Mensch und Sicherheit, Motivation und Ausbildung des Personals
- Informationssicherheit, IT-Sicherheit, Informationsschutz, Datenschutz
- Informationssicherheitsmanagementsystem ISMS (ISO 27001/27002)
- Die Rolle des Informations- und Sicherheitsbeauftragten
- Integration aller Mitarbeitenden in die Sicherheitsarbeit (Mitarbeitersensibilisierung)
- Risikomanagement, Risikoanalyse, Massnahmenplanung und -behandlung
- Physische Sicherheit, Zutrittsschutz und kritische Infrastrukturen
- Business Continuity Management (ISO 22301/BCMS), BCP und Disaster Recovery, Business Impact-Analysen
- Krisenmanagement: Aufbau und Kontinuität von Ausbildungen für Krisenstäbe
- Rechtliche Aspekte: Datenschutz und Datensicherheit, Privatrecht und öffentliches Recht, Haftungsfragen, Benutzerregeln für Internet/E-Mail
- Mobile Security/BYOD
- Technische Sicherheit, Authentisierungsmethoden und Passwortsicherheit
- Malware, Applikationssicherheit
- Technische und organisatorische Sicherheitsmassnahmen
- Outsourcing: Wo liegen die Gefahren?
- Personelle Sicherheitsmassnahmen
- Planung und Durchführung von Audits im Bereich Sicherheit (ISO 27001/ISMS)
- Fallstudien und Vorgehenskonzepte für die Praxis
- Anforderungen an das interne Regelwerk




ZIELGRUPPE


Security Officer, Information Security Officer, Sicherheitsbeauftragte, Sicherheitsverantwortliche, IT-Leiter, Business Unit-Leiter, Projektleiter, Themeninteressierte



Informations- und IT-Sicherheitsbeauftragter (IT-SIBE)

Lehrgang für Information und IT Security Officer

 5 Tage

 max. 12 Personen

TERMINE/ORTE

08.06.2026 - 12.06.2026 Sursee
17.08.2026 - 21.08.2026 Digital*
14.12.2026 - 18.12.2026 Sursee

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/is01

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.

Wir veranstalten diesen einmaligen Lehrgang in der Schweiz seit 1992 mit grossem Erfolg. Die durchwegs positiven Referenzen zu diesem Lehrgang beweisen dessen Qualität.



«Guter Überblick über die zahlreichen Themen und Aspekte eines IT-SIBEs. Gutes Networking, da vor Ort spannende Diskussionen entstanden und man sich mit anderen Kursteilnehmern abgleichen konnte.»

*Konstanze Schäfer, ICT-Security Officerin,
Informatik Stadt Bern*

«Mein Highlight der Woche war der technische Teil, der sehr informativ war und coole Demo Sessions enthielt. Aber auch die eher trockenen rechtlichen Themen wurden abwechslungsreich, humorvoll und kurzweilig rübergebracht.»

*Cedric Neuenschwander, ICT-Security Officer,
Informatik Stadt Bern*

«Es war ein intensives und beeindruckendes Lernerlebnis in einem engagierten Team mit Leidenschaft für IT-SIBE-Aufgaben. Die TrainerInnen der Swiss Infosec haben sehr wirksam einen kompakten Transfer zentraler Kompetenzen ermöglicht. Vielen Dank.»

*Alexander Höhne, Leitung ICT,
Freie Gemeinschaftsbank Genossenschaft*



AI Manager Security & Privacy

Know-how zu Sicherheits- und Rechtsfragen von KI/AI-Systemen und -Services

🕒 5 Tage

👥 max. 12 Personen

GENERATIVE KI/AI IM ZEICHEN VON SECURITY UND PRIVACY

Nach diesem Lehrgang verfügen Sie über KI/AI-bezogenes Grundlagenwissen in den Themen Sicherheit (u.a. Informationssicherheit, IT-Sicherheit) und Recht (u.a. Datenschutz, Urheberrecht). Sie sind in der Lage, Begrifflichkeiten rund um künstliche Intelligenz einzuordnen, haben ein klares Verständnis für KI/AI entwickelt und können KI/AI-Projekte aus Sicht Security und Privacy beurteilen. Ebenfalls erfahren Sie, welche Vorgaben zu KI/AI bestehen (national und international, u. a. EU AI Act).

INHALT

- Grundlagenwissen und gemeinsames Verständnis generativer KI/AI
- Governance (Ethik, Prinzipien, Richtlinien etc.), Rolle der Information Governance
- Risiken und Bedrohungen
- KI/AI und das Thema Sicherheit: Problemstellungen, Spannungsfelder, Fragestellungen
- Übergeordnete Grundsätze und rechtliche Herausforderungen insbesondere bezüglich Urheberrecht und Datenschutz
- Datenschutz und KI/AI, Privacy by Design und Privacy by Default
- Anonymisierung und Pseudonymisierung von Daten
- Incident Response und Notfallplanung
- ISMS und KI/AI
- Risikoanalyse und Sicherheitsbewertungen
- Compliance und Risikomanagement

- Umsetzung der Anforderungen
- Anwendungsbeispiele: Bild- und Videoanalysen gegen Deepfakes

ZIELGRUPPE

Funktionsträger mit Aufgaben im Bereich KI/AI, die sich fundiertes Wissen bez. Sicherheit (Informationssicherheit, IT-Sicherheit) und Recht (u.a. Datenschutz) aneignen wollen.

TERMINE/ORTE

04.05.2026 - 08.05.2026 Digital*
21.09.2026 - 25.09.2026 Sursee
09.11.2026 - 13.11.2026 Digital*

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: [infosec.ch/is16](https://www.infosec.ch/is16)



Corporate Security Officer (CSO)

Die umfassende 360°-Sicht zum Thema Integrale Sicherheit

 5 Tage

 max. 12 Personen

ALLE ASPEKTE DER INTEGRALEN SICHERHEIT

Nach diesem Lehrgang sind Sie in der Lage, ein integrales Sicherheits-Managementsystem projektartig aufzubauen, umzusetzen und zu betreiben. Sie lernen Prozesse und Instrumente für das Managen der Integralen Sicherheit kennen. Zudem erlangen Sie die Fähigkeit, Synergien zu bestehenden Managementsystemen sowie Handlungsfelder und Anknüpfungspunkte zu Schweizer Gesetzen und Vorschriften zu erkennen und zu nutzen.

INHALT

- Managementsystem: Inhalte, PDCA-Zyklus, Konzipierung, Aufbau, Betrieb, Tools
- Integrale Sicherheits-Policy, Fachkonzepte
- Sicherheitsorganisation, -kultur, -prozesse
- Risk Management, Risk Analysis, Risk Treatment, Risk Treatment Planning
- BCM, Business Impact-Analyse, BC Planning
- Notfall- und Krisenmanagement
- Compliance
- Versicherungsschutz
- Physische Sicherheit
- Arbeitssicherheit und Gesundheitsschutz
- Informations- und IT-Sicherheit
- Sensibilisierung, eLearning
- Integration in bestehende Managementsysteme und Prozesse, ISO 27001

KOSTEN

CHF 4950.– (exkl. MwSt.)

METHODIK

Aktive Mitarbeit, Transfer mittels Praxisarbeit. Durchführung einer Analyse für das eigene Unternehmen und Entwicklung eines Grobkonzeptes für die Realisierung eines integralen Sicherheits-Managementsystems.

ZIELGRUPPE

Fachpersonen (Sicherheit, Qualität, Risiko, Umwelt, Arbeitssicherheit), die sich mit integrelem Sicherheitsmanagement auseinandersetzen wollen sowie Verantwortliche, die Sicherheitsmanagement systematisch und nachhaltig betreiben möchten.

TERMINE/ORTE

15.06.2026 - 19.06.2026 Sursee

23.11.2026 - 27.11.2026 Digital*

Weitere Infos und Buchung: infosec.ch/is02




NEU!

Security Awareness Manager

Know-how zur Erstellung eines Security Awareness-Konzepts und einer Ausbildungsplanung

 3 Tage

 max. 12 Personen

FÜR EINE SICHERHEITSBEWUSSTE KULTUR IM UNTERNEHMEN

Nach Abschluss dieses Kurses sind Sie in der Lage, ein umfassendes und strukturiertes Security Awareness-Konzept zu entwickeln und dessen erfolgreiche Umsetzung zu planen. Sie lernen bewährte Methoden, Ansätze der Verhaltenspsychologie und Techniken zur Förderung eines sicherheitsbewussten Handelns. Sie erfahren, wie Sie Security Awareness-Programme in die Unternehmensstrategie integrieren und den Erfolg anhand messbarer KPIs überwachen, um Ergebnisse der Geschäftsleitung zu präsentieren. Zudem lernen Sie, menschenzentrierte Sicherheitskonzepte zu gestalten und technologische Entwicklungen im Bereich Cybersicherheit zu berücksichtigen.

INHALT

- Erstellung eines Security Awareness-Konzepts und einer Ausbildungsplanung zugeschnitten auf Ihr Unternehmen anhand einer Vorlage
- Planung von Sensibilisierungsmassnahmen
- Trends und aktuelle Bedrohungen im Bereich der Cybersicherheit
- Kennen von Faktoren für den Erfolg
- Überblick über Tools und Hilfsmittel, Techniken und Methoden zur Steigerung des Sicherheitsbewusstseins
- Verstehen, wie Menschen Entscheidungen treffen und Ihr Verhalten positiv beeinflusst werden kann
- Human-Centered Security
- Messung und Erfolgskontrolle
- Üben von Argumentation gegenüber GL

ZIELGRUPPE

Security Awareness Manager, CISO, IT-Sicherheitsbeauftragte, HR-Fachkräfte und Compliance-Verantwortliche, die eine sicherheitsbewusste Kultur etablieren möchten, um regulatorische Anforderungen (z.B. DSGVO / DSGVO / ISO 27001) und interne Sicherheitsstandards zu erfüllen.

TERMINE/ORTE

15.06.2026 - 17.06.2026 Digital*
26.10.2026 - 28.10.2026 Sursee

KOSTEN

CHF 3050.– (exkl. MwSt.)

Weitere Infos und Buchung: [infosec.ch/is17](https://www.infosec.ch/is17)



Business Continuity Manager (BCM) Krisenmanager (KM)

Lernen Sie die Aufgaben eines Ausnahmekönners

 5 Tage

 max. 12 Personen

MEISTERN SIE AUSNAHMESITUATIONEN

Business Continuity Manager und Krisenmanager haben die Aufgabe, als Ausnahmekönner Ausnahmesituationen in der Unternehmung zu meistern. Sie müssen die unternehmenskritischen Produkte, Dienstleistungen oder Prozesse mittels Business Continuity-Plänen und Krisenmanagement unter allen Umständen aufrechterhalten.

ZIEL

Die Teilnehmenden sind nach erfolgreichem Abschluss dieses Lehrgangs in der Lage, ihrem Management ein für ihr Unternehmen spezifisches, wirtschaftlich sinnvolles Business Continuity Management-System als Konzept zu präsentieren. Mit dem erlernten Fachwissen, den Methoden und den Techniken sind sie in der Lage, dieses Managementsystem im Einzelnen zu definieren, aufzubauen und zu betreiben. Nach diesem Lehrgang kennen die Teilnehmenden alles Wichtige über den ISO-Standard 22301.

Die Lehrgangsteilnehmenden können die vielfältigen Abhängigkeiten zwischen den Ressourcen IT, Infrastruktur, Menschen, Dienstleistungen Dritter und den Business-Prozessen respektive Produkten und Dienstleistungen erkennen und

instrumentalisieren. Im Weiteren werden die Zusammenhänge zwischen Business Continuity Management, Krisenmanagement, Risk Management und Integrale Sicherheitsmanagement mit seinen organisatorischen, physischen, technischen und personellen Aspekten verständlich und praxisorientiert dargelegt.

METHODIK

Die gute Mischung aus fundiertem Hintergrundwissen und praxiserprobten Umsetzungsbeispielen macht den Lehrgang nicht nur zu einer spannenden Angelegenheit, sondern sorgt explizit dafür, dass die Teilnehmenden als kompetente Ansprechpersonen in aussergewöhnlichen Situationen erfolgreich bestehen können.

Business Continuity Manager (BCM) Krisenmanager (KM)

Lernen Sie die Aufgaben eines Ausnahmekönners

🕒 5 Tage

👥 max. 12 Personen

INHALT

- Business Continuity Management System (BCMS): Inhalte, kontinuierlicher Verbesserungsprozess, Konzipierung, Aufbau, Betrieb, Management-Tools
- BCM Policy, Fachkonzepte, Weisungen, Regelwerk
- BCM-Organisation, BCM-Kultur, BCM-Prozess
- Definition der relevanten Szenarien
- Business Impact-Analyse (BIA): Methoden, Techniken
- Service Impact-Analysen bei Dienstleistungen der IT, Infrastruktur, Human Resources und Dritter
- Risk Management, Risk Analysis, Risk Treatment, Risk Treatment Planning
- BC-Strategie: Entwicklung strategischer Massnahmen
- Service-Strategien in den Bereichen IT, Infrastruktur, HR, Dritte
- BC-Planning: Entwicklung, Umsetzung, technisch-organisatorische Testverfahren, Training, Überprüfung der Pläne
- BC-Dokumentation
- BC-Kultur: Ausbildung, Sensibilisierung, eLearning
- Krisenmanagement: ein besonderer Business Continuity Plan
- Führungssystem in Krisen: Prozess (Führungsrhythmus), Organisation (Funktionen), Logistik
- Szenariotechnik: nach-, mit-, vorausdenken
- Aussage – Erkenntnis – Konsequenz
- Kommunikation in Krisen
- Krisenstabsübungen: Formen, Konzipierung, Durchführung als Training oder Überprüfung, Auswertung
- Integration in bestehende Managementsysteme und Prozesse, ISO 22301




ZIELGRUPPE

Der Lehrgang richtet sich an Fachpersonen (Sicherheit, Qualität, Risiko) und insbesondere an angehende Business Continuity Manager, Service Continuity Manager (IT, Infrastruktur, HR, Drittdienstleister), Business Continuity-Planer, Krisenmanager und Mitglieder des Krisenstabs.



Business Continuity Manager (BCM) Krisenmanager (KM)

Lernen Sie die Aufgaben eines Ausnahmekönners

 5 Tage

 max. 12 Personen

TERMINE/ORTE

24.08.2026 - 28.08.2026 Digital*

16.11.2026 - 20.11.2026 Sursee

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/bc01

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.

Stärken Sie das Vertrauen Ihrer Geschäftspartner, indem Sie einen Business Continuity Manager oder Krisenmanager kompetent bei uns ausbilden und so die Geschäftskontinuität Ihres Unternehmens sicherstellen.



«Uns wurde nicht nur Theorie vermittelt, sondern auch eine Methoden- und Toolbox inklusive Vorlagen und Praxisübungen mitgegeben, die man als Anwender direkt einsetzen kann.»

*Stefan Rusch, Head of Operations Support,
Reichle & De-Massari AG*

Guter Mix von Teilnehmern aus unterschiedlichen Branchen. So kann man sich über verschiedene Ansichten austauschen. Mit der Praxisübung am 5. Tag kam der Stein ins Rollen, denn Übungen sind sehr wichtig, um das Zusammenspiel zu verstehen.

*Remo Blättler, Leiter Systemtechnik,
Gemeindeverband ICT*

«Es war eine sehr lehrreiche und intensive Woche. Trotz viel eigener Praxiserfahrung konnte ich einiges an Fachwissen auffrischen und ergänzen. Dieser Lehrgang hat mir neue Perspektiven eröffnet, die für das Verständnis und die Umsetzung sehr hilfreich sind.»

*Guido Zauta, Arbeitssicherheit und Gesundheitsschutz,
Meier Tobler AG*



Evakuations

Grundlagen für die Umsetzung von Evakuationsinstruktionen

🕒 1 Tag

👥 max. 12 Personen

EVAKUATIONSSINSTRUKTIONEN SINNVOLL VORBEREITEN UND DURCHFÜHREN

In diesem Kurs lernen Sie, wie Sie ein Evakuationskonzept erstellen und wie Sie die Aus- und Weiterbildung zum Thema «Evakuation» sinnvoll und zielführend planen und durchführen können. Praktische Übungen veranschaulichen das theoretische Wissen, so dass Sie die erworbenen Grundlagen rasch an Ihre Gegebenheiten vor Ort anpassen können und erste Ausbildungen durchführen können.

INHALT

- Arbeitssicherheit und Gesundheitsschutz
- Rechtliche Anforderungen
- Nahtstellen zum Notfall- und Krisenmanagement
- Potentielle Gefahren: Brand, Rauch, Naturkatastrophen, Explosionsgefahr in der Umgebung, Geiselnahmen, Amoklauf, Bombendrohungen
- Arten von Evakuationen
- Richtiges Verhalten
- Bauliche Voraussetzungen für die Durchführung von Evakuationen (VKF15)
- Evakuationsorganisation
- Alarmierungsarten, abgestimmt auf die verschiedenen Gefahren
- Weitere Inhalte online: infosec.ch/pi01

ZIELGRUPPE

Chief Security Officer, Facility Manager, Beauftragte physische Sicherheit, Personalbeauftragte, Beauftragte für Arbeitssicherheit und Gesundheitsschutz, Ausbildungsverantwortliche, Themeninteressierte

TERMIN/ORT

12.05.2026 Digital*
08.09.2026 Sursee

KOSTEN

CHF 1050.– (exkl. MwSt.)

FIRMENSCHULUNG

Diese Ausbildung kann auch als firmeninterne Schulung bei Ihnen vor Ort durchgeführt werden.

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.



Cloud- und IT Security-Manager

Sichere und konforme Bereitstellung von IT Services on-premise oder in der Cloud

🕒 5 Tage

👥 max. 12 Personen

NEUE HERAUSFORDERUNGEN FÜR IT UND COMPLIANCE

Cloud-Technologien, Microsoft 365 und vielfältige Betriebsmodelle verändern die Anforderungen an IT- und Informationssicherheit grundlegend. IT-, Sicherheits- und Compliance-Verantwortliche stehen vor neuen Herausforderungen in Sicherheitsarchitektur, Datenschutz, Governance und regulatorischer Absicherung – sowohl technisch als auch organisatorisch.

Im Spannungsfeld zwischen Technologie, Organisation und Recht wächst der Bedarf an spezialisierten Fachkräften, die diese komplexen Anforderungen kompetent adressieren können.

ZIEL

Sie erhalten in diesem Lehrgang praxisnahes Wissen zu den technischen, organisatorischen und rechtlichen Massnahmen, welches Sie für eine sichere und konforme Bereitstellung von IT Services on-premise oder aus der Cloud in Ihrer Organisation anwenden können.

INHALT

- IT-Sicherheitsprozesse und -konzepte und deren Anwendung in modernen IT-Infrastrukturen, darunter Identity and Access Management, Encryption, Vulnerability Management, Cloud Security Posture Management (CSPM), Backup and Restore, Recovery and Redundancy, Third Party Risk Management (TPRM), Secure Software Development Concepts etc.
- Security und Data Protection beim Einsatz von Microsoft 365, darunter Sicherheits- und datenschutzbezogene Analysen von Defender for Endpoint, Defender for O365, Intune, SharePoint Online, Exchange Online, Teams und Entra ID
- Sicherheitsarchitektur und -konzepte bei Microsoft Azure und anderen Hyperscalern
- Überblick über die relevanten Standards, Normen und Best Practices im IT- bzw. Cloud Security Management
- Informationssicherheitsmanagement gemäss ISO 27001, mit cloud-spezifischer Vertiefung nach ISO 27017 und ISO 27018
- Information und IT Governance

Cloud- und IT Security-Manager

Sichere und konforme Bereitstellung von IT Services on-premise oder aus der Cloud

🕒 5 Tage

👥 max. 12 Personen

- Security Incident Response
- Business Continuity Management (BCM) und Disaster Recovery (DR)
- Datenschutz nach DSGVO und DSGVO
- Best Practices im Umgang mit Cloud-spezifischen Risiken wie Cloud Exit, Vendor Lock-in, Datenstandort und -hoheit, Datenschutz, Shared Responsibility, Cloud Security Posture, etc.
- Fallbeispiele und Vorgehenskonzepte aus der und für die Praxis

ZIELGRUPPE

CIO, IT-Leiter, IT-Sicherheitsarchitekten, CISO, Security Officer, Sicherheitsbeauftragte, Informationssicherheitsbeauftragte (ISB), Datenschutzbeauftragte, Data Protection Officers (DPO), Zuständige für Legal und Compliance, Risikomanager, Business Unit-Leiter, Projektleiter, Themeninteressierte.

TERMINE/ORTE

22.06.2026 - 26.06.2026 Sursee

14.09.2026 - 18.09.2026 Sursee

09.11.2026 - 13.11.2026 Sursee

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/it01

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.

FIRMENSCHULUNG

Dieser Lehrgang kann auch als firmeninterne Ausbildung bei Ihnen vor Ort durchgeführt werden.

Sie lernen technische, organisatorische und rechtliche Massnahmen kennen, die für eine sichere Erbringung von IT Services on-premise oder aus der Cloud benötigt werden.





NEU! Microsoft Cloud Security & Compliance Specialist

Überblick über Security und Datenschutz in der Microsoft Cloud

🕒 3 Tage

👥 max. 12 Personen

SECURITY & COMPLIANCE IN DER MICROSOFT CLOUD MEISTERN

Mit Microsoft Cloud Services wie Microsoft 365, Azure und Microsoft Entra stehen Verantwortliche vor der Herausforderung, in einer stetig wandelnden Umgebung den Überblick nicht zu verlieren. Es gilt, über die aktuellen Fähigkeiten, Herausforderungen und Konzepte der Microsoft Cloud Bescheid zu wissen, um den Sicherheitsanforderungen der eigenen Organisation und den Vorgaben von regulatorischen Behörden angemessen entsprechen zu können.

ZIEL

Sie erwerben praxisbewährtes Fachwissen, um als Microsoft Cloud Security und Compliance-Spezialist Unternehmen sicher und regelkonform beim Einsatz von Microsofts Cloud Services anzuleiten. Sie erhalten einen Überblick über den derzeitigen Stand der Technik beim Einsatz von Microsoft 365 und Microsoft Azure bezüglich Security und Datenschutz.

INHALT

- Microsoft Cloud-Architektur
- Identity & Access Management
- Security Operations und Incident Response
- Sichere und datenschutzkonforme Konfiguration
- Rechtliche Aspekte, Compliance
- Detaillierte Inhalte, weitere Infos und Buchung online: infosec.ch/it08

ZIELGRUPPE

CIO, IT-Leiter, IT-Sicherheitsarchitekten, CISO, Security Officer, Sicherheitsbeauftragte, Informationssicherheitsbeauftragte (ISB), Security und System Engineers, System Admins, Datenschutzbeauftragte, Data Protection Officers (DPO), Zuständige für Legal und Compliance, Themeninteressierte.

TERMINE/ORT

08.06.2026 - 10.06.2026 Digital*
05.10.2026 - 07.10.2026 Sursee
16.11.2026 - 18.11.2026 Digital*

KOSTEN

CHF 3050.– (exkl. MwSt.)

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat.



Mandat: Externer Cybersecurity Officer (CSO) / IT Security Officer (ISO)

Überlassen Sie Cybersecurity nicht dem Zufall, sondern unseren Spezialisten

Der externe Cybersecurity Officer / IT Security Officer übernimmt zum Beispiel folgende Aufgaben:

- Ansprechstelle und Fachberatung der Informatikmitarbeitenden und der Informatikführung
- Mitarbeit im Daily Business
- Interdisziplinäre Zusammenarbeit mit internen Stellen wie CISO, Risikomanagement, Datenschutz, Compliance / Legal
- Beurteilung der Sicherheit in Projekten, in Change-Prozessen oder im Ausnahmenmanagement
- Entwicklung von Sicherheitsspezifikationen, beispielsweise für Applikationen und Systeme oder bei Evaluationen
- Erarbeitung und Prüfung von Sicherheitskonzepten
- Ausarbeitung und Unterstützung bei der Umsetzung und Prüfung von IT-Sicherheitsmassnahmen; Überwachung der Massnahmen, Aufbau eines Internen Kontrollsystems (IKS)
- Weitere Aufgaben online ersichtlich: www.infosec.ch/mandat-cso

Kontaktieren Sie uns für ein konkretes Angebot oder für ein persönliches und unverbindliches Erstgespräch. +41 41 984 12 12, infosec@infosec.ch



Prüfungsvorbereitung CISSP

Prüfungsvorbereitung zum ISC2 Certified Information Systems Security Professional®

🕒 5 Tage

👥 max. 12 Personen

CISSP®-ZERTIFIZIERUNG DANK SERIÖSER VORBEREITUNG BEI UNS

Werden Sie mit dem CISSP® zum Top-Experten der Cybersecurity. Sie beweisen tiefes technisches und strategisches Know-how, um Unternehmen ganzheitlich zu schützen. Profitieren Sie vom weltweiten Goldstandard der Cybersecurity und sichern Sie sich Ihren Karrierevorsprung.

INHALT

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communications and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security
- Weitere Inhalte online: infosec.ch/it02

ZIELGRUPPE

Fach- und Führungspersonen wie z. B. CISOs, CIOs, IT-Manager, sowie Sicherheitsberater, Security- oder Network-Architekten, Security Systems Engineers, Security Consultants, Analysten, Manager, Auditoren oder Entwickler.

TEILNAHMEVORAUSSETZUNG

Know-how in der Informationssicherheit / Cybersecurity und Erfahrung im Bereich Telekom-

munikation und Netzwerke sind von Vorteil. Gute Englischkenntnisse sind Bedingung.

ANFORDERUNGEN UM DAS CISSP®-ZERTIFIKAT ZU ERHALTEN

Sie benötigen mindestens fünf Jahre einschlägige Berufserfahrung in Vollzeit. Diese Erfahrung muss mindestens zwei der acht Domains des CISSP® Exam Outlines abdecken.

TERMINE/ORTE

29.06.2026 - 03.07.2026 tbd / Hybrid

14.09.2026 - 18.09.2026 tbd / Hybrid

23.11.2026 - 27.11.2026 tbd / Hybrid

KOSTEN

CHF 5900.– (exkl. MwSt.), exkl. Mittagessen, inkl. Literatur, inkl. Prüfungsvoucher



Ethical Hacking

Angriffstechniken auf Netzwerk-, System- und Applikationsebene, inkl. Webapplikationen

 5 Tage

 max. 10 Personen

DAS VORGEHEN VON ANGREIFERN VERSTEHEN LERNEN

Lernen Sie, wie sich Angreifer Zugang zu Netzwerken verschaffen, wie sie sich darin bewegen und welche Techniken sowie Werkzeuge sie verwenden. Sie üben dies aus Sicht eines Angreifers in einer Lab-Umgebung und sind danach in der Lage, Netzwerke, Betriebssysteme und Webapplikationen auf Schwachstellen zu überprüfen und diese gemäss aktuellen Standards und Best Practices zu schützen.

INHALT

- Passive Information Gathering
- Host- und Service Discovery
- Network Sniffing
- Vulnerability Scanning
- Exploitation
- Erstellung von Payloads
- Privilege Escalation
- Laterale Bewegung
- Man-in-the-Middle-Angriffe
- Command & Control Frameworks
- Web Application Security, insbesondere OWASP Top 10
- Rapportieren von Schwachstellen

TEILNAHMEVORAUSSETZUNG

Technische Grundkenntnisse in den Bereichen Netzwerktechnologie, Computer- und Systemtechnik, Applikationsentwicklung und Programmcode.

ZIELGRUPPE

Netzwerk- und Systemadministratoren, Verantwortliche für Applikationen, Firewalls und Active Directory, Softwareentwickler, Softwaretester, (angehende) Penetration Tester und Security Engineers, Security Analysts.

TERMIN/ORT

19.10.2026 - 23.10.2026 Digital*

Weitere Infos und Buchung: infosec.ch/it03

KOSTEN

CHF 4950.– (exkl. MwSt.)

LEGAL DISCLAIMER

Die Teilnehmenden verpflichten sich, das vermittelte Wissen nicht für illegale Zwecke zu nutzen. Sollte ein Teilnehmender dies dennoch tun, trägt dieser dafür die Verantwortung.



Secure Coding

Grundwissen und Best Practice bzgl. Sicherheit beim Entwickeln und Ausrollen von Software

 4 Tage

 max. 10 Personen

SECURING SOFTWARE DEVELOPMENT AND OPERATIONS (DEVSECOPS)

Sie werden dazu befähigt, Schwachstellen von Software identifizieren zu können, deren Auswirkungen zu kennen sowie Massnahmen zu deren Behebung umzusetzen. Es wird ausserdem erläutert, wie sichere Entwicklungsmethoden in agile oder auch klassische Softwareentwicklung einfließen können. Sie üben das Gelernte anhand von praktischen Aufgaben auf einer Online-Lernplattform.

INHALT

- Secure Software Development Lifecycles
- Threat Modeling
- Datenschutzkonforme Software
- Kennenlernen der essenziellen OWASP-Ressourcen
- Security Scanning von IaC Templates
- Vertiefung OWASP Top 10 anhand von Übungen und Code Snippets
- Statische und dynamische Code-Analysen
- Exception Management
- Code Signing
- Zertifikatserstellung und -management
- Sichere Verwendung von Applikationsplattformen in der Cloud

TEILNAHMEVORAUSSETZUNG

Erfahrung in Softwareentwicklung oder Grundverständnis, um Code lesen und verstehen zu können.

ZIELGRUPPE

Softwareentwickler, Softwaretester, Applikationsverantwortliche, Applikationsspezialisten, Verantwortliche in den Bereichen Softwareentwicklung und -Testing, Themeninteressierte.

TERMIN/ORT

27.10.2026 - 30.10.2026 Digital*

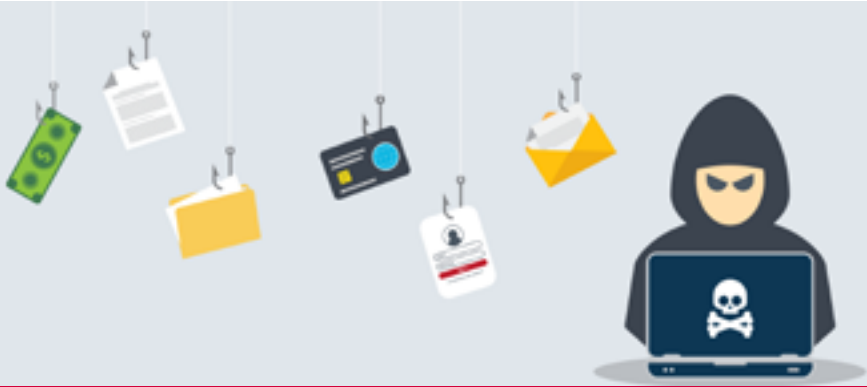
Weitere Infos und Buchung: infosec.ch/it04

KOSTEN

CHF 4150.– (exkl. MwSt.)

FIRMENSCHULUNG

Diese Ausbildung kann auch als firmeninterne Schulung bei Ihnen durchgeführt werden.



Awareness

Mitarbeitersensibilisierung – aber richtig

Mehr als 99% aller Cyberangriffe sind auf menschliches Fehlverhalten zurückzuführen. Deshalb ist es besonders wichtig, Ihre Mitarbeitenden für das Thema Sicherheit zu sensibilisieren. Motivieren Sie Ihre Belegschaft mit gezielten Massnahmen zu sicherem Handeln.

Wir unterstützen Sie mit folgenden individuell anpassbaren Serviceangeboten:

- Awareness Manager as a Service
- Awareness-Plattformen
- eLearning-Module
- Phishing-Simulationen per E-Mail, Telefon, Deepfakes
- Awareness Assessments
- Security Edutainments, Referate, Keynotes
- Social Engineering, Dumpster Diving, USB-Stick-Angriff
- Beiträge, Plakate und Publikationen

Awareness als Abo

Damit erhalten Sie regelmässig auf Ihr Unternehmen oder einzelne Teams zugeschnittene Mitteilungen, Beiträge für Newsletter, Blog, Intranet oder Plakate für den Aushang. Auf Wunsch können wir auch Phishing-Attacken simulieren, um die Awareness Ihrer Mitarbeitenden zu testen.

Neugierig? Wir freuen uns auf Ihre Anfrage: +41 41 984 12 12, infosec@infosec.ch
www.infosec.ch/awareness



Risikomanager

Mit SAQ-QUALICON-Zertifikat «Risikomanager»

 4 Tage (2 x 2 Tage)

 max. 16 Personen

RISIKEN ABSCHÄTZEN UND MÖGLICHE SCHÄDEN VERMINDERN

Sie lernen, wie ein professionelles Risikomanagementsystem (RMS) zum Erreichen der geschäftspolitischen Ziele beiträgt. Neben gesetzlichen und normativen Anforderungen geht es um die zeitgemässe Risikowahrnehmung, -ermittlung, -bewertung und -handhabung bis hin zum Umgang mit Restrisiken im Rahmen des Business Continuity Managements (BCM).

INHALT

- Normative Grundlagen (ISO 31000, ISO 22313)
- Risikomanagementeinbettung in die Organisation: Risikopolitik, -strategie und -toleranz
- Risikomanagementprozess und Schnittstellen
- Risikobeurteilung, Risikosteuerung, Risiküberwachung und Risikoberichterstattung
- Grundlagen Business Continuity Management (BCM) inkl. Notfall- und Krisenmanagement

Als Leistungsnachweis erarbeiten Sie eine Transferarbeit im Umfang von ca. 15 Seiten. Darin wenden Sie Analysen und Modelle aus dem Unterricht auf Ihr eigenes Unternehmen an, entwickeln Lösungsansätze und reflektieren Ihre Erkenntnisse.

ZIELGRUPPE

Geschäftsführer und Führungskräfte von KMUs, Risk-, Compliance- und IKS-Verantwortliche, interne oder externe Revisoren sowie Qualitätsbeauftragte, die ihre Fachkompetenz zur Ausgestaltung oder Optimierung des Risikomanagements vertiefen möchten.

TERMINE/ORT

06. - 07.05.2026 und 20. - 21.05.2026 Olten
19. - 20.10.2026 und 02. - 03.11.2026 Olten

KOSTEN

CHF 2590.– (exkl. MwSt.)

Detaillierte Terminübersicht, weitere Infos und Buchung: infosec.ch/ri02



Mandat Chief Information Security Officer (CISO)

Konsequente Informationssicherheit ist ein Muss, scheitert aber oft an fehlenden Personalressourcen und/oder mangelndem Spezial-Know-how. Mit einem externen Chief Information Security Officer der Swiss Infosec AG lösen Sie dieses Dilemma elegant und nachhaltig.

Der Einsatz des externen CISO richtet sich ganz nach Ihren Bedürfnissen. Ob als temporäre Unterstützung als Projektleiter, als Übergangslösung bei aktuellem Personalengpass oder fixe Grösse über einen längeren Zeitraum: Sie können auf uns zählen.

Auszug aus den Aufgaben:

- Ansprechstelle und Fachberatung von Management und Mitarbeitenden
- Operativer Betrieb des Informationssicherheitsmanagements
- Mitarbeit im Daily Business
- Konzeption, Vorbereitung und Durchführung von Ausbildungs-, Sensibilisierungs- und Kommunikationsmassnahmen
- Erarbeitung von Information Security-Vorgaben (Policy, Guidelines, etc.)
- Unterstützung bei der Umsetzung von Massnahmen; Tracking der Massnahmen
- Führung, Überwachung und kontinuierliche Verbesserung der Sicherheitsprozesse
- u.v.m.

Kontaktieren Sie uns für ein persönliches und unverbindliches Erstgespräch.

+41 41 984 12 12, infosec@infosec.ch

www.infosec.ch/mandat-ciso (PDF)

www.infosec.ch/mandate



ISO 27001 Lead Auditor

IRCA-zertifizierter Lehrgang

 5 Tage

 max. 10 Personen

WISSEN UND KNOW-HOW ZU ISO 27001

Dieser Lehrgang führt Sie umfassend in das Auditing bezüglich ISO 27001 und ISO 27002 ein. Am Ende des Lehrganges erfolgt die Zertifizierung als ISO 27001 Lead Auditor. Dies ist ein IRCA-zertifizierter Lehrgang.

ZIEL

Werden Sie mit unserer ISO 27001 Lead Auditor-Schulung eine qualifizierte und vom International Register of Certified Auditors (IRCA) anerkannte ISMS-Führungskraft. Sie werden von Experten für die ISO 27001 geschult und erlangen die Qualifikation, ISMS-Audits bis zur höchsten Stufe durchzuführen. Dieser Lehrgang wird Ihnen helfen, jede Phase des Zertifizierungs- und Auditprozesses zu verstehen. Als ein qualifizierter ISO 27001 Lead Auditor unterstützen Sie alle, die für Risk & Compliance arbeiten und leisten qualifizierte Unterstützung bei der Durchführung von Audits. In fünf Tagen werden nicht nur die wesentlichen Grundlagen der Informationssicherheit behandelt, sondern auch übergeordnete Aspekte wie Organisation, Technik oder Prozessmanagement. Die Teilnehmenden können interne und externe Audits planen.

INHALT

- Informationssicherheit
- Die Bedeutung der Informationssicherheit
- Einschätzung von Schwachstellen und Sicherheitsrisiken
- Management von Sicherheitsrisiken
- Auswahl von Kontrollmechanismen
- Erstellen eines Managementsystems zur Informationssicherheit (ISMS)
- Einleitung und Durchführung eines Audits
- Methoden für ISO 27001 Auditing
- Führen/Leiten eines ISO 27001 Audit Teams
- Befragungsstrategien
- Probeprüfung, Hausaufgaben
- Erstellen eines Audit-Berichts
- Abschlussprüfung (Lehrgangsende Freitag, ca. 13.00 Uhr)



ISO 27001 Lead Auditor

IRCA-zertifizierter Lehrgang

 5 Tage

 max. 10 Personen

TEILNAHMEVORAUSSETZUNG

Besuch des Kurses «Einführung ISO 27001, ISO 27002» oder Besuch des Kurses «ISO 27001 Manager» oder Nachweis der entsprechenden Praxis.

TERMINE/ORTE

04.05.2026 - 08.05.2026 Thalwil
10.08.2026 - 14.08.2026 Sursee
23.11.2026 - 27.11.2026 Sursee

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/io01

ZERTIFIKAT

Nach erfolgter Absolvierung erhält jeder Teilnehmende ein entsprechendes Zertifikat. Nach Bestehen der Prüfung können Sie sich im IRCA «International Register of Certified Auditors» registrieren lassen. www.irca.org

IRCA-SPEZIFIKATIONEN

Training Organization: BSI Training
Identification number: A17287

ABMELDUNG ODER VERSCHIEBUNG

Entgegen unserer Geschäftsbedingungen können wir bei diesem Lehrgang eine Abmeldung oder Verschiebung nicht akzeptieren, jedoch einen Ersatzteilnehmenden.



ZIELGRUPPE

Praktizierende interne oder externe Auditoren, Fachleute, die im Bereich IT- und Qualitätsmanagement arbeiten und im Bereich von ISO 27001-Zertifizierungen tätig werden möchten resp. ein formales Informationssicherheitsmanagement nach ISO 27001 einführen wollen.


Sie stellen alle Aspekte in den Mittelpunkt, die Vertraulichkeit, Verfügbarkeit und Integrität von allen Informationen in Ihrem Unternehmen sicherstellen. Sie untersuchen und bewerten die dazu benötigten Prozesse hinsichtlich deren Erfüllung.






ISO 27001 Manager

Kurs für beauftragte ISO 27001 Manager

 3 Tage

 max. 12 Personen

GRUNDLAGEN UND PROZESSE

In nur 3 Tagen erlangen Sie das wichtigste Wissen, um ein Informationssicherheitsmanagementsystem (kurz: ISMS) nach ISO 27001 aufbauen, betreiben und kontinuierlich verbessern zu können. Dabei bilden die 52 MUSS-Ziele der Norm mit den beiden wichtigsten Prozessen Risikomanagement und kontinuierliche Verbesserung den Schwerpunkt. Mittels systematischen Vorgehens erlangen Sie als Fachexperte die Kompetenz, in Ihrem Unternehmen den Ist-Stand zu eruieren, einen Plan für den sukzessiven Aufbau eines ISMS zu entwerfen und das Wesentliche hinsichtlich einer möglichen Zertifizierung zu erkennen.

ZIEL

Als beauftragter ISO 27001 Manager lernen Sie, wie Sie in Ihrem Unternehmen ein eigenes Informationssicherheitsmanagementsystem systematisch aufbauen, betreiben und kontinuierlich erfolgreich verbessern.

Verbesserungsprozesses (Plan-Do-Check-Act) im Bereich der Informationssicherheit

- Vorlagen für die erforderlichen Dokumentation
- Praxisorientierte Tipps zum Betreiben eines Managementsystems

INHALT

- Systematischer Aufbau eines Informationssicherheitsmanagementsystems nach ISO 27001 (Projekteinführungsplan)
- Schaffung von Transparenz und Sicherheit im Umgang mit Informationen
- Konzipierung, Anwendung und Überwachung des Risikomanagement- und des kontinuierlichen


DOKUMENTATION


Den Teilnehmenden werden für die Dauer des Kurses die erforderlichen ISO-Normen ausgehändigt. Diese müssen aus lizenzrechtlichen Gründen nach Kursende wieder retourniert werden.



ISO 27001 Manager

Kurs für beauftragte ISO 27001 Manager

 3 Tage

 max. 12 Personen

TERMINE/ORTE

01.06.2026 - 03.06.2026 Sursee

28.09.2026 - 30.09.2026 Digital*

09.12.2026 - 11.12.2026 Sursee

TEILNAHMEVORAUSSETZUNG

Keine

KOSTEN

CHF 3050.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/io02

ZERTIFIKAT UND AUSZEICHNUNG

Nach erfolgter Absolvierung erhält jeder Teilnehmende seitens Swiss Infosec AG ein Zertifikat.

FIRMENKURS

Dieser Kurs kann auch als Firmenschulung gebucht werden, die auf die spezifischen Anforderungen Ihrer Unternehmung eingeht.



ZIELGRUPPE

Dieser Kurs richtet sich an Personen, die ihr Informationssicherheitsmanagementsystem ISMS nach ISO 27001 aufbauen, betreiben und kontinuierlich verbessern wollen. Auch für die Vorbereitung auf eine ISO 27001-Zertifizierung eignet sich der Kurs bestens.

Sie lernen, wie man Informationssicherheitsrisiken abschätzt und senkt. Und Sie lernen die Grundlagen für die Einrichtung Ihres eigenen Informationssicherheitsmanagementsystems kennen.






NEU! ISO 42001 Lead Auditor

Einführung in das Auditing bezüglich der ISO-Norm 42001, inkl. Zertifizierung

 5 Tage

 max. 12 Personen

WISSEN UND KNOW-HOW MIT BSI-TRAINING

Dieser Lehrgang führt Sie in das effektive Auditing eines Artificial Intelligence Management Systems (AIMS) ein. Nach erfolgreichem Abschluss erhalten Sie ein international anerkanntes BSI-Zertifikat.

INHALT

- Artificial Intelligence, Terminologie, PDCA-Kreislauf
- Audits von Erst-, Zweit- und Drittparteien
- Auditprozess (Auditziele, -umfang und -kriterien, Auditressourcen, Auditmethoden)
- Rollen und Verantwortlichkeiten
- Auditplan
- Zweck und Vorteile für die Organisation
- Die Rolle des Prüfers
- AIMS-Kontext der Organisation, AIMS-Dokumentation
- Management Review (Audit des obersten Managements)
- Risikobehandlungspläne der Organisation
- Prozess der Folgenabschätzung der AI/KI-Systeme
- Prozess der Auditvorbereitung, -durchführung und -nachbereitung
- Nicht-Konformitäten
- Erstellen eines Auditberichts
- Hausaufgaben
- Abschlussprüfung

ZIELGRUPPE

Sicherheits- und Qualitätsfachleute, bestehende Informationssicherheitsauditoren, Beraterinnen und Berater, die Beratung zu ISO 42001 AIMS-Audits anbieten möchten etc.

TEILNAHMEVORAUSSETZUNG

Gute Kenntnisse der ISO 42001 und der wichtigsten Grundsätze eines AIMS sind erforderlich.

TERMIN/ORT

07.09.2026 - 11.09.2026 Sursee

KOSTEN

CHF 4950.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/io09

ZERTIFIKAT

Nach erfolgreichem Abschluss erhalten Sie ein international anerkanntes BSI-Zertifikat.



Aufbau ISMS nach ISO 27001

Mit der Erfahrung der Swiss Infosec AG erfolgreich ans Ziel kommen

Schaffen Sie Transparenz und Sicherheit im Umgang mit Ihren Informationen und Daten durch die Erreichung der Zertifizierbarkeit oder die Zertifizierung gemäss ISO 27001. Planen und setzen Sie Ihr Vorhaben mit Spezialisten ihres Fachs um: mit uns, der Swiss Infosec AG.

Unser Coaching- und Consulting-Service lässt keine Wünsche offen. Wir unterstützen Ihre Projektorganisation, übernehmen auf Wunsch auch die Projektleitung oder wachen bei Ihnen vor Ort als externer Mitarbeiter auf Mandatsbasis. Wir schärfen Ihren Blick fürs Notwendige und finden Lösungen, die auf Ihr Unternehmen zugeschnitten sind und passen.

Unser ISO 27001-Angebot führt auch Sie effizient und konsequent zum Ziel.

Kontaktieren Sie uns, wir beantworten gerne Ihre Fragen.

+41 41 984 12 12, infosec@infosec.ch

www.infosec.ch/angebot-isms (PDF)

www.infosec.ch/projektsupport

www.infosec.ch/mandate

Workshop zum Schweizer Datenschutzgesetz (DSG)

Datenschutzlücken? Unsere Experten liefern Antworten und Empfehlungen

 1/2 Tag

 2 bis 4 Personen

SCHWEIZER DATENSCHUTZGESETZ (DSG)

Das Schweizer Datenschutzgesetz (DSG) ist nahe an den Vorgaben der Europäischen Union, enthält verschiedene Governance-Pflichten und Bussenregelungen und beschreibt die Aufsichtskompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Nach diesem Workshop haben Sie DSG-Anforderungen wie u.a. die Informationspflichten (Datenschutzerklärung) etc. besser im Griff.

Vor dem Workshop erhalten Sie eine Checkliste für eine Standortanalyse. Die Resultate helfen es dabei, im Workshop auf Ihre individuellen Bedürfnisse einzugehen und auf Sie zugeschnittene Arbeitspakete zu schnüren.

ZIEL

Sie werden über mögliche Datenschutzlücken aufgeklärt, finden angemessene Umsetzungslösungen und sind damit DSG-konform.

INHALT

- Überblick über das Schweizer Datenschutzgesetz (DSG)
- Governance-Pflichten
- Bussen
- Organisation des Datenschutzes in Ihrer Organisation
- Empfehlungen zur Umsetzung
- Konkrete Umsetzungsplanung

ZIELGRUPPE

Geschäftsleitung, Management, Sicherheitsbeauftragte, Compliance, Rechtsdienst/Legal, Programmierer, Systembetreiber, HR, Marketing, Mitarbeitende aller Stufen.

TERMIN/ORT

Individuelle Vereinbarung

TEILNEHMERZAHL

Sie bestimmen, wer seitens Ihres Unternehmens, Ihrer Organisation oder Behörde teilnimmt. In der Regel sind es zwischen zwei und vier Personen.

Weitere Infos und Buchung: infosec.ch/ds12


KOSTEN


CHF 2400.– (exkl. MwSt.)



NEU! Workshop Medizin und Datenschutz

Für einen aktuellen und praxisorientierten Umgang mit Gesundheitsdaten

 1/2 Tag oder 1 Tag

 2 bis 15 Personen

PATIENTENDATEN SICHER MANAGEN

In diesem Workshop vermitteln wir Ihren Mitarbeitenden die Grundlagen aus den einschlägigen Datenschutzgesetzen für einen aktuellen und praxisorientierten Umgang mit Gesundheitsdaten..

Durchgeführt wird der Workshop von unseren Datenschutzberatern und -experten, die in Spitälern, Betreuungs- und Pflegeeinrichtungen, Medtech-Unternehmen und medizinischer Forschung tätig sind.

INHALT

- Anwendbares Recht (DSG, kantonale Datenschutzgesetze, etc.)
- Einwilligung der PatientInnen und Informationspflichten der Institutionen
- Sicherer Umgang mit Patientendaten innerhalb der Institution
- Weitergabe von Patientendaten (z.B. Überweisungen, Besprechungen im Konsil, Daten aus Smart Devices, usw.)
- Auslagerung der Datenspeicherung in Cloud-Lösungen
- Verwendung von KI (Personalplanung, Voice-to-Text, generative KI zur Diagnosestellung od. zum Verfassen von Berichten, etc.)

TEILNAHMEVORAUSSETZUNG

Ideal sind erste Erfahrungen und Grundlagenwissen im Datenschutz.

ZIELGRUPPE

Spitäler, Arztpraxen, Pflegeeinrichtungen, Forschungsinstitutionen, MedTech-Unternehmen etc. Die Teilnahme ist auf Personal aus Medizin, Pflege, Administration, Compliance und IT ausgerichtet.

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.

TEILNEHMERZAHL

In der Regel zwischen zwei und 15 Personen.

KOSTEN

1/2 Tag: CHF 2400.– (exkl. MwSt.)

1 Tag: CHF 3900.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/ds14

Workshop Information Governance

Vorteile dieses ganzheitlichen Ansatzes, um Informationen und digitale Daten zu verwalten

 1/2 Tag

 3 bis 5 Personen

WO BESTEHT IN IHREM UNTERNEHMEN OPTIMIERUNGSPOTENTIAL?

In diesem Workshop erfahren Sie, wie es um die Information Governance in Ihrem Unternehmen bestellt ist, also ob Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit des wertvollen Business Asset «Informationen und Daten» jederzeit sichergestellt sind.

Wir analysieren gemeinsam mit Ihnen die konkrete Situation Ihres Unternehmens und identifizieren Lösungsansätze. Sie erhalten einen kurzen, schriftlichen Bericht mit unseren Handlungsempfehlungen.

INHALT

- Überblick über das «Mindset Information Governance» und dessen Zusammenhänge mit:
 - Corporate Governance, Risk und Compliance
 - Informationssicherheit: Datenschutz, Informationsschutz und IT Security
 - Records Management, u.a. Archivierung, Löschung
- Überprüfung und Diskussion der bestehenden Information Governance bzw. der bestehenden Verwaltung von Daten und Informationen in Ihrer Organisation (Standortbestimmung)
- Empfehlung zur Optimierung der bestehenden Information Governance und/oder Umsetzung neuer Massnahmen innerhalb der Information Governance.

ZIELGRUPPE

Mitglieder der Geschäftsleitung, Compliance Officer, GRC-Funktionen, Leiter IT, Records Management-Funktionen, Datenschutz und Informationssicherheit.

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.

TEILNEHMERZAHL

Sie bestimmen selbst, wer an diesem Workshop teilnimmt. In der Regel sind dies drei bis fünf Personen.

KOSTEN

CHF 3900.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/is13

NEU! Workshop Cybervorfall: Vorbereitung und Incident Response

Praxisnaher Überblick über den Umgang mit Cyberfällen

🕒 1/2 Tag

👥 6 Personen

IST IHRE ORGANISATION BEREIT FÜR DEN ERNSTFALL EINES CYBERANGRIFFS?

Wir analysieren gemeinsam mit Ihnen, wie resilient Ihre Organisation gegenüber möglichen Cyberfällen aufgestellt ist. Sie lernen bewährte Vorgehensweisen in der Abwehr von Cyberangriffen kennen und erhalten konkrete Empfehlungen, wie Sie Ihre technische Infrastruktur, Ihre Abläufe und Verantwortlichkeiten für den Fall eines Cyberangriffs verbessern können.

INHALT

- Überblick über typische Cyberfälle und aktuelle Bedrohungsszenarien
- Durchspielen eines Cyberfalls im Table-Top-Modus
- Überprüfung der Cyberresilienz Ihrer Organisation entlang der Cyber Kill Chain
- Diskussion der essenziellen Massnahmen (präventiv und reaktiv)
- Beurteilung der bestehenden Wiederherstellungsprozesse
- Diskussion IT-technischer Abhängigkeiten von geschäftskritischen Prozessen
- Incident Response und Geschäftskontinuität: Abläufe, Eskalationsstufen, Abhängigkeiten sowie Kommunikation intern und extern, Zusammenarbeit mit externen Partnern und Spezialisten
- Diskussion von Praxisbeispielen und konkreten Fragestellungen
- Zusammenstellung der Lessons Learned und Empfehlungen in einem kurzen Bericht

ZIELGRUPPE

Mitglieder der Geschäftsleitung, IT-Leiter und IT-Verantwortliche, Informationssicherheitsverantwortliche (z. B. CISO, ISB, IT-SIBE), Security Officers und Cybersecurity-Verantwortliche, Verantwortliche für Risiko und Compliance, Krisenmanagement oder Business Continuity

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.


KOSTEN

CHF 3400.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/it09

Workshop IT Security und Datenschutz

Technik und Datenschutz vereint an einem halben Tag

 1/2 Tag

 2 bis 4 Personen

TECHNIK UND DATENSCHUTZ KOMPAKT

Wir analysieren mit Ihnen, wo Sie aktuell bezüglich Abwehr von Cyberangriffen stehen und wie Ihr Unternehmen die Anforderungen des Datenschutzgesetzes erfüllt. Unsere Handlungsempfehlungen zeigen Ihnen, wo und wie Sie Ihre IT-Sicherheitsmassnahmen optimieren, allfällige Datenschutzlücken schliessen und das Datenschutzgesetz angemessen und rechtskonform umsetzen können.

INHALT

- Kennenlernen des Ablaufs und der wichtigen Eigenheiten von Cyberangriffen
- Besprechung relevanter Sicherheitsbereiche zur angemessenen Vorbereitung auf mögliche Angriffe
- Auseinandersetzung mit den Inhalten des Datenschutzgesetzes und den daraus resultierenden Must-haves
- Analyse der bereits ergriffenen und Bestimmung der noch erforderlichen Massnahmen zur sachgerechten und effizienten Umsetzung des Datenschutzgesetzes

TEILNEHMERZAHL

Sie bestimmen selbst, wer seitens Ihres Unternehmens, Ihrer Organisation oder Behörde an diesem Workshop teilnimmt. In der Regel sind dies zwischen zwei und vier Personen.

ZIELGRUPPE

Entscheidungs- und Risikoträger, Sicherheitsverantwortliche und -beauftragte, IT-Leiter, Security Officer, Information Security Officer, IT-Sicherheitsbeauftragte, Datenschutzverantwortliche, Fach- und Führungskräfte mit Datenschutzverantwortung, Datenschutzberater, Projektleiter und Themeninteressierte.

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.

KOSTEN


CHF 3600.– (exkl. MwSt.)


Weitere Infos und Buchung: infosec.ch/it06



NEU! Workshop KI-Sicherheit

Klärung Ihrer Fragen im Zusammenhang mit KI und Sicherheit/Datenschutz

 1/2 Tag

 2 bis 4 Personen

KI-ANWENDUNGEN: ANFORDERUNGEN AN SICHERHEIT UND DATENSCHUTZ

Der KI-Weg ist mit Fragen und Unsicherheiten gepflastert, insbesondere was die Sicherheit und den Datenschutz betrifft. In diesem Workshop erhalten Sie fundierte Antworten und einen Bericht mit konkreten auf Ihr Unternehmen zugeschnittenen Handlungsempfehlungen.

INHALT

- Überblick über das Thema KI mit Fokus Sicherheit und Datenschutz
 - Was KI ausmacht (Datenmenge, Datenzugriff)
 - Was KI für Konsequenzen für die (Informations-)Sicherheit hat
 - Was das Datenschutzgesetz sagt
 - Was das (aktuelle) Fehlen von verbindlichen Rahmenbedingungen für Unternehmen bedeutet
- Blick auf geplante oder bereits bestehende KI-Anwendungen in Ihrem Unternehmen
 - Diskussion über konkrete Fragestellungen in Bezug auf Sicherheit und Datenschutz
 - Handlungsfelder, Möglichkeiten und Stolpersteine
- Empfehlungen für angemessene Massnahmen zur Sicherstellung von Sicherheit und gesetzeskonformem Datenschutz.

TEILNEHMERZAHL

Sie bestimmen selbst, wer seitens Ihres Unternehmens, Ihrer Organisation oder Behörde an diesem Workshop teilnimmt. In der Regel sind dies zwischen drei und fünf Personen.

ZIELGRUPPE

Mitglieder der Geschäftsleitung, Digital (Risk) Officer, Digital Transformation Manager, Leiter IT, Datenschutz und Informationssicherheit.

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.


KOSTEN


CHF 3600.– (exkl. MwSt.)

Weitere Infos und Buchung: infosec.ch/is14

NEU! IT Security Workshop

Überprüfung Ihrer IT-Sicherheitsmassnahmen zur Abwehr möglicher Cyberangriffe

 1/2 Tag

 2 bis 4 Personen

IT SECURITY-BEST PRACTICES FÜR IHR UNTERNEHMEN

In diesem Workshop decken wir zusammen mit Ihnen mögliche Einfallstore für Angreifer in Ihre IT-Infrastruktur auf. Wir diskutieren, wie Sie die essenziellen Punkte einer grundlegenden, modernen und wirksamen IT-Sicherheitsarchitektur in Ihrer Organisation verankern können.

Sämtliche Erkenntnisse und Empfehlungen werden direkt innerhalb des Workshops besprochen und anschliessend in einem Kurzbericht aufbereitet.

INHALT

Wir besprechen die geltenden IT Security-Best Practices und passen diese ganzheitlich sowie angemessen auf den Kontext Ihrer Organisation an.

Themen (Liste nicht abschliessend):

- Network Security
- Identity & Access Management
- Backup & Restore
- Incident Response und Business Continuity
- Dokumentation und Inventarisierung
- E-Mail Security
- System Security
- und andere wichtige Themen der IT-Sicherheit

Weitere Infos und Buchung: infosec.ch/it05

ZIELGRUPPE

Entscheidungs- und Risikoträger, Sicherheitsverantwortliche, IT-Leiter, IT-Mitarbeitende, IT Security Manager, Sicherheitsbeauftragte, Security Officer, Information Security Officer, IT-Sicherheitsbeauftragte, Projektleiter.

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.

TEILNEHMERZAHL

Sie bestimmen selbst, wer seitens Ihres Unternehmens, Ihrer Organisation oder Behörde an diesem Workshop teilnimmt. In der Regel sind dies zwischen zwei und vier Personen.

KOSTEN

CHF 3900.– (exkl. Anfahrt und MwSt.)



NEU! Standortbestimmung IKT-Minimalstandard Gas

Überprüfung des Handlungsbedarfs in Bezug auf den IKT-Minimalstandard Gas

🕒 1/2 Tag

👥 2 bis 6 Personen

WO STEHT IHR UNTERNEHMEN BEZÜGLICH IKT-MINIMALSTANDARD GAS?

Vielleicht wurden einzelne Massnahmen bereits realisiert, andere sind in Planung oder wurden noch nicht berücksichtigt. Ohne eine strukturierte Bewertung bleibt das Sicherheitsniveau häufig subjektiv eingeschätzt, lückenhaft dokumentiert und der Umsetzungsgrad des Standards unklar.

Die Standortbestimmung zum IKT-Minimalstandard Gas liefert Ihnen:

- Eine strukturierte Analyse aller für Ihre Schutzstufe (A, B oder C) relevanten Massnahmen
- Eine nachvollziehbare Bewertung des Umsetzungsgrades
- Eine klare Sicht auf Stärken, Schwächen und Handlungsfelder
- Ein einheitliches objektiv angewendetes Bewertungsraster

ZIEL

Im Rahmen dieser Standortbestimmung analysiert einer unserer Informationssicherheitsexperten gemeinsam mit Ihnen die konkrete Situation Ihres Unternehmens und identifiziert Lösungsansätze.

Im Nachgang erstellen wir eine Auswertung und geben Ihnen konkrete Handlungsempfehlungen zur gezielten Umsetzung des IKT-Minimalstandard Gas.

ZIELGRUPPE

Unternehmen im Bereich der Gasversorgung

TERMIN/ORT

Bei Ihnen vor Ort oder auf Wunsch auch digital, zum Beispiel via Microsoft Teams.

TEILNEHMERZAHL

Sie bestimmen selbst, wer an diesem Workshop teilnimmt. In der Regel sind dies zwischen zwei bis sechs Personen.

KOSTEN

Schutzstufe C: CHF 2900.– (exkl. MwSt.)
Schutzstufen A, B: ab CHF 3900.– (exkl. MwSt.)

Weitere Infos zur Unterscheidung der Schutzstufen und zur Buchung: infosec.ch/is18



#DSGFITNESS

Fit im Datenschutz:

Trainieren Sie Ihr Team mit Online-Trainings!

Datenschutz ist wichtiger denn je. Mit unseren eLearning-Modulen zum Thema Datenschutz schulen Sie Ihre Mitarbeitenden online, effektiv und schnell. Sorgen Sie dafür, dass jedes Teammitglied im Datenschutz fit ist!

Kostenloser Testzugang: www.infosec.ch/testzugang



Zertifikat der
Swiss Infosec AG



printed in
switzerland

Swiss Infosec AG
Meienriesliweg 15
CH-6210 Sursee
Schanzenstrasse 1
CH-3008 Bern
Technoparkstrasse 1
CH-8005 Zürich
+41 41 984 12 12
infosec@infosec.ch



Zertifizierte und anerkannte Lehrgänge
u.a. von BSI, IRCA, (ISC)², SAQ