

AUSBILDUNG**IT-SICHERHEITSBEAUFTRAGTE* R (CISO)**

Lehrgangsnummer: CS-2-03

- ZIEL**
 Erlernen des Know-how, um ein vollständiges IT-Sicherheitskonzept gemäß ISO/IEC 27000 ff. im eigenen Unternehmen zu implementieren und zu managen.
 Kennen und Beurteilen der rechtlichen Rahmenbedingungen für eine ISMS-Kompetenz, um gegenüber Dritten (z.B. Behörden) als Ansprechpartner für IT-Sicherheit anerkannt zu werden.
- ZUGANGSVORAUSSETZUNG**
 Mindestens nachgewiesene Qualifikation auf dem Niveau einer Ausbildung nach oder analog zur ISMS Foundation
- LERNMETHODIK**
 Lehrvortrag, Diskussion, Projektarbeit
- LEHRGANGSMATERIALIEN**
 Als seminarbegleitende Unterlage erhalten Sie ein Lehrgangsskript in digitaler Form oder auf Wunsch auch auf Papier.
- ZERTIFIKATSERWERB**
 Zum Abschluss des Lehrgangs erhalten Sie eine Teilnahmebescheinigung. Sofern der Lehrgang mit einer bestandenen Prüfung endet, wird Ihnen ein Zertifikat ausgestellt.
- FACHLICHER ANSPRECHPARTNER**
 Prof. h.c. PhDr. Stefan Loubichi
 CISO-MCSE-MCDBA-MCAD-CCNA
 Telefon 0201 4862-201 | E-Mail s.loubichi@ksg-gfs.de
- ANMELDUNG**
 Daniela Ruhrus
 Telefon 0201 4862-151 | E-Mail d.ruhrus@ksg-gfs.de
- LEHRGANGSINHALTE**
 - DSGVO und Informationssicherheit
 - IT-Management und Informationssicherheit
 - Informationssicherheitsstrategie
 - Informationssicherheitsziele
 - Aktuelle Bedrohungen der Cyber-Security
 - IT-Compliance
 - IT-Governance
 - IT-Sicherheitsgesetz und Kritis-VO
 - NIS Richtlinie und Cyber Security Act
 - ITIL und COBIT
 - IT-Controlling
 - IT-Scorecard
 - Kennzahlen in der Informationssicherheit
 - Aufgaben der beauftragten Person für IT-Sicherheit
 - Sicherheitsorganisation und Verantwortlichkeiten im ISMS
 - Die Aufbauorganisation im ISMS
 - Fachbegriffe der ISO/IEC 270xx und der IT-Sicherheit
 - Überblick über die ISO/IEC 270xx Normenreihe
 - Zusammenwirken zwischen ISO/IEC 27001 und 27002
 - Informationssicherheitsleitlinie
 - Planung, Betrieb, Kontrolle und Aufrechterhaltung eines ISMS
 - Benötigte Ressourcen für ein ISMS
 - Verantwortlichkeiten und Rollen im ISMS
 - Risikolagen und Bedrohungsszenarien
 - Strukturanalyse
 - Schutzbedarfsfeststellung
 - Schutzbedarfsklassen
 - Überblick über den BSI IT-Grundschutz
 - Erstellung eines IT-Sicherheitskonzeptes
 - Umsetzung des IS-Sicherheitsprozesses
 - Risikomanagement nach ISO 31000
 - Der IT-Risikomanagementprozess
 - IT-Risiko-Assessment
 - Risikobehandlung und Maßnahmenumsetzung
 - Business Continuity Management (BCM) nach ISO 22301
 - Business Impact Analyse (BIA)
 - Erstellung eines IT-Notfallkonzeptes
 - Branchenspezifische Normen wie die ISO/IEC 27019

DATEN UND FAKTEN

Dauer	4 Tage
Teilnehmer*innen	min. 12 - max. 20
Termine	12. - 15.05.2020 und 26. - 29.10.2020 oder auf Anfrage
Zeit	8.00 - 16.30 Uhr
Gebühren	2.000,00 € zzgl. MwSt.
Ort	Simulatorzentrum in Essen oder Siemens Energy Standort Karlsruhe oder Erlangen oder als Inhouse-Seminar bei Ihnen vor Ort

