Leistungsportfolio

SECURITY | PRIVACY | CONTINUITY

www.cis-cert.com

WILLKOMMEN!

INHALT

Liebe Leserinnen und Leser,

als akkreditierter Zertifizierungspartner ist CIS Certification auf Informationssicherheit, Datenschutz, Cloud Computing, NISG 2026, Rechenzentren, IT-Service-Management-Systeme sowie auf Business Continuity Management spezialisiert. CIS Certification ist außerdem führende Zertifizierungsstelle für ISO 27001 (Informationssicherheit), ISO 22301 (Business Continuity) und größter NIS-Prüfer in Österreich.

RECHTLICHE FORTSCHRITTE IN DER CYBERSECURITY

Das neue Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) bringt strengere Anforderungen an Cybersicherheit, Risikomanagement und Meldepflichten. Mit dem Cyber Resilience Act (CRA), dem Artificial Intelligence (AI) Act und dem Digital Operational Resilience Act (DORA) rückt Cybersecurity auch gesamtgesellschaftlich immer stärker in den Fokus. Stärken Sie Ihre Informationssicherheit und Compliance: Nichts ist so aussagekräftig wie ein Zertifikat, basierend auf einer unabhängigen Prüfung durch ein akkreditiertes Unternehmen.

KÜNSTLICHE INTELLIGENZ IM FOKUS

Der digitale Wandel und technologische Fortschritt einschließlich Artificial Intelligence verändern Unternehmen und Gesellschaft gleichermaßen. Sie bieten neue Chancen, aber auch ein erhöhtes Bedrohungspotenzial. Mit der ISO 42001 bietet CIS Certification den weltweit ersten Standard für AI Managementsysteme an, sowie die dazu passende Ausbildungen als AI Manager und Auditor.

KOMPETENZ IM VORDERGRUND

Unser langjährig erfahrenes Team aus Auditorinnen und Auditoren führt qualitativ hochwertig Audits durch, immer mit Fokus auf Mehrwert für Ihre Organisation. Durch die Akkreditierung nach ISO 17021-1 sind Systemzertifikate der CIS Certification als objektiver Nachweis international anerkannt. In unseren praxisorientierten Ausbildungen vermitteln Ihnen erfahrene Vortragende, worauf es in der Praxis ankommt. Aufgrund der Akkreditierung nach ISO 17024 gelten CIS-Personenzertifikate als staatlich und international anerkannte Dokumente.

Ob Zertifizierungen oder Trainings – wir haben das passende Angebot für Sie. Stay Secure!

Thomas Mann
Geschäftsführer CIS

MISSION

WOFÜR WIR STEHEN

CIS - Certification & Information Security Services GmbH ist ein österreichisches Dienstleistungsunternehmen und 100%ige Tochter der Quality Austria Holding GmbH. CIS hat ihren Ursprung im Bereich der **Zertifizierung von Managementsystemen und der Zertifizierung von Personen**. Für beide Dienstleistungsbereiche ist sie vom Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET) bzw. der Akkreditierung Austria als Zertifizierungsstelle akkreditiert. Darüber hinaus ist CIS zusätzlich durch die internationale Organisation APMG akkreditiert, um weltweit Systemzertifikate für ISO 20000 nach den Anforderungen der ISO 17021-1 auszustellen.

Die Zertifizierung von Managementsystemen wird ausschließlich unter **Anwendung internationaler Normen (ISO)** durchgeführt, im Bereich von Personen werden anerkannte normative Dokumente als Basis der Zertifizierung angewendet.

Als akkreditierter Zertifizierungspartner ist CIS auf Informationssicherheit, Datenschutz, IT-Services, Cloud Computing, Rechenzentren sowie auf Business Continuity Management spezialisiert. Das international hohe Ansehen von CIS-Zertifikaten erweist sich oftmals als deutlicher Vorteil im Wettbewerb – sowie auch als „Türöffner" in weltweiten Genehmigungsverfahren genauso wie in nationalen und internationalen Ausschreibungen. Darüber hinaus kann der erprobte Zertifizierungsablauf einen erheblichen Mehrwert für die Organisationen generieren. Im Rahmen eines Zertifizierungsprojekts bringen CIS-Auditor*innen ihr profundes Fachwissen in der Vorbereitungsphase und in den Audits aktiv ein.

Der Wert unserer Zertifizierung zeichnet sich durch folgende Prämissen aus:

- **praxisorientierte Audits mit erkennbarem Mehrwert für die zertifizierte Organisation,**
- **Anwendung international anerkannter Regeln (z. B. ISO Normen oder CENELEC Normen),**
- **Akkreditierung durch eine kompetente Akkreditierungsstelle und**
- **der Einhaltung der nachfolgend beschriebenen Grundsätze:**

UNPARTEILICHKEIT

CIS ist ein eigenständiges Unternehmen und dadurch frei in der Festlegung ihrer Politik, ihres Handelns und ihrer Entscheidungen und somit nur ihren Kund*innen verpflichtet. Die Leistungserbringung für diese erfolgt unbeeinflusst und unabhängig von Beratungsorganisationen, Wettbewerbsunternehmen oder sonstigen einflussnehmenden Interessensgruppen. CIS hat eine Akkreditierung als Zertifizierungsstelle für Managementsysteme und Personen aus der Überzeugung angestrebt, dass eine Wissensvermittlung und Bescheinigung der Kompetenz von einzelnen Organisationen und in Organisationen tätigen Menschen für eine Einführung und Aufrechterhaltung eines Managementsystems essenziell ist und nachhaltig wirkt.

VERANTWORTLICHKEIT

CIS ist sich der Tatsache bewusst, dass jedes Audit nur Stichproben-Charakter haben kann. Um trotzdem über die Erfüllung der Anforderungen für die Zertifizierung eine unabhängige Entscheidung treffen zu können, ist vor allem eine umfassende und nachvollziehbare Audit-Berichterstattung wesentlich.

OFFENHEIT

CIS legt alle sachdienlichen Informationen, welche die Zertifizierung betreffen und nicht der Vertraulichkeit unterliegen, auf ihrer Website offen.

VERTRAULICHKEIT

Alle im Namen der CIS handelnden Personen sind durch entsprechende Vereinbarungen zur strikten vertraulichen Behandlung von in Erfahrung gebrachten Sachverhalten oder eingesehenen Informationen/Dokumenten verpflichtet.

KOMPETENZ

CIS ist auf das Dienstleistungsspektrum im Bereich der Zertifizierung von Managementsystemen für Informationssicherheit, Datenschutz, IT Service Management und Business Continuity Management fokussiert. Spezifisches Fachwissen und Erfahrung bringen CIS-Auditorinnen und -Auditoren im Rahmen des Zertifizierungsablaufs direkt ein. Darüber hinausgehende Zusatzleistungen auf dem Gebiet der Beratung werden aus Gründen der Unparteilichkeit nicht angeboten.

FACTS

AKKREDITIERUNG

Mit einem CIS-Zertifikat befinden sich Unternehmen und Organisationen buchstäblich auf der sicheren Seite. Denn die CIS - Certification & Information Security Services GmbH ist in ihrer Funktion als **unabhängige Zertifizierungsgesellschaft staatlich akkreditiert** und damit strengen Richtlinien unterworfen.

Regelmäßig wird die CIS nach gesetzlich vorgeschriebenen Standards durch das österreichische Wirtschaftsministerium überprüft und erfüllt damit die Anforderungen der internationalen Normen

- ISO/IEC 17021-1 für die **Systemzertifizierung**
- ISO/IEC 17024 für die **Personenzertifizierung**
- ISO/IEC 17065 für **Produktzertifizierung**

WELTWEITE GÜLTIGKEIT

Die nationale Akkreditierung besitzt aufgrund der Abkommen mit EA und IAF weltweite Gültigkeit.

MITARBEITER*INNEN

15 Mitarbeitende (Österreich)

Über 180 Netzwerkpartner*innen
Österreich und International

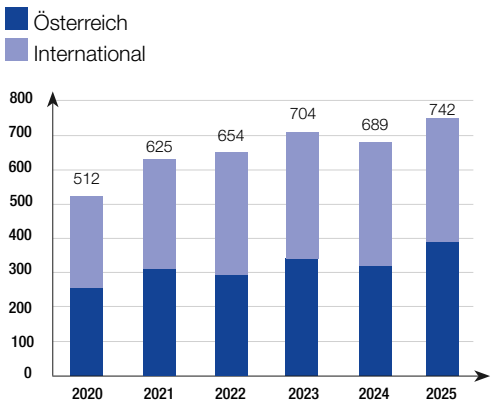
CIS COMPLIANCE SUMMIT

Der CIS Compliance Summit ist die österreichische Plattform für Expert*innen, Sicherheits-Verantwortliche und Entscheidungsträger*innen der Security-Industrie. Best Practices, Keynote-Präsentationen, langjährige Hands-on-Erfahrungen und Networking mit rund 300 Gleichgesinnten inklusive.

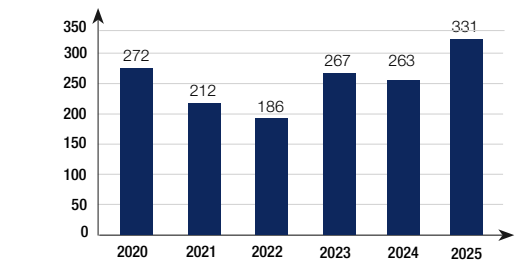
TAUSCHEN WIR UNSER WISSEN AUS UND
WERDEN SIE TEIL DER SECURITY-COMMUNITY!

www.cis-cert.com/cis-compliance-summit

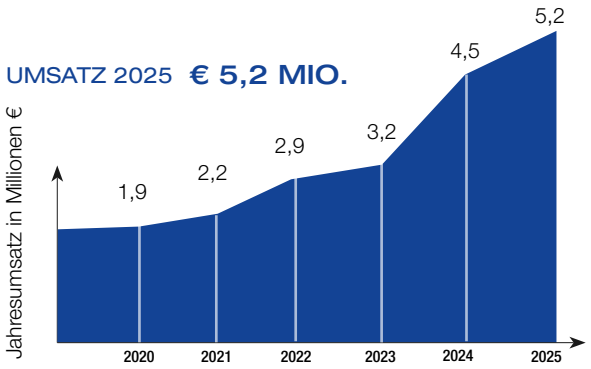
AUSGESTELLTE SYSTEMZERTIFIKATE



AUSGESTELLTE PERSONENZERTIFIKATE



UMSATZ 2025 € 5,2 MIO.



VORTEILE

IHRE VORTEILE

CIS Certification bietet als regionaler und internationaler Zertifizierungspartner Vorteile, die sich rechnen.

- **Impulse**: CIS-Auditberichte liefern detaillierte Stärken-/Schwächen-Analysen
- **Mehrwert**: Vorsprung bei Ausschreibungen durch anerkanntes ISO-Zertifikat
- **Vertrauen**: hohes Ansehen der CIS-Zertifikate weltweit bei Kund*innen & Behörden
- **Synergien**: bis zu 20 Prozent Ersparnis durch Kombi-Audits, auch mit ISO 9001
- **Fachwissen**: profunde Expertise durch CIS-Spezialisierung auf IT-affine Standards
- **Internationalität**: nutzen Sie CIS-Services aus einer Hand – in mehr als 30 Nationen
- **Unsere Erfahrung zu Ihrem Vorteil:** CIS-Auditor*innen bringen ihr Know-how praxisnah ein
- **Objektivität und Unabhängigkeit**: nachgewiesene Transparenz durch unabhängige Prüfung

UNSERE PARTNERSCHAFTEN

Als global agierende Zertifizierungsorganisation ist CIS Certification für Sie mit ihrem Leistungsangebot in mehr als 30 Nationen präsent. Unsere lokalen Niederlassungen und Repräsentationen betreuen Sie optimal vor Ort.

Erfahren Sie mehr dazu auf der nächsten Seite!

UNSERE KERNKOMPETENZEN

- Security
- Privacy
- Artificial Intelligence
- Continuity
- IT-Services
- Rechenzentren

COMMUNITY

Quality Austria Holding GmbH

Quality Austria Certification GmbH

CIS Certification & Information Security Services GmbH

Quality Austria Academy GmbH

TOCHTERGESELLSCHAFTEN

CIS Schweiz
Certification & Information Security Services AG
CIS Anteil 100% | **CEO**: Theo Zahner

CIS Polen
Certification & Information Security Services Sp. z.o.o.
CIS Anteil 71% | **CEO**: Miroslaw Bienioszek

CIS Tschechien
Certification & Information Security Services s.r.o.
CIS Anteil 51% | **CEO**: Petr Kopecky

CIS Ungarn
Információ Biztonságtechnikai Szolgáltató és Tanusít ó Kft.
CIS Anteil 80% | **CEO**: Tamas Jokay

MUTTERGESELLSCHAFT

CIS – Certification & Information Security Services GmbH ist Teil der Quality Austria Gruppe und eine 100%ige Tochter der Quality Austria Holding GmbH.

SCHWESTERGESELLSCHAFTEN

Unsere Kund*innen profitieren von unseren integrierten Managementsystem- und Trainingslösungen durch enge Zusammenarbeit mit unseren Schwestergesellschaften Quality Austria Certification und Quality Austria Academy.

TOCHTERGESELLSCHAFTEN

CIS ist als internationaler Player mit Gesellschaften mit Mehrheitsbeteiligung in vier Ländern vertreten (siehe Grafik links). Diese Tochterunternehmen liefern CIS Services aus erster Hand in lokaler Sprache, und bedienen insbesondere die Märkte in der Region Zentral- und Osteuropa.

PARTNERGESELLSCHAFTEN

- Quality Austria Adriatic d.o.o., Zagreb, Kroatien
- Quality Austria Center d.o.o., Belgrade, Serbien
- Quality Italia S.r.l. Roma, Italien
- Quality Austria Certification Gulf, W.L.L. Doha, Katar
- Quality Austria Central Asia, New Delhi, Indien
- Quality Austria Polska, Polen
- QMD Services, Österreich
- SIQ Slovenian Institute for Quality and Metrology, Ljubljana, Slowenien
- Shanghai OQS International, China
- TCIC Ltd. Surrey, B.C., Kanada
- LSQA Uruguay

SERVICE

WIR HELFEN IHNEN GERNE WEITER.

Wir freuen uns auf Ihre Kontaktaufnahme!

CIS NEWSLETTER

Der CIS Newsletter liefert Ihnen topaktuelle News – profitieren Sie von Expert*inneninsights und Informationen aus erster Hand zu Zukunftstrends, Case Studies, Events und dem CIS-Leistungsportfolio. Jetzt kostenlos abonnieren und immer up-to-date bleiben!

www.cis-cert.com/newsletter

CIS SOCIAL MEDIA

News und Trends aus der Branche warten auf Sie – vernetzen Sie sich mit Gleichgesinnten und verpassen Sie keine Updates mehr. Jetzt den CIS LinkedIn Kanal abonnieren. LET'S CONNECT!

www.linkedin.com/company/cis-certification-information-security-services-gmbh/

AGB

Die Allgemeinen Geschäftsbedingungen für unsere Dienstleistungen im Bereich Systemzertifizierung und Begutachtung sowie für Personenzertifizierung und Aus- und Weiterbildung finden Sie online: **www.cis-cert.com/agb**

KONTAKT

Unsere Trainingsräumlichkeiten bieten unseren Kund*innen moderne Schulungsräume mit zeitgemäßer Technologie.
Wir freuen uns auf Ihren Besuch:

Salztorgasse 2/3/7, 1010 Wien

Gerne stehen wir Ihnen im Web per Kontakt-Formular oder telefonisch unter **Tel.: +43 1 532 98 90** zur Verfügung.

www.cis-cert.com/kontakt

KARRIERE

Wir erweitern laufend unser Team. Momentan sind wir nicht aktiv auf der Suche, aber freuen uns über Initiativbewerbungen und spannende Persönlichkeiten. **office@cis-cert.com**

UNSERE SERVICEKOORDINATION

Claudia Gusso
Head of Servicekoordination
office@cis-cert.com

Jasmin Abdel-Wahed
Servicekoordination
office@cis-cert.com

Astrid Danzinger
Servicekoordination
office@cis-cert.com

Sabine Ihl
Servicekoordination
office@cis-cert.com

Christian Lassnig
Servicekoordination
office@cis-cert.com

FRAGEN ZU AUS- UND WEITERBILDUNGEN?

trainings@cis-cert.com

FRAGEN ZU AUDITS UND SYSTEMZERTIFIZIERUNGEN?

audit-services@cis-cert.com

ALLGEMEINE ANFRAGEN?

office@cis-cert.com

SYSTEMZERTIFIZIERUNG

Wir bieten Ihnen mit Analyst*innen aus der Praxis Zertifizierungen und Assessments in den Bereichen:

INFORMATIONSSICHERHEIT

- **ISO 27001** Die Norm für Informationssicherheit: Sicherer Rahmen, individuelles Design.
- **ISO 27701** Zertifiziertes Privacy Information Management System (PIMS) für DSGVO-orientierten Datenschutz.

NISG 2026 | NIS-2

- Überprüfung nach dem Netz- und Informationssystemsicherheitsgesetz (NISG)
- NIS und ISO 27001 im Kombi-Audit
- NISG 2026 Stage Review

TISAX® ASSESSMENT

- Trusted Information Security Assessment Exchange für die Automotive-Industrie

KÜNSTLICHE INTELLIGENZ

- **ISO 42001** Weltweit erste Norm für KI-Managementsysteme. Wettbewerbsfähig bleiben!

CLOUD COMPUTING

- **ISO 27017 und ISO 27018** Datenschutz und Informationssicherheit für die Cloud

ENERGIEWIRTSCHAFT

- **ISO 27019** Informationssicherheitsmaßnahmen für die Energieversorgung
- **Energiewirtschaftsgesetz** (EnWG §11)

BUSINESS CONTINUITY UND IT RESILIENZ

- **ISO 22301** Business Continuity Management: Auf Worst-Case-Szenarien vorbereitet sein.

SERVICE MANAGEMENT

- **ISO 20000** Qualitätsverbesserung und Effizienzsteigerung

RECHENZENTREN

- **EN 50600** Einrichtungen & Infrastrukturen von Rechenzentren – Data Center Design
- Österreichisches **Umweltzeichen** „Rechenzentren UZ 80“ Prüfung

ANSPRECHPERSONEN SYSTEMZERTIFIZIERUNG

Robert Jamnik
Head of Audit Services | Lead Auditor ISO 20000, ISO 27001 und NIS
audit-services@cis-cert.com

Wolfgang Glowatzki
Lead Expert Information Security | Lead Auditor TISAX® und ISO 27001
audit-services@cis-cert.com

Bernhard Kropacek
Audit Services
audit-services@cis-cert.com

Doris Pannosch
Audit Services
audit-services@cis-cert.com

Jessica Bauer
Audit Services
audit-services@cis-cert.com

Elma Pichler
Audit Services
audit-services@cis-cert.com

Zur Übersicht
System- und Produktzertifizierungen

Bei konkreten Fragen und Anliegen stehen wir Ihnen gerne zur Verfügung!

audit-services@cis-cert.com

IHR WEG ZUM SYSTEMZERTIFIKAT

Muster Systemzertifizierung

1. INFORMATIONSGESPRÄCH

Erhalten Sie einen Überblick über den Zertifizierungsprozess und klären Sie offene Fragen.

2. ANALYSE

Bewertung Ihrer bestehenden Prozesse und Identifikation von Optimierungspotenzialen.

3. IMPLEMENTIERUNG

Umsetzung der erforderlichen Maßnahmen gemäß der gewählten Norm.

4. OPTIONALES STAGE-REVIEW

Vorabprüfung zur Identifikation von Stärken und Schwächen.

5. SYSTEM- & RISK-REVIEW

Detaillierte Vorbegutachtung als Generalprobe vor dem Hauptaudit.

6. ZERTIFIZIERUNGSAUDIT

Umfassende Prüfung durch unsere Auditor*innen mit Fokus auf Wirksamkeit und Konformität.

7. ZERTIFIKAT

Erhalt des Zertifikats mit einer Gültigkeit von drei Jahren.

8. ÜBERWACHUNGSAUDITS

Jährliche Audits zur Sicherstellung der kontinuierlichen Verbesserung.

9. REZERTIFIZIERUNG

Erneuerung des Zertifikats nach Ablauf der Gültigkeitsdauer.

INTEGRIERTES MANAGEMENT-SYSTEM UND KOMBINATIONSAUDITS

Der Trend geht in Richtung Integriertes Managementsystem, das Security Management, IT Service Management, Qualitäts- oder Umweltmanagement zu einem einheitlichen Gesamtsystem vereint. Übergeordnete Strategiefindungs- oder Planungsprozesse lassen sich auf diese Art deutlich effizienter gestalten. Unternehmen berichten von Zeit- und Kosteneinsparungen von weitaus mehr als 20 Prozent. Als Fundament für integrierte Gesamtsysteme dient in der Praxis meist ein gut implementiertes Managementsystem, wie z. B. ISO 9001, da dieser Standard inhaltlich am breitesten ausgerichtet ist. Grundsätzlich ist jeder Standard auf Basis des Annex SL denkbar.

ERWEITERUNG

Ein solches grundlegendes Managementsystem lässt sich schrittweise um weitere Komponenten wie zum Beispiel Informationssicherheit (ISMS nach ISO 27001), Datenschutz (DSMS nach ISO 27701), IT Service Management (ITSMS nach ISO 20000) und Business Continuity (BCMS nach ISO 22301) sowie ISO 9001, ISO 14001 u. ä. erweitern.

KOMBINATIONSAUDITS

Für die Zertifizierung eines Integrierten Managementsystems sind integrierte Kombinationsaudits sinnvoll. Durch die Kombination von zwei oder mehr Modellen kann nicht nur der Auditaufwand reduziert werden, sondern eine breitere Sicht auf das Unternehmen und damit auch noch nutzbringendere Ansatzpunkte für die Weiterentwicklung identifiziert werden.

Effizienz durch Systemintegration:

- Vereinfachtes Handling, Übersichtlichkeit und Transparenz
- Gemeinsame Audits für mehrere Systeme entlasten die oberen Führungsebenen
- Effiziente Management Reviews für integrierte Managementsysteme
- Gemeinsame Dokumentation umfasst alle Management- und Businessprozesse
- Ersparnis von Kosten und Zeitaufwand

SYNERGIEN DURCH GESAMTSICHT

Bei fortschreitender Systemreife können die Vorteile der effizienten Kombinationsaudits voll genutzt werden. Integrierte Audits werden in Absprache mit den Prüfer*innen gut geplant, um genau auf die vorhandenen Prozesse aus den unterschiedlichen Managementthemen eingehen zu können. Interessant sind Kombinationsaudits, weil multifunktionell geschulte Auditor*innen eine sonst nicht zu erreichende Sicht auf das Gesamtsystem erhalten, und Optimierungspotenziale über Themen-Grenzen hinweg aufzeigen können.

INFORMATIONSSICHERHEIT

Sicherheitsvorfälle kosten Unternehmen viel Zeit und führen im schlimmsten Fall zu großflächigen Systemausfällen – Reputationsverlust und Schäden in Millionenhöhe inklusive. Es braucht allerdings ein strukturiertes Managementsystem statt nur einzelner Maßnahmen, um Informationen im gesamten Unternehmen heute sichern zu können. Die Einführung eines Informationssicherheitsmanagements bietet ein stabiles Gerüst an funktionierenden Prozessen und Maßnahmen bei Sicherheitsvorfällen.

ISO 27001

Das umfassende Framework des Zertifizierungsstandards ISO/IEC 27001 und des Praxisleitfadens ISO/IEC 27002 ermöglichen die Einführung eines Informationssicherheitsmanagementsystems (ISMS) aus „einem Guss“. Mit dem strukturierten Prozessansatz werden Probleme vermieden, die durch die Implementierung von Einzelmaßnahmen entstehen können. Sicherheitslücken werden systematisch bewertet und minimiert. Die Risikoanalyse zeigt den individuellen Sicherheitsbedarf einer Organisation auf, wobei Wirtschaftlichkeit ein wesentliches Kriterium für die Maßnahmenumsetzung ist.

IHRE VORTEILE

- Erprobter Standard zum Schutz Ihres immateriellen Vermögens: analoge und digitale Informationen
- Framework für technische und organisatorische Maßnahmen mit Wirksamkeitskontrolle sowie Optimierungsschleifen
- Höchster Schutz von Daten und Informationen
- Hochverfügbarkeit der IT-Dienste

ZERTIFIZIERUNG

Zertifiziert wird nach dem ISO 27001 Standard, der die Anforderungen an ein ISMS beschreibt. Bei der Einführung und dem Aufbau eines ISMS stehen weiterführende Informationen als Hilfestellung zur Verfügung (ISO 27002, ISO 27003, ISO 27004, ISO 27005).

Der Standard erlaubt Organisationen jeder Größe und Branche Informationssicherheit zu implementieren, zu messen, zu steuern und zur Selbstprüfung intern zu auditieren.

Die Überprüfung des ISMS durch eine unabhängige, akkreditierte Organisation wie der CIS mündet nach dem vorgegebenen Zertifizierungsablauf in der ISO 27001 Zertifizierung.

DIE NORM FÜR INFORMATIONSSICHERHEIT: SICHERER RAHMEN, INDIVIDUELLES DESIGN.

www.cis-cert.com/informationssicherheit

NISG 2026 – NIS-2 RICHTLINIE

WAS IST NIS-2?

Mit dem Netz- und Informationssicherheitsgesetz 2026 (NISG 2026) setzt Österreich die EU-Richtlinie NIS-2 verbindlich um. Sie ist die Nachfolgerin der ursprünglichen NIS-Richtlinie von 2016 und wurde entwickelt, um europaweit einheitliche und wirksamere Standards für Cybersicherheit zu schaffen. Betroffen sind Unternehmen mit mehr als 50 Mitarbeiter*innen oder einem Umsatz von über 10 Mio. Euro, aus nahezu allen Sektoren (Energie, Transport, Gesundheit, Handel, Produktion, Lebensmittelversorgung, IT-Dienstleister etc.). Auch für kleinere Unternehmen kann NISG 2026 verbindlich sein, wenn sie als Dienstleister oder Lieferant über die Lieferkette oder als Vertrauensdienstanbieter in einen besonderen Anwendungsbereich fallen. **Gehören Sie dazu? Bei Nicht-Einhaltung drohen Bußgelder in Millionenhöhe und beträchtliche Schäden für Ihr Unternehmen.**

Wir stärken Ihnen den Rücken mit zahlreichen Angeboten und empfehlen Ihnen, Synergien zu nutzen: Unternehmen, die bisher schon ein zertifiziertes Managementsystem nach ISO 27001 auf hohem Niveau betrieben haben, können mit geringem Aufwand NISG-konform werden.

NISG 2026 STAGE REVIEW

Wo stehen Sie aktuell in Ihrer Umsetzung? Sie bekommen Empfehlungen direkt aus der Praxis – damit sind Sie perfekt vorbereitet für die Umsetzung.

NISG 2026 PRÜFBERICHT IM KOMBI-AUDIT

ISO 27001 sichert Ihnen den organisatorischen Teil der NISG 2026 Prüfung, wir bieten Ihnen gerne die Kombi aus Audit und Prüfbericht an.

NISG 2026 FÜR GROSSUNTERNEHMEN

Sie müssen NISG 2026 für mehrere Standorte umsetzen? Dann eignet sich die Multisite-Zertifizierung nach IAF MD 01 für Sie.

WEITERBILDUNG FÜR JEDES LEVEL

Wir gehen auf individuelle Anforderungen Ihres Unternehmens ein und vermitteln Ihnen die Inhalte rasch und effizient!

Durch die jahrelange Erfahrung der CIS Certification Expert*innen bringen wir vor allem Praxisbezug und Pragmatismus mit. CIS Certification ist die führende Zertifizierungsstelle für ISO 27001 (Informationssicherheit), ISO 22301 (Business Continuity) und größter NIS-Prüfer in Österreich. Als qualifizierte Stelle wird CIS Certification ab 01.Oktober 2026 automatisch unabhängiger NIS-Prüfer nach NISG 2026 (unabhängige Stelle).

NACHWEIS DER GESETZESKONFORMITÄT

Per Bescheid durch das Bundesministerium für Inneres wurde die Zertifizierungsorganisation CIS im Februar 2020 bevollmächtigt, als Qualifizierte Stelle für NIS-Überprüfungen zu fungieren.

CYBERSECURITY FÜR WESENTLICHE UND WICHTIGE SEKTOREN.

www.cis-cert.com/produktgruppen/nis-2

TISAX®

TRUSTED INFORMATION SECURITY ASSESSMENT EXCHANGE

TISAX® (Trusted Information Security Assessment Exchange) ist ein branchenspezifischer Austauschmechanismus der Automobilindustrie für Ergebnisse aus Informationssicherheitsassessments. Diese Assessments basieren auf dem ISA Prüfkatalog, welcher Kontrollfragen zur Informationssicherheit (basierend auf der ISO 27001), zu Prototypenschutz und zum Datenschutz beinhaltet.

ÜBERBLICK

Mit einem TISAX® Assessment stellen Sie sicher, dass Ihre Lieferant*innenzulassung aufrecht bleibt, und verschaffen Ihrem Unternehmen einen Wettbewerbsvorteil in Entwicklungs- und Prototypenprojekten.

IHRE VORTEILE

- Erfüllung der automotiven Kund*innenanforderungen
- Nachweis eines geprüften Informationssicherheitslevels
- Anerkennung der Prüfergebnisse am automotiven Markt / in der automotiven Supply Chain
- Erhöhter Schutz der eigenen Informationswerte
- Bewusstseinsschärfung der Mitarbeiter*innen
- Basis für eine zusätzliche Zertifizierung nach ISO 27001
- Zusätzlicher Schutz in den Bereichen Prototyping und Datenschutz

OBJEKTIVE BEGUTACHTUNG

Mit einem TISAX® Assessment weisen Sie die Reife Ihres Informationssicherheitsmanagementsystems (ISMS) entsprechend Ihrer Kund*innenanforderungen nach. Dies kann auf unterschiedlichen Prüflevels und den Zusatzanforderungen zum Prototypen- und Datenschutz Ihrer Kund*innen erfolgen.
Als Nachweis zur Reife Ihres ISMS werden Ihnen sogenannte TISAX®-Prüflabel ausgestellt, die Sie mit Ihren Geschäftspartner*innen über die TISAX®-Plattform teilen können.
Damit stellt TISAX® die Grundlage zum Prüf- und Austauschmechanismus Ihres Informationssicherheitsmanagementsystems in der Automobilindustrie dar. Für die Umsetzung benötigen Sie eine gute Basis, welche Sie mit dieser Qualifizierung erlangen können.

NACHGEWIESENE SICHERHEIT FÜR AUTOMOTIVE PRODUZENTEN UND ZULIEFERER.

www.cis-cert.com/tisax

KÜNSTLICHE INTELLIGENZ

ISO 42001

Künstliche Intelligenz (KI) ist gekommen, um zu bleiben. Egal, ob Sie bereits KI einsetzen oder ob sich Ihr Unternehmen in den nächsten Jahren damit beschäftigen wird: KI ist ein Thema, an dem Unternehmen nicht mehr vorbeikommen werden, wenn sie wettbewerbsfähig bleiben möchten.

ÜBERBLICK

Die ISO 42001 ist der weltweit erste Standard für KI-Managementsysteme und bietet wertvolle Leitlinien für dieses sich schnell verändernde Technologiefeld. Sie spezifiziert Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines KI-Managementsystems in Organisationen, insbesondere für Unternehmen, die KI-basierte Produkte oder Dienstleistungen bereitstellen oder nutzen.

Dabei gewährleistet die ISO 42001 eine verantwortungsvolle Entwicklung und Nutzung von KI-Systemen. Der Standard behandelt die einzigartigen Herausforderungen, die KI mit sich bringt, wie ethische Überlegungen, Transparenz und kontinuierliches Lernen, und legt einen strukturierten Ansatz zur Bewältigung der mit KI verbundenen Risiken und Chancen fest.

IHRE VORTEILE

Eine Zertifizierung nach ISO 42001 dient als greifbarer Beweis für das klare Engagement einer Organisation für verantwortungsvolle KI-Praktiken:

- Stellen Sie ethische Entwicklung und Anwendung von KI-Systemen sicher
- Profitieren Sie von robusten Governancestrukturen
- Stärken Sie Ihr KI-bezogenes Risikomanagement
- Kümmern Sie sich um die Einhaltung von sich laufend verändernden KI-Compliance Anforderungen
- Profitieren Sie von der Integration in bestehende Managementstrukturen
- Setzen Sie ein Zeichen der Verantwortung an Ihre Kund*innen und Partner*innen
- Bleiben Sie dem Wettbewerb eine Nasenlänge voraus

ZERTIFIZIERUNG

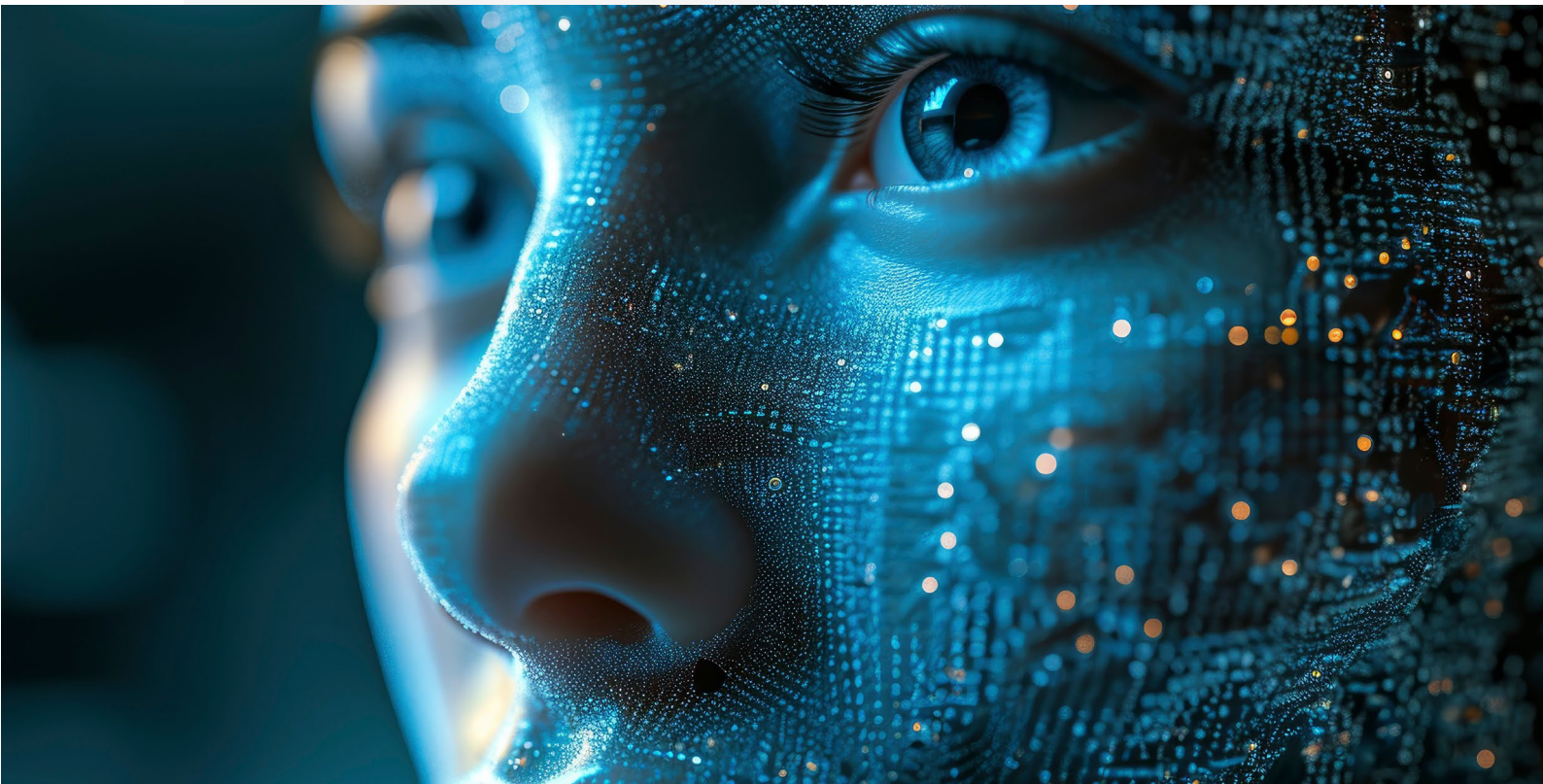
Wenn Sie einen Ansatz für KI-Management suchen, der bestmöglich integrierbar mit bestehenden Managementstrukturen ist, dann ist ISO 42001 ein gutes Rahmenwerk für das strategische Management diverser KI-bezogener Themen. CIS bietet Ihnen in einem Erstgespräch die Möglichkeit, weitere Schritte zu besprechen.

AUSBILDUNG AI MANAGER UND AUDITOR

Wir vermitteln Ihnen wesentliche Grundlagen, um als Artificial Intelligence Manager bzw. Auditor erfolgreich zu agieren. Unsere Kurse legen Wert auf praxisnahes und fundiertes Wissen u.a. in folgenden Bereichen: ISO 42001, Rechtsgrundlagen, Ethik und Risikomanagement.

DER WELTWEIT ERSTE STANDARD FÜR KI-MANAGEMENT-SYSTEME!

www.cis-cert.com/KI



DATENSCHUTZ

INTEGRIERTER ANSATZ AUF BASIS VON ISO 27001 UND ISO 27701

Die Norm ISO 27701 hilft Ihnen dabei, die datenschutzrechtlichen Anforderungen systematisch und effizient umzusetzen und aufrechtzuerhalten. Sie stellt eine Erweiterung der bekannten ISO 27001 dar. Sie ergänzt den Standard für Informationssicherheitsmanagementsysteme (ISMS) um eine Reihe wesentlicher Datenschutzaspekte.

ÜBERBLICK

Beide Normen und das gemeinsame Managementsystem basieren auf den Prinzipien Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen. So ist das Zusammenwirken dieser ISO Normen wenig überraschend und eine gemeinsame Implementierung ist sehr empfehlenswert.

Eine ISO 27701 Zertifizierung kann gemeinsam mit einer ISO 27001 Zertifizierung erworben werden, sofern diese noch nicht vorhanden ist. Mit der neuen Fassung der ISO 27701 ist das DSMS aber auch unabhängig von der ISO 27001 zertifizierbar. Dieser generisch aufgebaute Standard richtet sich an alle Arten und Größen von Organisationen mit Anforderungen an einen umfassenden Schutz von Daten und Informationen – unabhängig von Branche und Gesellschaftsform.

IHRE VORTEILE

- Erhöhung der Rechtssicherheit und Transparenz
- Sicherstellung solider Datenschutzmechanismen
- Erhöhung der Datenschutzkompetenz
- Risikominimierung für Datenschutzverletzungen und Konsequenzen daraus
- Vertrauensbildung bei bestehenden und potenziellen Kund*innen

ZERTIFIZIERUNG

CIS bietet als eine der ersten international akkreditierten Anbieter*innen das Zertifikat für Datenschutzmanagement nach ISO 27701 – als Add-On zu ISO 27001 – welches einen objektiven Nachweis für DSGVO-orientierten Datenschutz in Ihrem Unternehmen darstellt. Das Zertifikat schafft nach innen sowie nach außen Vertrauen und ist ein klares Signal am Markt.

ZERTIFIZIERTES PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS) FÜR DSGVO-ORIENTIERTEN DATENSCHUTZ.

www.cis-cert.com/datenschutz

CLOUD COMPUTING

Die wichtigsten Anforderungen an Cloud-Dienste sind Datenschutz und Verfügbarkeit. Gemäß den geltenden nationalen Datenschutzgesetzen sowie der Datenschutzgrundverordnung (DSGVO) haften Organisationen und Unternehmen für ihre Daten auch dann, wenn diese im Rahmen einer Auftragsdatenverarbeitung bei einem Cloud Provider verarbeitet werden und es dort zu Datenpannen kommt. Um der gesetzlich geforderten Sorgfaltspflicht nachzukommen, müssen Organisationen und Unternehmen, wenn sie als Verantwortliche Daten verarbeiten, die Sicherheit der Datenverarbeitung – auch beim Dienstleister oder Auftragsverarbeiter – sicherstellen. Dies muss durch geeignete Verträge sowie Prüfungen und Nachweise erfolgen!

ISO 27017 – INFORMATIONSSICHERHEIT FÜR CLOUD SERVICES

Die ISO 27017 ist eine Erweiterung der ISO 27002 und bietet im Zusammenspiel mit der ISO 27001 sowohl für Cloud Service Betreiber als auch für Unternehmen, die Cloud Service Kund*innen sind, ein Rahmenwerk, mit deren Hilfe sie spezifische Maßnahmen für Cloud Services implementieren können. Dabei erfolgt die Auswahl und Umsetzung der spezifischen Sicherheitsmaßnahmen auf Basis der Risikoanalyse, wie sie von der ISO 27001 gefordert wird.

ISO 27018 – DATENSCHUTZ FÜR CLOUD SERVICES

Der international anerkannte Cloud-Standard ISO 27018 für Datenschutz setzt ein starkes Signal für Ihre Kund*innen. Die ISO 27018 fokussiert sich auf den „Schutz von personenbezogenen Daten in der Cloud“ für Dienstleistende bzw. Auftragsverarbeitende, indem sie spezifischere Vorgaben hinsichtlich der Umsetzung von Datenschutzmaßnahmen macht.

IHRE VORTEILE

- Gut gerüstet für den Cloud-Markt der Zukunft
- Weltweit gültig und international anerkannt
- Erhöht das Vertrauen von Kund*innen in Cloud-Dienste für kritische Unternehmensbereiche
- Höchster Schutz von Personendaten
- Minimierung des Risikos von Vertragsbrüchen
- Anforderungen der EU-Datenschutzgrundverordnung umsetzen
- Nutzen Sie Synergie-Effekte mit der ISO 27001

DATENSCHUTZ UND SERVICEQUALITÄT ALS STARKES SIGNAL AN IHRE KUND*INNEN.

www.cis-cert.com/cloud-computing

ENERGIEWIRTSCHAFT

Die Zukunft der Energieversorgung – und vieler anderer Bereiche – ist von einer funktionierenden Informations- und Kommunikationstechnologie abhängig. Für Betreibende und Unternehmen ist es nicht immer einfach, sich im Dickicht verschiedener Normen und Standards zurechtzufinden. Gleichzeitig bieten die existierenden Normen sehr gute Implementierungshilfen auf dem Weg als Unternehmen sicherer und besser zu werden. CIS als langjähriger Zertifizierungspartner greift auf umfassendes Know-How zurück und bietet Systemzertifizierungen im Rahmen der ISO 27000-Serie (ISO 27019 – speziell für Energieversorger).

ISO 27019 – SICHERHEITSMASSNAHMEN FÜR ENERGIEVERSORGER

Mit der ISO 27019 steht Energieversorgern eine international anerkannte Norm zur Weiterentwicklung der unternehmenseigenen Sicherheitsmaßnahmen zum Schutz für Systeme der Energieversorgung zur Verfügung.

Die Norm baut auf der ISO 27001 und der ISO 27002 auf und lässt sich daher leicht in ein neues oder bestehendes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 integrieren. Konkretisierungen und Erweiterungen der ISO 27002 unter Berücksichtigung des risikoorientierten Ansatzes der ISO 27001 ermöglichen eine zielgerichtete Weiterentwicklung der bereits bestehenden Sicherheitsmaßnahmen zum Schutz von Systemen der Energieversorgung im Unternehmen.

ENERGIEWIRTSCHAFTSGESETZ (ENWG §11)

Gesetzeskonformität und Impulse zur Weiterentwicklung der Sicherheit von Energieversorgungsnetzen und Energieanlagen

EnWG §11 Absatz 1a, EnWG §11 Absatz 1b

Der deutsche Gesetzgeber definiert im Energiewirtschaftsgesetz (EnWG) die Pflicht zum Betrieb eines sicheren Energieversorgungsnetzes bzw. sicherer Energieanlagen. Basis hierfür sind die ISO 27001, ISO 27019 und der Sicherheitskatalog gemäß EnWG §11 1a bzw. EnWG §11 1b. Betreiber von Energieversorgungsnetzen und/oder Energieanlagen, die unter dieses Gesetz fallen, sind verpflichtet eine entsprechende Umsetzung durch ein akkreditiertes Unternehmen nachzuweisen.

EFFIZIENT, NACHHALTIG, ZUKUNFTSGELADEN: ENERGIEWIRTSCHAFT VON MORGEN ENTWICKELN.

www.cis-cert.com/energiewirtschaft

BUSINESS CONTINUITY MANAGEMENT

In einer zunehmend digitalisierten und vernetzten Welt sind Unternehmen gefordert, nicht nur ihre Betriebsfähigkeit in Krisensituationen sicherzustellen, sondern auch den verantwortungsvollen Einsatz neuer Technologien wie Künstlicher Intelligenz (KI) zu gewährleisten.

Ein ganzheitliches Business Continuity Management nach ISO 22301 schafft belastbare Strukturen, um auch bei Ausfällen oder Störungen handlungsfähig zu bleiben – das gilt insbesondere für Unternehmen, die eine kritische Versorgungsrolle für die Gesellschaft einnehmen (Energieversorger, Gesundheitsdienstleister, Banken, IT- und Telekommunikationsdienstleister, etc.).

Gleichzeitig gibt es auch bei NISG 2026 (NIS-2) einen starken Fokus auf das Thema Resilienz. Gemeinsam bilden beide Normen die Grundlage für resiliente, zukunftsorientierte Organisationen, die technologische Innovation und kritische Infrastruktur mit nachhaltiger Risiko- und Krisenvorsorge verbinden.

ISO 22301 BUSINESS CONTINUITY

Notfall- und Desaster Recovery Pläne können bei disruptiven Ereignissen für den operativen Betrieb von immenser Bedeutung sein. Das jedoch nur, wenn sie den tatsächlichen Bedarf abdecken, aktuell sind und regelmäßig auf Wirksamkeit überprüft wurden – ein gelebtes Business Continuity Management System (BCMS) nach ISO 22301 stellt das sicher.

- **Sicherstellung der Geschäftskontinuität**
  Minimiert Ausfallzeiten und gewährleistet betriebliche Resilienz bei Krisen.
- **Risikominimierung**
  Identifiziert und behebt potenzielle Risiken für kritische Geschäftsprozesse.
- **Stärkung des Unternehmensimages**
  Zeigt Ihren Kund*innen und Partner*innen, dass das Unternehmen auf Krisensituationen vorbereitet ist.
- **Erfüllung gesetzlicher Anforderungen**
  Hilft, branchenspezifische und regulatorische Vorgaben zu erfüllen.
- **Wettbewerbsvorteil**
  Differenziert das Unternehmen durch nachgewiesene Krisensicherheit und kontinuierliche Verbesserung.

IT RESILIENZ STATT PRODUKTIONSAUSFALL UND STILLSTAND.

www.cis-cert.com/it-resilienz

SERVICE MANAGEMENT

ISO 20000

Die Leistung von IT-Diensten steigern und gleichzeitig die Kosten senken – bei höherer Service-Qualität. Mit ISO 20000 ist dies möglich, denn das Regelwerk ist weltweit der erste zertifizierbare Standard, der sich speziell auf IT-Service Management bezieht und auf Qualitätsverbesserung, Effizienzsteigerung sowie eine Kostenreduktion von IT-Leistungen fokussiert.

ÜBERBLICK

Kernstück der Norm sind ein Managementsystem sowie definierte Prozesse zur Entwicklung, Implementierung und Aufrechterhaltung von Services. Ein kontinuierlicher Verbesserungsprozess sorgt für eine Weiterentwicklung und Verbesserung des Gesamtsystems. Diese laufende System-Optimierung führt zu einer nachhaltig höheren Qualität und Effizienz von IT-Diensten. Die Definition von Zielen und dazugehörigen Kennzahlen wie „Kund*innenzufriedenheit“ oder „Service-Verfügbarkeit“ werden regelmäßig erhoben und Maßnahmen zu ihrer Verbesserung erarbeitet.

IHRE VORTEILE

- Kostensenkung und -transparenz
- Ressourcenschonung (z. B. Arbeitszeit bei Fehlerbehebung) und Produktivitätssteigerung
- Erhöhte Transparenz und Qualität der erbrachten Leistungen
- Qualität durch Optimierung
- Weltweit anerkannter Standard
- Sichtbarer Vorsprung durch ein Zertifikat
- Benchmark durch standardisierte Leistungen

ZERTIFIZIERUNG

Ein Managementsystem nach ISO 20000 zeichnet sich durch eine strukturierte Vorgangsweise, die Verantwortung des Managements für Planung, Steuerung und Kontrolle sowie die verpflichtende Dokumentation von Verantwortlichkeiten und Prozessen aus. Ähnlich wie bei anderen ISO Normen gehören die regelmäßige Messung der Zielerreichung und die ständige Verbesserung zu den Basisanforderungen. Zielgruppen für den ISO Standard für Service Management sind grundsätzlich alle Unternehmen, die Dienstleistungen erbringen.

Aufgrund seiner Flexibilität ist der Standard für alle Arten von Services, unabhängig von Unternehmensgrößen oder Branche, geeignet, auch für Abteilungen und Teilbereiche.

SERVICE MANAGEMENT: QUALITÄTSVERBESSERUNG UND EFFIZIENZSTEIGERUNG.

www.cis-cert.com/service-management

RECHENZENTREN

Rechenzentren – Rückgrat der digitalen Welt. Ein Rechenzentrum ist das digitale Herzstück jedes Unternehmens. Hier werden Daten gespeichert, verarbeitet und geschützt – und das rund um die Uhr. Ob Kund*innendaten, Geschäftsprozesse oder Online-Dienste: Unsere Welt basiert auf funktionierenden und stabilen Rechenzentren.

Damit Unternehmen sicher, zuverlässig und effizient arbeiten können, braucht es höchste Standards bei der Verfügbarkeit, Sicherheit und Technologie. Genau hier setzen Zertifizierungen an: Sie garantieren geprüfte Qualität und Ausfallsicherheit, schützen sensible Informationen und schaffen Vertrauen – sowohl für das eigene Unternehmen als auch für Kund*innen und Partner*innen.

CIS arbeitet aktiv im europäischen Normungsausschuss der CENELEC TC 215/WG 3 Facilities and Infrastructures mit, der für die Weiterentwicklung der EN 50600 zuständig ist. Auf nationaler Ebene ist die CIS dazu im diesbezüglich zuständigen österreichischen Normungsgremium des OVE (Österreichische Verband für Elektrotechnik) vertreten. Dadurch bleiben wir stets up-to-date und am Puls der Entwicklungen – und geben dieses Know-How an unsere Kund*innen weiter.

EN 50600

Mit der vom „European Committee for Electrotechnical Standardization“ (CENELEC) herausgegebenen EN 50600-Serie wurde der erste europaweit länderübergreifende Standard für Rechenzentren (RZ) mit einem ganzheitlichen Ansatz geschaffen. Mit diesem ganzheitlichen Ansatz bietet die EN 50600 nicht nur technische Vorgaben, sondern auch strukturierte Methoden zur Bewertung von Risiken, Verfügbarkeit, Energieeffizienz und Betriebsprozessen. Dadurch wird die Qualität eines Rechenzentrums transparent und zertifizierbar – ein wachsender Wettbewerbsvorteil für Betreibende und ein wichtiges Kriterium für Kund*innen in Zeiten von Cloud-Computing und IT-Outsourcing.

UMWELTZEICHEN UZ 80 RECHENZENTREN

Das Österreichische Umweltzeichen wird durch die Republik Österreich, vertreten durch die Bundesministerin für Klimaschutz, nach eingehender Prüfung der Erfüllung der Kriterien für vier Jahre vergeben. Antragsinteressent*innen erhalten die Antragsunterlagen beim Verein für Konsumenteninformation.
Als Nachweis für die Umsetzung der genannten Kriterien ist ein Gesamtgutachten von einer qualifizierten unabhängigen Prüfstelle vorzulegen. CIS Auditoren und Auditorinnen sind als zugelassene Prüfstelle für „Rechenzentren UZ 80“ auf der Website für das Österreichische Umweltzeichen gelistet.

WER DATEN SICHERN WILL, DARF DIE BASIS NICHT VERGESSEN: DAS RECHENZENTRUM.

www.cis-cert.com/rechenzentren

AUS- UND WEITERBILDUNG & PERSONENZERTIFIZIERUNG

SCHACHZUG FÜR IHRE KARRIERE

Die CIS-Lehrgänge vermitteln fundierte Fachkenntnisse „direkt vom Zertifizierungspartner“. Lernen und vertiefen Sie wie man Managementsysteme wirksam implementiert, betreibt und optimiert, zielgerichtet auditiert und wirksam kommuniziert. Die CIS-Lehrgänge behandeln zentrale Norminhalte, ihre Interpretation und Anwendung sowie Rechtsgrundlagen und Psychologie.
Alle Trainings sind auf Anfrage als individuelle Inhouse-Trainings buchbar.

CYBER LEADERS ACADEMY

CYBER LEADERS ACADEMY

KPMG, USTP – University of Applied Sciences St. Pölten und CIS Certification haben die Cyber Leaders Academy gegründet, um Unternehmen langfristig vor aktuellen und zukünftigen Cyberbedrohungen zu schützen. Maßgeschneiderte Schulungen bereiten Sie gezielt auf den richtigen Umgang mit Herausforderungen wie die der Cybersecurity, neuen gesetzlichen Vorgaben und innovativen Technologien vor.

LEHRGANGSREIHEN

- Information Security Manager nach ISO 27001
- Business Continuity Manager nach ISO 22301
- Artificial Intelligence Manager nach ISO 42001
- Information Security Auditor nach ISO 27001
- Business Continuity Auditor nach ISO 22301
- Artificial Intelligence Auditor nach ISO 42001

TRAININGS

- Data Protection Manager nach ISO 27701
- ISO 27001 und Cyber Security für Softwareentwickler*innen
- Refreshings für Information Security Manager, Information Security Auditoren, Business Continuity Manager
- Kompaktkurs Konfliktmanagement
- Kompaktkurs Datenschutz
- Data Protection Auditor nach ISO 27701

NISG 2026 / NIS-2 ANGEBOT

- NIS-2 Führungskräfteschulung
- Unabhängiger NIS Prüfer
- ISO 27001 & NIS-2 Lehrgang
- NIS-2 Grundlagenseminar

ANSPRECHPERSONEN

Stefanie Murguia
Head of Personenzertifizierung und Trainings
stefanie.murguia@cis-cert.com

Tina Hojsa
Personenzertifizierung und Trainings
trainings@cis-cert.com

Tamara Safranek
Personenzertifizierung und Trainings
trainings@cis-cert.com

Im Fall von besonderen Bedürfnissen, z. B. eingeschränkter Mobilität, wenden Sie sich an uns, wir helfen Ihnen gerne weiter.

trainings@cis-cert.com

Zur Übersicht
Trainings und Personenzertifizierungen

IHR WEG ZUM PERSONENZERTIFIKAT

CIS-TRAININGS BIETEN FACH-WISSEN „AUS ERSTER HAND“

Aufgrund der Akkreditierung gelten CIS-Personenzertifikate für Prüfungen als staatlich und offiziell anerkannte Dokumente mit internationalem Ansehen.

Trainer*innen und Referent*innen der CIS erfüllen die komplexen Ansprüche in der Informationssicherheit und im IT-Service Management durch hohe Fachkompetenz: Sie sind oder waren hauptberuflich in diesen Bereichen tätig und fungieren als Auditor*innen bei der Systemzertifizierung. So fließen viel Wissen und Erfahrung in die Lehrgangsinhalte ein. Auf diese Weise garantieren unsere Top-Trainer*innen praxisnahe Ausbildungen auf höchstem Niveau. Ein strategischer Schachzug für die Karriere.

QUALIFIKATIONS-CHECK

Zur Überprüfung der Konformität hinsichtlich Zertifizierungsprogramm und Aktualität der von Zertifikatswerber*innen beigebrachten Referenzen wird ein **Qualifikations-Check** durchgeführt. Dieser besteht aus der formalen Prüfung der Zugangsvoraussetzungen und optional aus einem mündlichen Fachgespräch.

ZULASSUNG ZU PRÜFUNGEN

Die **Zulassungsbedingungen** für jede Prüfung sind im jeweiligen CIS-Lehrgang angeführt.

Muster Personenzertifikat

Die **Anmeldung** zu einer Prüfung hat schriftlich bei der CIS zu erfolgen, wobei die Erfüllung der Zulassungsbedingungen durch den bzw. die Zertifikatswerber*in darzulegen ist. Sollte die Ausbildung im Rahmen der CIS-Lehrgänge absolviert worden sein, findet eine automatische Anerkennung statt, sofern mindestens 80% der Veranstaltungszeit pro Modul besucht wurde.

ANRECHNUNGEN

Sollte sich ein*e Zertifikatswerber*in andere Ausbildungen anrechnen lassen wollen, ist es erforderlich, ihre **Gleichwertigkeit zum Zertifizierungsprogramm** zu bestimmen. Zur Feststellung dieser ist ein gesonderter, schriftlicher Antrag zu stellen. Dem Antrag ist eine Darstellung über die absolvierten Ausbildungen und deren Vergleich mit den Anforderungen des Zertifizierungsprogramms beizulegen. Diese Anforderungen sind bei der Zertifizierungsstelle erhältlich.

CIS INHOUSE-TRAININGS

Zu den wirkungsvollsten Ausbildungsmethoden zählt das Lernen direkt im Unternehmen, gemeinsam mit Kolleg*innen und Führungskräften, anhand von aktuellen Beispielen aus der eigenen Branche.

Alle öffentlichen CIS-Trainings lassen sich 1:1 als Inhouse-Schulung buchen. Dies bringt vor allem für Großunternehmen Kostenvorteile, da Reisekosten, externe Räumlichkeiten, Catering und Ähnliches entfallen. Auch einzelne Lehrgangsmodule können als Inhouse-Schulung gebucht werden, sodass sämtliche Ausbildungsangebote direkt zu Ihnen kommen.

IHRE VORTEILE

- Maßgeschneiderte Unterstützung
- Kostengünstiger und effektiver durch Entfall von Reise- und Aufenthaltskosten
- Durch Teamarbeit mit gemeinsamen Ziel wird das firmeninterne Netzwerk nachhaltig gestärkt
- Unternehmensspezifische Herausforderungen werden adressiert, ohne dass firmeninternes Wissen nach außen dringt

ALLE TRAININGS AUCH
INHOUSE
BUCHBAR

INFORMATION SECURITY MANAGER NACH ISO 27001

ZENTRALE POSITIONEN IM UNTERNEHMEN, IN DER FÜHRUNGS- UND TECHNOLOGIEKOMPETENZ SIND GLEICHERMASSEN GEFRAGT.

Diese 4-tägige Ausbildung vermittelt Ihnen die Kompetenzen eines Information Security Managers. Diese Rollen nehmen eine jener zentralen Positionen im Unternehmen ein, in der Führungs- und Technologiekompetenz gleichermaßen gefragt sind. Sie betreiben eigenverantwortlich im Auftrag der obersten Leitung den Aufbau, die Implementierung sowie die ständige Verbesserung des Informationssicherheitsmanagementsystems (ISMS) und fungieren als Schnittstelle zwischen der obersten Führungsetage und allen Unternehmensbereichen.

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

MODULE

Entsprechend der hohen Anforderungen an Information Security Manager ist der Bogen der Ausbildungsinhalte weit gespannt. Die Ausbildung dauert 4 Tage und umfasst drei Module (auf Anfrage einzeln buchbar):

- **Die ISMS-Normen ISO 27001 und ISO 27002**: Informationssicherheit richtig implementieren und optimieren (2 Tage)
- **Rechtsgrundlagen für Information Security Manager**: Compliance (1 Tag)
- **Psychologische Grundlagen für Information Security Manager**: Von Mitarbeiter-Motivation bis zu Konfliktfähigkeit (1 Tag)
- **Prüfung**

ZERTIFIZIERUNG

CIS ist seit 2002 in Österreich für die Personenzertifizierung akkreditiert. Die von uns ausgestellten Zertifikate entsprechen somit staatlich und international anerkannten Standards.
Nach erfolgreicher Prüfung erhalten Sie das international anerkannte **Zertifikat „Information Security Manager nach ISO/IEC 27001“**, sofern Sie über mindestens zwei Jahre Berufserfahrung (innerhalb der letzten 3 Jahre) im Bereich Informationssicherheitsmanagement verfügen.
Falls Sie aktuell noch keine zwei Jahre Erfahrung nachweisen können, wird Ihnen das Zertifikat mit dem Status „Anwärter“ ausgestellt. Sobald die erforderliche Praxis vorliegt, schreiben wir Ihr Zertifikat kostenfrei um – einfach, unbürokratisch und als Ausdruck unseres Qualitätsanspruchs. Bitte beachten Sie: Der Anwärterstatus kann nicht verlängert werden.

INFORMATION SECURITY AUDITOR NACH ISO 27001

INTERNE AUDITS SELBST DURCHFÜHREN UND ZUR KONTINUIERLICHEN VERBESSERUNG BEITRAGEN.

Die Lehrgangsreihe zum Information Security Auditor ist die ideale Ergänzung für ausgebildete Information Security Manager.

Denn mit der Ausbildung zum Auditor können Sie alle internen Audits selbst durchführen und zur kontinuierlichen Verbesserung beitragen sowie ein Unternehmen mit Hilfe der im Kurs vermittelten Methoden optimal auf externe Audits vorbereiten.

Darüber hinaus können Sie bei entsprechender Berufserfahrung möglicherweise freiberuflich als CIS-Auditor tätig werden.

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

MODULE

Die Ausbildung zum Information Security Auditor dauert 4 Tage und besteht aus:

- **Audittechniken**: Interne Audits als mächtiges Instrument für die Systemverbesserung, 1 Tag)
- **Psychologische Grundlagen**: Zwischen Prüfer und Developer. Systemisch denken, wirksam kommunizieren (2 Tage)
- **Spezifikationsmodul zur Norm ISO 27001** (4. Tag, 2 Stunden, remote)
- **Prüfung** Information Security Auditor (4. Tag, 1 Stunde, remote)

ZERTIFIZIERUNG

Nach erfolgreicher Prüfung erhalten Sie das Zertifikat **„Information Security Auditor nach ISO/IEC 27001“**, sofern Sie über mindestens zwei Jahre Berufserfahrung (innerhalb der letzten 3 Jahre) im Bereich Informationssicherheitsmanagement verfügen und 4 Audits mit mindestens insgesamt 15 Audittagen im Bereich Informationssicherheit (inkl. Vor- und Nachbearbeitung, innerhalb der letzten 3 Jahre) vorweisen können.

Falls Sie aktuell noch keine zwei Jahre Erfahrung bzw. genügend Audittage nachweisen können, wird Ihnen das Zertifikat mit dem Status „Anwärter“ ausgestellt. Sobald die erforderliche Praxis vorliegt, schreiben wir Ihr Zertifikat kostenfrei um – einfach, unbürokratisch und als Ausdruck unseres Qualitätsanspruchs. Bitte beachten Sie: Der Anwärterstatus kann nicht verlängert werden.

BUSINESS CONTINUITY MANAGER NACH ISO 22301

AUF NOTFÄLLE UND KRISENSITUATIONEN VORBEREITET SEIN MIT BUSINESS CONTINUITY MANAGEMENT NACH ISO 22301.

Unternehmen stehen zunehmend vor der Herausforderung, auf Notfälle und Krisensituationen vorbereitet zu sein. Mit unserer Business Continuity Manager (BCM) Ausbildung erlangen Sie das notwendige Wissen und die Fähigkeiten, um Unternehmen sicher durch Krisen zu führen und die Geschäftskontinuität zu gewährleisten. Diese Schulung basiert auf den Anforderungen der ISO 22301 und vermittelt umfassende rechtliche, organisatorische und psychologische Grundlagen.
Innerhalb von 4 Tagen lernen Sie die wesentlichen Elemente des Business Continuity Managements kennen. Die Ausbildung kombiniert theoretisches Wissen, praktische Übungen und reale Szenarien, um Sie optimal auf Ihre Rolle als BCM-Manager vorzubereiten.

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

MODULE

- **Rechtlichen Grundlagen**: Überblick über nationale und internationale Vorschriften (einschließlich der DSGVO und IT-Sicherheitsgesetze), Übungen: Brainstorming zu den Anforderungen in Unternehmen
- Einführung Risikomanagement
- Einführung in Business Continuity Management
- ISO 22301 – Anforderungen und Umsetzung
- **Krisenübungen und Szenarien**: Praxisnahe Übungen zur Bewältigung von Notfällen.
- Psychologie im Zusammenhang mit Druck und Stress in Krisensituationen
- **Prüfung**

Die Ausbildung bietet eine Kombination aus verschiedenen Lehrmethoden, um Theorie und Praxis ideal zu verbinden: Vorlesungen und Präsentationen, Workshops, Krisensimulationen, Fallstudien und Rollenspiele, Notfallübung.

Nach erfolgreicher Prüfung erhalten Sie das Zertifikat **„Business Continuity-Manager nach ISO 22301“**. Details dazu finden Sie im Web.

BUSINESS CONTINUITY AUDITOR NACH ISO 22301

DIE AUSBILDUNG ZUM BUSINESS CONTINUITY-AUDITOR IST DIE IDEALE ERGÄNZUNG FÜR AUSGEBILDETE BUSINESS CONTINUITY-MANAGER.

Mit der Ausbildung zum Business Continuity-Auditor können Sie alle internen Audits selbst durchführen und zur kontinuierlichen Verbesserung beitragen sowie ein Unternehmen mit Hilfe der im Kurs vermittelten Methoden optimal auf externe Audits vorbereiten.

Darüber hinaus können Sie bei entsprechender Berufserfahrung möglicherweise freiberuflich als CIS-Auditor tätig werden.

MODULE

Die Ausbildung zum Business Continuity-Auditor dauert 4 Tage und besteht aus:

- **Audittechniken**: Interne Audits als mächtiges Instrument für die Systemverbesserung (1 Tag)
- **Psychologische Grundlagen**: Zwischen Prüfer und Developer. Systemisch denken, wirksam kommunizieren. (2 Tage)
- **Spezifikationsmodul zur Norm ISO 22301** (4. Tag, 2 Stunden, remote)
- **Prüfung** zum „Business Continuity-Auditor nach ISO 22301“ (4. Tag, 1 Stunde, remote)

Nach erfolgreicher Prüfung erhalten Sie das Zertifikat **„Business Continuity-Auditor nach ISO 22301“**, sofern Sie die entsprechenden Voraussetzungen nachweisen können. Details dazu finden Sie im Web.

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

MODULARE ERWEITERUNG FÜR AUDITOREN

Nach Besuch des 3-tägigen Grundkurses besuchen Sie das bzw. die gewählten Spezifikationsmodule zu den Themen Informationssicherheitsmanagementsysteme, Artificial Intelligence, Business Continuity Management und Data Protection und schließen mit der jeweiligen Zertifizierungsprüfung ab. Hinweis: Bitte beachten Sie die jeweiligen Teilnahmevoraussetzungen zur Prüfung – sollten Sie diese zum Zeitpunkt der Prüfung nicht erfüllen, können Sie den Kurs (inkl. Spezifikationsmodul) trotzdem besuchen und erhalten eine Teilnahmebestätigung.

ARTIFICIAL INTELLIGENCE MANAGER NACH ISO 42001

AM PULS DER ZEIT BLEIBEN MIT AI-MANAGEMENT NACH ISO/IEC 42001

Die rapide Etablierung von KI-Systemen stellt Unternehmen vor noch nie dagewesene Herausforderungen. Wer KI nicht nutzt, wird langfristig keine Chance gegen Konkurrent*innen und Mitbewerber*innen haben. Dennoch stellt Künstliche Intelligenz auch ein massives Risiko dar, vor allem im Bereich Datenschutz und Informationssicherheit.

Die CIS hat als Vorreiterin auf diesem Gebiet das erste ISO 42001 Zertifikat an ein österreichisches Unternehmen verliehen. Mit unserer Ausbildung erhalten Sie sowohl das nötige Know-how für eine sichere und effiziente Implementierung eines KI-Managementsystems als auch die Anerkennung Ihrer Kompetenz durch ein CIS Zertifikat – ein starkes Signal an Kund*innen und Geschäftspartner*innen.

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

MODULE

Innerhalb von 3 Tagen lernen Sie die wesentlichen Elemente der Norm ISO/IEC 42001, der Implementierung eines KI Managementsystems sowie die rechtlichen Grundlagen und deren praktische Umsetzung. Der Kurs kombiniert topaktuelles Know-how mit Praxisübungen, um Sie optimal auf Ihre Rolle als AI-Manager vorzubereiten. Die Schwerpunkte liegen auf:

- **Norm ISO 42001:** Einführung und detailliertes Verständnis der neuen Norm, die den Einsatz von KI in Unternehmen regelt.
- **Rechtsgrundlagen:** Überblick über die rechtlichen Rahmenbedingungen und Regularien, die für den verantwortungsvollen Umgang mit KI relevant sind.
- **Ethik und Risikomanagement:** Wie Sie ethische Fragen im Zusammenhang mit KI bewerten und Risiken im Umgang mit dieser Technologie effizient managen.
- **Praxisbezug:** Wie gehe ich vor, um KI wertstiftend und erfolgreich in meinem Unternehmen einzusetzen.
- **Prüfung**

Nach erfolgreichem Absolvieren der Abschlussprüfung erhalten Sie das Zertifikat **„Artifical Intelligence-Manager nach ISO/IEC 42001“**. Details dazu finden Sie im Web.

ARTIFICIAL INTELLIGENCE AUDITOR NACH ISO 42001

DIE AUSBILDUNG ZUM ARTIFICIAL INTELLIGENCE AUDITOR IST DIE IDEALE ERGÄNZUNG FÜR AUSGEBILDETE ARTIFICIAL INTELLIGENCE MANAGER.

Mit der Ausbildung zum Artificial Intelligence Auditor können Sie alle internen Audits selbst durchführen und zur kontinuierlichen Verbesserung beitragen sowie ein Unternehmen mit Hilfe der im Kurs vermittelten Methoden optimal auf externe Audits vorbereiten. Darüber hinaus können Sie bei entsprechender Berufserfahrung möglicherweise freiberuflich als CIS-Auditor tätig werden.

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

MODULE

Die Ausbildung zum Artificial Intelligence-Auditor dauert 4 Tage und besteht aus:

- **Audittechniken**: Interne Audits als mächtiges Instrument für die Systemverbesserung (1 Tag)
- **Psychologische Grundlagen:** Zwischen Prüfer und Developer. Systemisch denken, wirksam kommunizieren (2 Tage)
- **Spezifikationsmodul zur Norm ISO/IEC 42001** (4. Tag, 2 Stunden, remote)
- **Prüfung** zum „Artifical Intelligence-Auditor nach ISO/IEC 42001“ (4. Tag, 1 Stunde, remote)

Nach erfolgreichem Absolvieren der Abschlussprüfung erhalten Sie das Zertifikat **„Artifical Intelligence-Auditor nach ISO/IEC 42001“**, sofern Sie die entsprechenden Voraussetzungen nachweisen können. Details dazu finden Sie im Web.

MODULARE ERWEITERUNG FÜR AUDITOREN

Nach Besuch des 3-tägigen Grundkurses besuchen Sie das bzw. die gewählten Spezifikationsmodule zu den Themen Informationssicherheits-Managementsysteme, Artificial Intelligence, Business Continuity Management und Data Protection und schließen mit der jeweiligen Zertifizierungsprüfung ab. Hinweis: Bitte beachten Sie die jeweiligen Teilnahmevoraussetzungen zur Prüfung – sollten Sie diese zum Zeitpunkt der Prüfung nicht erfüllen, können Sie den Kurs (inkl. Spezifikationsmodul) trotzdem besuchen und erhalten eine Teilnahmebestätigung.

NISG 2026 – NIS-2

NIS-2 FÜHRUNGSKRÄFTE-SCHULUNG

Für Führungskräfte wie Geschäftsführer*innen, Inhaber*innen und Risikoverantwortliche bringt die Europäische NIS-2-Richtlinie nicht nur ein erhöhtes Haftungsrisiko mit sich, sondern auch die gesetzliche Verpflichtung, sich im Bereich Cybersicherheit fortzubilden.
Wir bieten diese maßgeschneiderte Schulung mit Expert*innen aus der Praxis an, um Ihnen auf Augenhöhe in Kürze die wichtigsten Kernhinhalte und Handlungspunkte zu vermitteln.

Dauer: 2 Stunden

UNABHÄNGIGER NIS PRÜFER

Als Absolvent*in dieses Lehrgangs verstehen Sie den rechtlichen Aufbau und die Grundlagen einer NISG 2026-Prüfung und können NISG 2026-konforme Prüfungen selbstständig durchführen. Sie verstehen den inhaltlichen Zusammenhang zwischen den rechtlichen Anforderungen, der Informationssicherheit, Prüfhandlung und dem Prüfbericht.

ZIELGRUPPE

CISOs, IT-Prüfer*innen, interne Revision sowie NIS-Berater*innen, die sich optimal auf eine NIS-Prüfung vorbereiten oder durchführen wollen.

INHALTE

- Wissensaufbau über aktuelle rechtliche Grundlagen (NISG 2026, CRA)
- Produkt- und Organisationsrecht (Lieferantenmanagement)
- Richtiger Umgang mit Lieferanten (intern u. extern) - CRA
- Durchführung von Audits
- Erstellung eines rechtskonformen Prüfberichts
- Ablauf Behördenverfahren
- Ablauf Prüfverfahren – Tipps direkt aus der Auditpraxis
- Weiterführende Rahmenwerke zur Erfüllung des NISG 2026 (Stand der Technik)
- Synergieeffekte mit der ISO 27001 für NISG-Prüfung nutzen

PRÜFUNG

Im Anschluss an den Lehrgang findet die Prüfung zum*zur unabhängigen NIS-Prüfer*in statt. Dauer: 1 Stunde.

VORAUSSETZUNGEN

mind. 2-jährige Berufserfahrung im Bereich Cybersecurity und/oder im Rechtsbereich.

Dauer: 2,5 Tage

ISO 27001 & NIS-2 LEHRGANG: DER STRUKTURIERTE EINSTIEG IN EU-CYBERSECURITY

Als Absolvent*in dieses Lehrgangs kennen Sie die Prozesse und Normanforderung zur Implementierung der ISO 27001 und ISO 27002 und können diese praktisch anwenden.
Es werden die Grundlagen der Informationssicherheit und auch übergeordnete Aspekte wie Organisation, Technik oder Prozessmanagement behandelt. Mittels Fallbeispielen werden die Teilnehmenden an die selbstständige Umsetzung des Gelernten herangeführt. Darüber hinaus wird der Standard auch mit anderen Ansätzen zum Thema Informationssicherheit verglichen sowie auf mögliche Weiterentwicklungen der Norm selbst bzw. der Normenreihe eingegangen.
Dieses Seminar vermittelt weiters die zentralen Grundlagen von NIS-2 und zeigt praxisnah, wie Organisationen die Anforderungen effizient und nachhaltig umsetzen können. Der Fokus liegt auf den Kernmaßnahmen der NIS-2, dem Risikomanagementansatz der ENISA sowie den zentralen Pflichten für „wesentliche“ und „wichtige“ Einrichtungen.

Dauer: 3 Tage

NIS-2 GRUNDLAGENSEMINAR – KOMPAKT, PRAXISNAH, ENISA-KONFORM

Die neue NIS-2-Richtlinie stellt Unternehmen vor weitreichende Herausforderungen im Bereich Cybersecurity, Governance und Compliance. Dieses Seminar vermittelt die zentralen Grundlagen von NIS-2 und zeigt praxisnah, wie Organisationen die Anforderungen effizient und nachhaltig umsetzen können. Der Fokus liegt auf den Kernmaßnahmen der NIS-2, dem Risikomanagementansatz der ENISA sowie den zentralen Pflichten für „wesentliche“ und „wichtige“ Einrichtungen.
Teilnehmende erhalten einen klar strukturierten Überblick über:

- die regulatorischen Anforderungen und Umsetzungsfristen
- Risikomanagement und Sicherheitsmaßnahmen nach ENISA Best Practices
- Incident Reporting, Haftung und Governance Vorgaben
- praktische Schritte zur Vorbereitung auf Audits und Kontrollen

Das Seminar richtet sich an Führungskräfte, IT Verantwortliche, Compliance Beauftragte und Organisationen, die sich kompakt und verständlich auf die Anforderungen der NIS-2 Richtlinie vorbereiten möchten.

Dauer: 1 Tag

Alle Termine und weitere Details finden Sie online.
www.cis-cert.com/trainings

Hinweis
Preis- bzw. Produktänderungen und Druckfehler vorbehalten. Die Angaben in Bezug auf Gesetze, Normen und Richtlinien beziehen sich auf den Stand der Drucklegung.

Allgemeine Geschäftsbedingungen
Die Allgemeinen Geschäftsbedingungen der CIS für den Bereich Personenzertifizierung und Aus- und Weiterbildung finden Sie immer in der letztgültigen Fassung auf unserer Website unter **www.cis-cert.com/agb.**

TRAININGS & REFRESHINGS

KOMPAKTKURS DATENSCHUTZ

Innerhalb eines Tages lernen Sie Praxisbeispiele von einem der renommiertesten Datenschutzverantwortlichen des Landes, die Sie umgehend in Ihrem Unternehmen anwenden können. Das stärkt den Datenschutz in Ihrem Unternehmen und Ihre Position als Expert*in, der/die neue Trends mit Voraussicht in Geschäftsprozesse einbindet.

Dauer: 1 Tag

DATA PROTECTION MANAGER NACH ISO 27701

Mit der neuen Fassung der ISO 27701 ist das Datenschutz-Managementsystems (DSMS) unabhängig von der ISO 27001 zertifizierbar. Der Kurs setzt Kenntnisse über DSGVO und ihre Anforderungen voraus und zeigt effiziente Möglichkeiten auf, um ein zertifizierbares DSMS auf Basis der ISO 27701 aufzubauen.

ZIELGRUPPE

Datenschutzbeauftragte, AI-Manager, Compliance-Beauftragte, Interessierte

INHALTE

Der eintägige Workshop vermittelt zertifizierten Datenschutzbeauftragten in kompakter Form das strukturierte Fachwissen, um ISO 27701 im eigenen Unternehmen oder in der Behörde richtig einzuordnen und anzuwenden. Im Mittelpunkt stehen der Aufbau und Betrieb eines (DSMS) sowie das konkrete Mapping zur DSGVO.
Die Teilnehmenden lernen die ISO-Normenfamilie und das High-Level-Structure-Prinzip als Basis kennen, arbeiten sich durch alle relevanten Kapitel der Norm und wenden die Maßnahmenkataloge auf ihre eigene Praxis an.
Die Schulung richtet sich an Datenschutzbeauftragte mit DSGVO-Vorwissen, die ISO 27701 fachlich fundiert in bestehende Compliance-Strukturen integrieren wollen.

Dauer: 1 Tag

DATA PROTECTION AUDITOR NACH ISO 27701

Mit der Ausbildung zum Data Protection Auditor“ können Sie alle internen Audits selbst durchführen und zur kontinuierlichen Verbesserung beitragen sowie ein Unternehmen mit Hilfe der im Kurs vermittelten Methoden optimal auf externe Audits vorbereiten.
Darüber hinaus können Sie bei entsprechender Berufserfahrung möglicherweise freiberuflich als CIS-Auditor tätig werden.

Dauer: 4 Tage

REFRESHINGS

Unser Angebot umfasst Refreshings für „Information Security Manager“ und „Information Security Auditor“ sowie „Business Continuity Manager“.
Praxisnahe Fallbeispiele und Anforderungen gemäß ISO 27001 aus dem eigenen Arbeitsbereich werden zielgerichtet diskutiert. Der Refresher-Kurs umfasst dementsprechend neben Wissensaktualisierung auch Erfahrungsaustausch und Tipps für die Praxis.

VORAUSSETZUNGEN (VERLÄNGERUNG ZERTIFIKATE)

- Für alle Zertifikate: Nachweis über 2 Jahre Berufspraxis im Bereich Informationssicherheitsmanagement innerhalb der letzten 3 Jahre
- Für das Zertifikat „Auditor*in“ zusätzlich: 4 durchgeführte/begleitete IS-Audits mit insgesamt mind. 15 Audittagen (inkl. Vor- und Nachbearbeitung) innerhalb der letzten 3 Jahre
- Anwärter Status kann nicht verlängert werden

Details dazu finden Sie im Web.

Dauer: 2 Tage

ISO 27001 UND CYBER SECURITY FÜR SOFTWAREENTWICKLER*INNEN

Dieses individuelle Spezialtraining vermittelt den Teilnehmenden die Grundlagen der Normen ISO 27001/ISO 27002 – den Fundamenten für moderne Informationssicherheitsmanagementsysteme.

Dauer: 2 Tage

KOMPAKTKURS KONFLIKTMANAGEMENT

In diesem eintägigen Seminar lernen die Teilnehmer*innen wirksame Strategien zur Konfliktbearbeitung kennen, die sie sofort in ihrem Arbeitsumfeld anwenden können.

INHALTE

- Persönlicher Konfliktstil, persönliche Konfliktbiografie
- Prägung des individuellen und sozialen Konfliktverhaltens (persönliche Kompetenz, professionelle Haltung und Rollenverständnis)
- Bearbeitung persönlicher Konfliktszenarien
- Handlungsstrategien zur Konfliktbewältigung

Dauer: 1 Tag

SECURE YOUR BUSINESS

CIS – Certification & Information Security Services GmbH

office@cis-cert.com
Salztorgasse 2/3/7
1010 Wien, Austria
Tel.: +43 1 532 98 90

www.cis-cert.com

Hinweis
Alle personenbezogenen Bezeichnungen in dieser Broschüre beziehen sich in gleicher Weise auf jedes Geschlecht. CIS Certification behält sich Änderungen hinsichtlich ihrer Produkte vor. Die Angaben in Bezug auf Gesetze, Normen und Richtlinien beziehen sich auf den Stand der Drucklegung. Wir bitten um Verständnis.

Impressum
Für den Inhalt verantwortlich: CIS - Certification & Information Security Services GmbH. Fehler und Änderungen vorbehalten.
Ausgabe: August 2026

Dok.nr.: CIS-M002_Portfolio_202308 | Ausgabe: 08/2026