Leistungsportfolio

SECURITY | PRIVACY | CONTINUITY

www.cis-cert.com

Inhalt

Inhalt 2

Unsere Mission 3

CIS Facts 4

Ihre Vorteile 5

CIS Community 6

Ihr Weg zum Systemzertifikat 8

Informationssicherheit 9

Datenschutz 9

Cloud Computing 10

Energiewirtschaft 10

Überprüfung nach NISG 11

Business Continuity Management 11

Service Management 12

Rechenzentren 12

Blockchain Assessment 13

TISAX® Assessment 13

Ihr Weg zum Personenzertifikat 15

Information Security Manager nach ISO 27001 16

Information Security Auditor nach ISO 27001 17

Seminare/Refreshings/Webinare 18

Service 19

Liebe Leser und Leserinnen,

als akkreditierte Zertifizierungspartnerin ist CIS auf Informationssicherheit, Datenschutz, Cloud Computing, IT Service Management, Rechenzentren sowie auf Business Continuity Management spezialisiert.

STELLEN SIE IHR BEKENNTNIS ZUR INFORMATIONSSICHERHEIT ZUR SCHAU

Ob Sie es für Kund*innen, Geschäftspartner*innen, zum Wettbewerbsvorteil oder aus innerer Überzeugung tun: Nichts ist so aussagekräftig wie ein Zertifikat, basierend auf einer unabhängigen Prüfung durch ein akkreditiertes Unternehmen, wie der CIS – Certification & Information Security Services GmbH.

Der digitale Wandel und technologische Fortschritt verändern Unternehmen, die Gesellschaft, Privatpersonen und die Wissenschaft. Sie bringen neue Chancen und Möglichkeiten, aber auch ein erhöhtes Bedrohungspotenzial mit breit gestreuter Wirkung. Was bei all der Veränderung immer sichergestellt werden sollte: Datenschutz und Informationssicherheit!

Unser langjährig erfahrenes Team aus Auditoren und Auditorinnen sorgt dafür, dass CIS Audits qualitativ hochwertig und immer mit Fokus auf Mehrwert für Ihre Organisation durchgeführt werden. Durch die Akkreditierung nach ISO 17021-1 sind CIS-Systemzertifikate als objektiver Nachweis international anerkannt.

KOMPETENZ IM FOKUS

In unseren praxisorientierten Ausbildungen vermitteln wir Ihnen, worauf es bei Informationssicherheit, Cybersecurity und Datenschutz ankommt. Die eingesetzten Vortragenden kommen direkt aus der Praxis und bringen erprobtes Wissen und jahrelange Erfahrung in die Lehrgangsinhalte. Aufgrund der Akkreditierung nach ISO 17024 gelten CIS-Personenzertifikate als staatlich und offiziell anerkannte Dokumente mit internationalem Ansehen. Ein Schachzug für Ihre Karriere, der sich bezahlt macht!

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

Secure Your Business!

Harald Erkinger
Geschäftsführer CIS

Unsere Mission

WOFÜR WIR STEHEN

Die **CIS – Certification & Information Security Services GmbH** ist ein österreichisches Dienstleistungsunternehmen und 100%ige Tocher der Quality Austria - Trainings, Zertifizierungs und Begutachtungs GmbH. Die CIS hat ihren Ursprung im Bereich der **Zertifizierung von Managementsystemen und der Zertifizierung von Personen**. Für beide Dienstleistungsbereiche ist sie vom Bundesministerium für Arbeit und Wirtschaft (BMAW) bzw. der Akkreditierung Austria als Zertifizierungsstelle akkreditiert. Darüber hinaus ist die CIS zusätzlich durch die internationalen 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 akkreditierte Zertifizierungspartnerin ist die 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

Die 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 Kunden und Kundinnen der CIS erfolgt unbeeinflusst und unabhängig von Beratungsorganisationen, Wettbewerbsunternehmen oder sonstigen einflussnehmenden Interessensgruppen. Die 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

Die 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

Die 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

Die 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-Auditor*innen im Rahmen des Zertifizierungsablaufs direkt ein. Darüber hinausgehende Zusatzleistungen auf dem Gebiet der Beratung werden aus Gründen der Unparteilichkeit nicht angeboten.

CIS 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 für die **Systemzertifizierung** sowie
- ISO/IEC 17024 für die **Personenzertifizierung**
- ISO/IEC 17065 für **Produktzertifizierung** (ab Herbst 2023).

WELTWEITE GÜLTIGKEIT

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

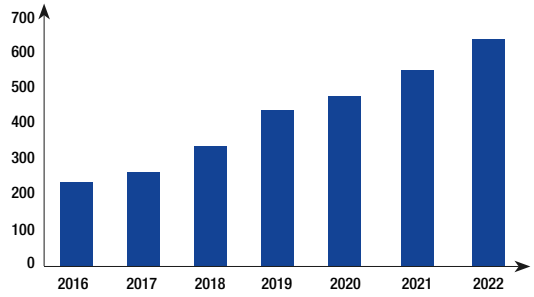
MITARBEITER*INNEN

8 Mitarbeiter*innen (Österreich)

170 Netzwerkpartner*innen
Österreich und International

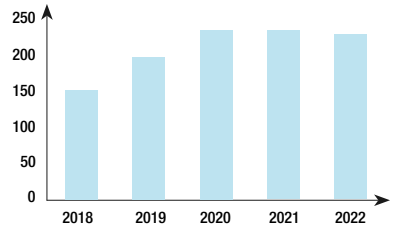
AUSGESTELLTE SYSTEMZERTIFIKATE

Österreich & International



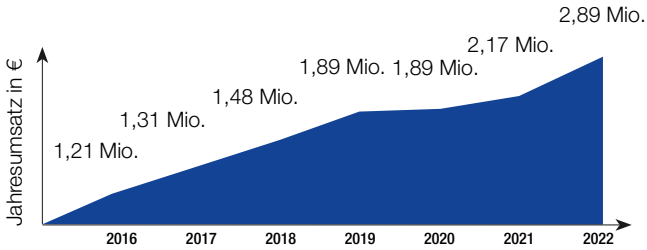
AUSGESTELLTE PERSONENZERTIFIKATE

Österreich & International



UMSATZ 2022

€ 2,89 MIO.



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 200 Gleichgesinnten inklusive. Seit 2023 gehen wir auch einen internationalen Schritt weiter mit einer Simultan-Übersetzung auf Englisch.

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

www.cis-cert.com/summit

Ihre Vorteile

KUND*INNENNUTZEN

Die CIS bietet als regionale und internationale Zertifizierungspartnerin 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 die CIS 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!

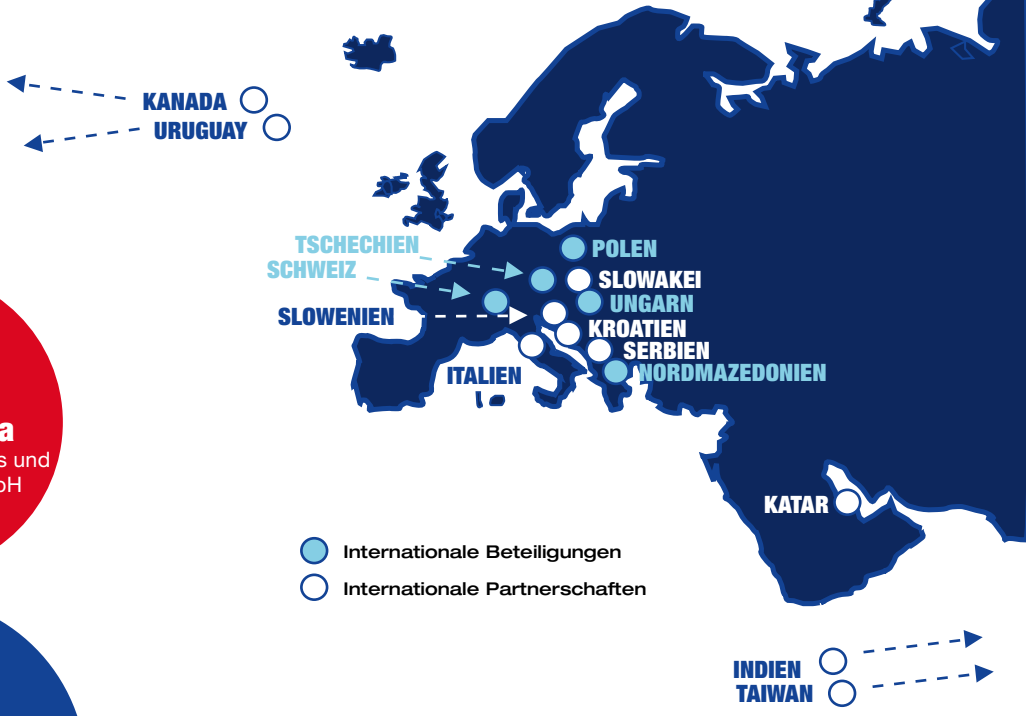
UNSERE KERNKOMPETENZEN

- Security
- Privacy
- Continuity
- IT-Services
- Rechenzentren

12 Fakten
warum sich eine Zertifizierung mit uns lohnt

1. Erhöhte Kund*innenzufriedenheit
2. Gesteigerte Wettbewerbsfähigkeit
3. Optimierte Prozesse
4. Realisierbarer Imagegewinn
5. Kostenreduktion und Investitionsschutz
6. Förderung der Mitarbeiter*innenmotivation
7. Fokussierte Zielerreichung
8. Minimierung von Fehlern
9. Praxisorientiertes Risikomanagement
10. Verstärkte Profitabilität
11. Verbesserte Rechtssicherheit
12. Steigerung des Marktwertes

Community



Quality Austria
Trainings, Zertifizierungs und Begutachtungs GmbH

CIS
Certification & Information Security Services 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 Nordmazedonien
Macedonia Certification & Information Security Services d.o.o.
CIS Anteil 58% | **CEO**: Georgi Milev

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

Die CIS – Certification & Information Security Services GmbH ist eine 100%ige Tochter der Quality Austria – Trainings, Zertifizierungs und Begutachtungs GmbH. Unsere Kund*innen profitieren von unseren **quality**austria Kooperationen z. B. im Bereich Integriertes Managementsystem und Digital Economy.

TOCHTERGESELLSCHAFTEN

CIS ist als internationaler Player mit Gesellschaften mit Mehrheitsbeteiligung in 5 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.

SCHWESTERGESELLSCHAFTEN

- LSQA Uruguay
- QA Center Belgrad
- Quality Austria Polska
- Quality Austria Adriatic
- Shanghai OQS International (China)
- Quality Austria Central Asia
- Betriebsstätte Tschechien
- QMD Services

PARTNERGESELLSCHAFTEN

- SIQ Slovenian Institue for Quality and Metrology, Ljubljana, Slovenia
- Quality Austria Adriatic d.o.o., Zagreb, Croatia
- Quality Austria Center d.o.o., Belgrade, Serbia
- Quality Italia S.r.l. Roma, Italia
- Quality Austria Certification Gulf, W.L.L. Doha, Qatar
- Quality Austria Central Asia, New Delhi, India
- TCIC Ltd. Surrey, B.C., Canada

SYSTEMZERTIFIZIERUNG

Als Ihre professionelle Zertifizierungspartnerin ist die CIS auf Informationssicherheit, Datenschutz, Cloud Computing, IT-Services, Rechenzentren sowie auf Business Continuity Management spezialisiert.

INFORMATIONSSICHERHEIT
- ISO 27001: Informationssicherheit mit System S. 9

DATENSCHUTZ
- ISO 27701: Zertifikat für Datenschutz- und Informationssicherheit S. 9

CLOUD COMPUTING
- ISO 27018 für Cloud Privacy und Schutz für Personendaten S. 10

ENERGIEWIRTSCHAFT
- ISO 27019: Informationssicherheitsmaßnahmen für die Energieversorgung S. 10

ÜBERPRÜFUNG NACH NISG
- Überprüfung nach dem Netz- und Informationssystemsicherheitsgesetz (NISG) S. 11

BUSINESS CONTINUITY
- ISO 22301: Business Continuity statt „Blackout“ S. 11

SERVICE MANAGEMENT
- ISO 20000-1: Qualität & Effizienz von IT-Services S. 12

RECHENZENTREN
- EN 50600: Einrichtungen & Infrastrukturen von Rechenzentren – Data Center Design S. 12

BLOCKCHAIN ASSESSMENT S. 13

TISAX® ASSESSMENT S. 13

ANSPRECHPARTNER SYSTEMZERTIFIZIERUNG

Robert Jamnik
Head of Audit Services
Lead Auditor ISO 20000, ISO 27001
und NISG-Überprüfungen
r.jamnik@cis-cert.com

Ihr Weg zum Systemzertifikat

CIS-RECERTIFICATION-AUDIT
Nach **3 Jahren** kann das abgelaufene Zertifikat erneuert werden.

Muster Systemzertifizierung

CIS-SURVEILLANCE-AUDIT
Das **einmal pro Jahr** durchgeführte Surveillance-Audit überprüft die Effektivität des gesamten Managementsystems sowie seine ständige Verbesserung.

CIS-LICENCE
Mit der „**Certificate Issuance & Right to Use Licence**“ erwerben Sie das 3 Jahre gültige CIS-Zertifikat.

CIS-CERTIFICATION-AUDIT
Die CIS-Auditor*innen überprüfen das implementierte Managementsystem durch multiple Stichproben auf verschiedenen Ebenen.
Der **Auditbericht** zeigt Verbesserungspotenziale auf.

CIS-SYSTEM-&-RISK-REVIEW (Vorbegutachtung)
Mängel und Verbesserungspotenziale zur Norminterpretation und Dokumentation werden in einem Kurzbericht festgehalten. Diese Vorbegutachtung dient als „**Generalprobe**“ vor dem Zertifizierungsaudit.

CIS-STAGE-REVIEW (freiwillige Vorbeurteilung)
Auf Wunsch werden die implementierten System-Elemente überprüft und ein **Stärken-Schwächen-Profil** erstellt.

IMPLEMENTIERUNG
Einführung von **Maßnahmen** nach entsprechender Norm. CIS als unabhängige Prüfstelle ist nicht involviert.

INFORMATION
Ein **Erstgespräch** liefert Details zum Prozess. Es folgen Registrierung und Projektplanung.

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

ISO 27001

Der Standard ISO 27001 für Informationssicherheit verbucht weltweit einen exponentiell wachsenden Anwenderkreis: Im Jahr 2019 waren knapp 40.000 Unternehmen verschiedenster Branchen und Größen zertifiziert – von KMU bis zu multinationale Unternehmen, da ISO 27001 durch den integrierten Risikoansatz flexibel einsetzbar ist.

ÜBERBLICK

Relevant ist die ISO 27001 vor allem dadurch, dass sie einen systematischen und risikobasierten Ansatz bietet, der die Informationssicherheitsrisiken sichtbar und damit steuerbar macht. Digitalisierung, Komplexität, steigende Abhängigkeit von Informationsverarbeitungsprozessen und die gleichzeitige Professionalisierung der internationalen Cyber-Kriminalität führen dazu, dass der Stellenwert von „sicherer" Informationsverarbeitung kontinuierlich steigt.

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 Information 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 vorgegebenem Zertifizierungsablauf in der ISO 27001 Zertifizierung. Informationen zu den Projektphasen und dem Ablauf der Zertifizierung finden Sie auf Seite 8.

HÖCHSTER SCHUTZ VON SENSIBLEN DATEN UND UNTERNEHMENSKRITISCHEN INFORMATIONEN

www.cis-cert.com/informationssicherheit

Datenschutz

INTEGRIERTER ANSATZ AUF BASIS VON ISO 27001 UND ISO 27701

Die Norm ISO 27701 dient zum Nachweis eines eingeführten und wirksamen Datenschutzmanagementsystems und 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. Aufgrund der inhaltlichen Nähe zur Informationssicherheit kann bei der neuen Datenschutzerweiterung auf vorhandene Systeme und Strukturen aufgebaut werden. 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. Informationen zu den Projektphasen und dem Ablauf der Zertifizierung finden Sie auf Seite 8.

OBJEKTIVER NACHWEIS FÜR DSGVO-ORIENTIERTEN DATENSCHUTZ

www.cis-cert.com/datenschutz

Cloud Computing

ISO 27018

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

ÜBERBLICK

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 bei Dienstleistungs- oder Auftragsverarbeitungsunternehmen – sicherstellen. Dies muss durch geeignete Verträge sowie Prüfungen und Nachweise erfolgen!

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

ZERTIFIZIERUNG

Eine Cloud-Zertifizierung nach diesen Normen ist dann möglich, wenn bereits eine Basis-Zertifizierung nach ISO 27001 für Informationssicherheit für denselben Geltungsbereich innerhalb der Organisation realisiert wurde. Informationen zu den Projektphasen und dem Ablauf der Zertifizierung finden Sie auf Seite 8.

DATENSCHUTZ UND SERVICEQUALITÄT ALS STARKES SIGNAL AN IHRE KUND*INNEN

www.cis-cert.com/cloud-computing

Energiewirtschaft

ISO 27019

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

IHRE VORTEILE

- Internationale Anerkennung
- Weiterentwicklung Ihrer Sicherheitsmaßnahmen
- Leichte Integration in bestehendes ISMS
- Zielgerichtete Weiterentwicklung der bereits vorhandenen Sicherheitsmaßnahmen zum Schutz von Systemen der Energieversorgung im Unternehmen.

ZERTIFIZIERUNG

Die ISO 27019 baut auf der ISO 27001 und ISO 27002 auf und lässt sich in ein bestehendes Infomationssicherheitssystem nach ISO 27001 integrieren. Ist ein solches noch nicht vorhanden, kann aber auch zeitgleich eine ISO 27019 wie auch ISO 27001 Zertifizierung beantragt werden.

ENWG §11 1A UND ENWG §11 1B

Gesetzeskonformität und Impulse zur Weiterentwicklung der Sicherheit von Energieversorgungsnetzen und Energieanlagen. 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*innen von Energieversorgungsnetzen und/oder Energieanlagen, die unter dieses Gesetz fallen, sind verpflichtet eine entsprechende Umsetzung durch ein akkreditiertes Unternehmen nachzuweisen.

ZERTIFIZIERUNG

Die CIS ist nach EnWG §11 1a und 1b akkreditiert und kann für Sie eine Zertifizierung als Nachweis einer gesetzeskonformen Umsetzung nach EnWG §11 1a und 1b durchführen. Die Zertifikate dienen bei den Behörden als Nachweis einer gesetzeskonformen Umsetzung der Anforderungen aus dem EnWG §11 1a und 1b.

GESETZESKONFORMITÄT UND IMPULSE ZUR WEITERENTWICKLUNG

www.cis-cert.com/energiewirtschaft

Überprüfung nach NISG

NIS-GESETZ UND ISO 27001 IM KOMBI-AUDIT:

Zum Schutz kritischer Infrastruktur in Bereichen wie Energie, Verkehr oder Finanzen trat im Juli 2019 das NIS-Gesetz für Netz- und Informationssystemsicherheit (NISG) als nationale Umsetzung der EU-NIS-Richtlinie in Kraft. Im Dezember 2022 wurde bereits die 2. Version der NIS-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union verabschiedet.

ÜBERBLICK

Mit einer deutlichen Erweiterung der betroffenen Branchen und eine Absenkung der Kriterien ab wann ein Unternehmen betroffen ist, wird eine neue Ära im Bereich der Cybersicherheit eingeleitet. NIS 2.0 muss ab Oktober 2024 in Österreich umgesetzt werden. Die Anzahl von Cyber-Angriffen, ebenso wie die Schutzanforderungen, werden weiter steigen. Entsprechend umfassend fordert die NISG Sicherheitsmaßnahmen, die aufgrund von Risikoanalysen einzuführen und mittels kontinuierlichem Verbesserungsprozess auf dem neuesten Stand der Technik zu halten sind. Inhaltlich fordert die NISG zu mehr als 80 Prozent deckungsgleiche Sicherheitsmaßnahmen wie die internationale Norm für Informationssicherheit ISO 27001.

IHRE VORTEILE

- Schutz für kritische Infrastruktur
- Nutzen von Synergien
- Minimieren Sie das Risiko für Störungen
- Sehr gut mit bestehender Zertifizierung nach ISO 27001 vereinbar

NACHWEIS DER GESETZESKONFORMITÄT

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

Unternehmen, die bisher schon ein zertifiziertes Managementsystem nach ISO 27001 auf hohem Niveau betrieben haben, können mit relativ geringem Aufwand NISG-konform gemacht werden. Beide Regelwerke können in einem Kombi-Audit effizient geprüft werden. Für Organisationen, die vor der Überprüfung auf Nummer sicher gehen wollen, führt die CIS auf Wunsch **Delta-Audits** durch, die einen notwendigen Lückenschluss zwischen ISO 27001 und NISG detailliert aufzeigen.

SCHÜTZEN SIE KRITISCHE INFRASTRUKTUR FÜR ENERGIE, VERKEHR UND FINANZEN

www.cis-cert.com/nisg-ueberpruefung

Business Continuity Management

ISO 22301

Die Lieferung von Produkten und die Bereitstellung von Dienstleistungen nach betriebsunterbrechenden Ereignissen innerhalb eines akzeptablen Zeitrahmens fortzusetzen oder die Auswirkung derartiger Ereignisse zu vermeiden bzw. auf ein vertretbares Niveau zu senken – das sind die übergeordneten Ziele eines Business Continuity Managementsystems (BCMS) nach ISO 22301.

ÜBERBLICK

Business Continuity (BC) ist ein Schlüsselthema zur Aufrechterhaltung der Betriebsfähigkeit nach disruptiven Ereignissen. Das gilt insbesondere dann, wenn das Unternehmen bzw. die Organisation (z. B. IT-Dienstleistung) eine kritische Position in der Lieferkette einnimmt.

Geeignete Strategien sind dabei auf Basis einer Business Impact Analyse und Risikobewertung festzulegen und Lösungen (Ausweichstandort, Notfallpläne etc.) dementsprechend umzusetzen. Die Effektivität der implementierten Lösungen und Notfallpläne wird mittels Übungen regelmäßig getestet und verbessert – ein Business Continuity Management System (BCMS) nach ISO 22301 stellt das alles sicher, und bietet damit ein ideales Steuerungsinstrument für das Top-Management zur Erzielung einer angemessenen Resilienz für das Unternehmen.

IHRE VORTEILE

- Vorbereitung auf betriebsunterbrechende Ereignisse
- Vermeidung von Produktionsausfall und Stillstand
- Nachweis von Schutzmaßnahmen zur Aufrechterhaltung der Geschäftsprozesse als Wettbewerbsvorteil

ZERTIFIZIERUNG

Mit der staatlichen Akkreditierung für Systemzertifizierungen nach ISO 22301 ist die CIS Vorreiterin in Österreich und gehört auch international zu den ersten Global Playern, die Zertifizierungen für Business Continuity Managementsysteme durchführen können. Der Ablauf einer Zertifizierung nach ISO 22301 ist konform mit der Struktur von Zertifizierungsprojekten nach ISO 27001 für Informationssicherheit und ISO 20000 für Service Management, so dass eine Systemintegration nahtlos möglich ist und durch kombinierte Zertifizierungsaudits sinnvolle Synergien nutzbar werden. Informationen zu den Projektphasen und dem Ablauf der Zertifizierung bzw. des Stage Reviews finden Sie auf Seite 8.

BUSINESS CONTINUITY STATT PRODUKTIONSAUSFALL UND STILLSTAND

www.cis-cert.com/business-continuity

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 die 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. Aufgrund seiner Flexibilität ist der Standard für alle Unternehmensgrößen und Branchen geeignet, auch für Abteilungen und Teilbereiche.

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.

LAUFENDE PROZESS-OPTIMIERUNG ALS WETTBEWERBSVORTEIL

www.cis-cert.com/service-management

Rechenzentren

EN 50600

Mit der von CENELEC herausgegebenen EN 50600-Serie wurde der erste länderübergreifende europäische Standard mit einem ganzheitlichen Ansatz für Rechenzentren (RZ) geschaffen, welcher neben den „Allgemeinen Konzepten“ (Business Impact und Risikoanalyse, RZ-Funktionsbereiche und Schutzklassen sowie Verfügbarkeitsklassen und Niveaus für die Befähigung zur Energieeffizienz) in der Untergruppe „Auslegung“ (Design) die Anforderungen an Einrichtungen und Infrastrukturen an RZ-Standorten beschreibt.

ÜBERBLICK

Für Eigentümer*innen und auch für Betreiber*innen von Rechenzentren ist es oberste Priorität, das Vertrauen ihrer Kund*innen zu gewinnen, welche für ihre Informations- und Kommunikationstechnik (IKT) Systeme im Rechnerraumbereich eine qualitativ hochwertige RZ-Basisinfrastrukturdienstleistung erwarten.

In Europa und insbesondere auch im deutschsprachigen Raum steigt die Nachfrage für die Zertifizierung von Rechenzentren nach anerkannten Regeln der Technik, also auf Basis einer international anerkannten Norm. Sowohl der Trend zum IT-Outsourcing als auch zum Cloud Computing sowie erhöhte gesetzliche Anforderungen wie z. B. die NIS-Richtlinie machen es erforderlich, dass die Resilienz und das physische Sicherheitsniveau von RZ-Standorten mittels Zertifikat einer unabhängigen Prüfstelle nachgewiesen werden kann.

IHRE VORTEILE

- Unabhängige Prüfstelle für die Resilienz Ihrer RZ-Standorte und deren RZ-Basisinfrastrukturen
- Überprüfung der Einhaltung der Gestaltungsgrundsätze für die RZ-Infrastrukturbereiche laut EN 50600-2-X: Gebäudekonstruktion, Energieversorgung und Energieverteilung, Regelung der Umgebungsbedingungen, Infrastruktur der Telekommunikationsverkabelung, Sicherheitssysteme

ZERTIFIZIERUNG

Eine erfolgreich durchgeführte Zertifizierung nach dem Modell „EN 50600 – Design“ bescheinigt die Konformität der baulichen und technischen Auslegung (Design) des RZ-Standorts mit den in der EN 50600-1 sowie den Teilen der EN 50600-2-X festgehaltenen Gestaltungsgrundsätzen (design principles), und zwar in der angegebenen technischen Verfügbarkeitsklasse / im angegebenen Niveau für die Befähigung zur Energieeffizienz / im angegebenen physischen Sicherheitslevel.

QUALITÄT, RESILIENZ UND PHYSISCHE SICHERHEIT IHRES RECHENZENTRUMS

www.cis-cert.com/rechenzentren

Blockchain Assessment

Distributed Ledger Technologien (DLT) haben gezeigt, dass sie das Potenzial haben die digitale Welt zu revolutionieren. Praktisch alle Branchen experimentieren momentan mit ihrer Verwendung in einer Vielzahl von Anwendungsfällen. DLT selbst gelten zwar als manipulationssicher, doch unterliegen Lösungen, die auf der Technologie aufbauen, Risiken – genau wie jede andere IT-Implementierung.

ÜBERBLICK

Durch die objektive Überprüfung Ihrer Blockchain Lösung stellen Sie sicher, dass die technische Lösung die gestellten Anforderungen an Sicherheit, Transparenz und Vertraulichkeit von individuellen Daten und Assets erfüllt. Dabei überprüfen wir die Anwendung der DLT bedarfsgerecht hinsichtlich ihrer organisatorischen sowie technischen Implementierung, und berücksichtigen die relevanten Anforderungen in puncto Informationssicherheit und IT Service Management (ISO 27001 und ISO 20000).

IHRE VORTEILE

- Stetige Transparenz für das gesamte Netzwerk
- Sicherstellung der Datenintegrität
- Verhinderung von Betrugsfällen und Manipulation
- Verlässlichkeit und Qualität der Implementierung
- Aufbau von Vertrauen
- Offizielle Bestätigung von einer unabhängigen Stelle, dass Ihre Lösung auf dem aktuellen Stand der Technik ist, den regulativen Anforderungen entspricht und damit vertrauenswürdig ist

OBJEKTIVE BEGUTACHTUNG

Das Assessment umfasst eine standardisierte Prüfung der Blockchain Lösung auf prozessualer Ebene bezüglich Betrieb, Entwicklung und Weiterentwicklung sowie auf technischer Ebene bezüglich eingesetzter Geschäftslogik, Spezialhardware und Distributed Ledger Technologie.

Die Assessment-Urkunde wird ausgestellt, sofern die Nutzung der Distributed Ledger Technologie aus Sicht von ISO 20000 bzw. ISO 27001 unbedenklich ist, und kann als international gültige Empfehlung für das nächste Audit verwendet werden.

SICHERHEIT UND VERTRAUEN FÜR IHRE BLOCKCHAIN LÖSUNG

www.cis-cert.com/blockchain-assessment

TISAX®

TRUSTED INFORMATION SECURITY ASSESSMENT EXCHANGE

TISAX® (Trusted Information Security Assessment Exchange) ist ein branchenspezifischer Austauschmechanismus von Ergebnissen aus Informationssicherheitsassessments der Automobilindustrie. Diese Assessments basieren auf dem VDA-ISA Prüfkatalog, welcher Informationssicherheitscontrols zu Informationssicherheit (basierend auf der ISO 27001), zu Prototypenschutz und Datenschutz beinhaltet.

ÜBERBLICK

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

IHRE VORTEILE

- Erfüllung der automotiven Kund*innenanforderungen
- Anerkennung der Prüfergebnisse am automotiven Markt / in der Automotiven Supply Chain
- Schutz der eigenen Unternehmenswerte
- Bewusstseinsschärfung der Mitarbeiter*innen
- Basis für eine mögliche ISO 27001 Zertifizierung
- Gesonderter 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 Prüflabel ausgestellt, die Sie mit Ihren Geschäftspartner*innen teilen können.

Damit ist TISAX® die Grundlage zum Prüf- und Austauschmechanismus Ihres Informationssicherheitsmanagementsystems in der Automobilindustrie. Für die Umsetzung benötigen Sie eine gute Basis, welche Sie in dieser Qualifizierung erlangen können.

TISAX® ist eine eingetragene Marke der ENX Association.

SECURITY FÜR AUTOMOTIVE PRODUZENT*INNEN UND ZULIEFERUNTERNEHMEN

www.cis-cert.com/tisax

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.

LEHRGANGSREIHEN

- Information Security Manager nach ISO 27001
- Information Security Auditor nach ISO 27001

SEMINARE, REFRESHINGS UND WEBINARE

- Seminar: Datenschutz nach ISO 27701 für Informationssicherheitsmanager*innen
- Seminar: ISO 27701 Das Informationssicherheits- und Datenschutzmanagementsystem
- Spezialtraining: ISO 27001 und Cyber Security für Softwareentwickler*innen
- VDA QMC Lizenztraining (in Kooperation mit ÖQA): Sind Sie sicher? VDA ISA im eigenen Unternehmen umsetzen – für ein erfolgreiches TISAX Assessment
- Refreshing für IS Manager*innen und IS Auditor*innen
- Webinar: Erfolgsfaktor Informationssicherheit und Datenschutz

ANSPRECHPARTNERIN TRAININGS UND PERSONENZERTIFIZIERUNG

Stefanie Pachhammer
Leitung Personenzertifizierung und Trainings
stefanie.pachhammer@cis-cert.com

ALLE TRAININGS AUCH
INHOUSE
BUCHBAR

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.

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

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.

ZULASSUNG ZU PRÜFUNGEN

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

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 Ausbildungen im Rahmen der CIS-Lehrgänge absolviert worden sein, findet eine automatische Anerkennung statt, sofern mindestens 80% der Veranstaltungszeit besucht wurde.

www.cis-cert.com

Zertifikat

ausgestellt nach den Kriterien der EN ISO/IEC 17024

Information Security Manager

Dr. Max Mustermann, MSc

geboren am XX.XX.XXXX

hat die Prüfung nach den Richtlinien der CIS, die den Anforderungen der Wirtschaft entsprechen, am XX.XX.XXXX in Wien bestanden.

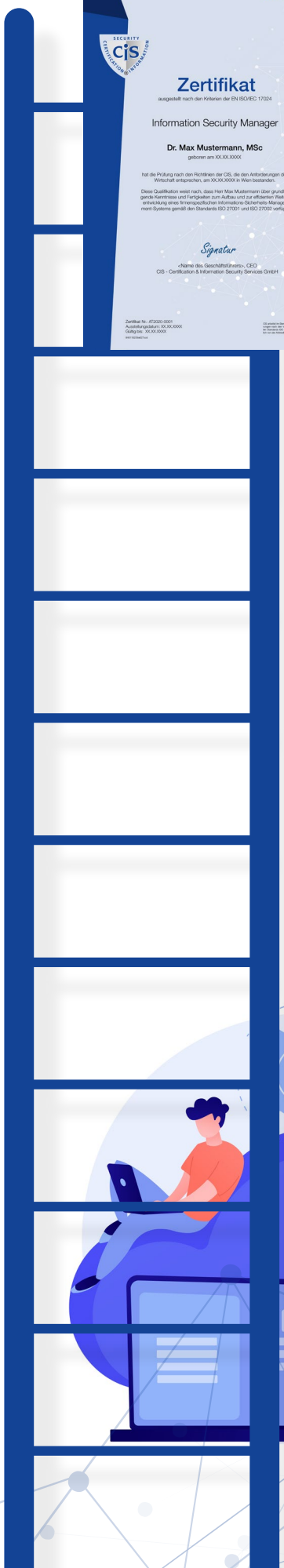
Diese Qualifikation weist nach, dass Herr Max Mustermann über grundlegende Kenntnisse und Fertigkeiten zum Aufbau und zur effizienten Weiterentwicklung eines firmenspezifischen Informations-Sicherheits-Management-Systems gemäß den Standards ISO 27001 und ISO 27002 verfügt.

Signatur

«Name des Geschäftsführers», CEO
CIS - Certification & Information Security Services GmbH

Zertifikat Nr.: 472020-0001
Ausstellungsdatum: XX.XX.XXXX
Gültig bis: XX.XX.XXXX

Muster Personenzertifikat



Information Security Manager*in nach ISO 27001

BERUFSBILD

Das übergeordnete Ziel von Information Security Manager*innen ist das Aufzeigen von Sicherheitsrisiken und Sicherheitslücken, die Planung und Dokumentation entsprechender Abwehrmaßnahmen sowie eine laufende Verbesserung gesetzter Schritte. Information Security Manager*innen sind zentrale Ansprechperson und Schnittstelle zwischen der Führungsetage und den operativen Unternehmensbereichen. Sie betreuen darüber hinaus den Aufbau, die Implementierung und die Verbesserung eines prozessorientierten Informationssicherheitsmanagementsystems.

STRUKTUR DER LEHRGANGSREIHE

ISMN → ISMR → ISMP → ISM-P

Die aktuelle Teilnahmegebühr für die gesamte Lehrgangsreihe inklusive Prüfung und Zertifikat finden Sie online. Preise für einzelne Lehrgänge auf Anfrage. Kontaktieren Sie uns gerne unter trainings@cis-cert.com

ISMN – 2 Tage, 09–17 Uhr – Die ISMS-Normen ISO 27001 und ISO 27002: Informationssicherheit richtig implementieren und optimieren

LEHRGANG

In zwei Tagen werden nicht nur die wesentlichen Grundlagen der Informationssicherheit behandelt, sondern auch übergeordnete Aspekte wie Organisation, Technik oder Prozessmanagement. Mittels praktischer Fallbeispiele werden die Teilnehmer*innen an die selbständige Umsetzung des Gelernten herangeführt. Darüber hinaus wird der Standard auch mit anderen Ansätzen zum Thema Informationssicherheit verglichen sowie auf mögliche Weiterentwicklungen der Norm selbst und auch der Normreihe ISO 27x eingegangen.

ZIEL

Die Teilnehmenden kennen nach Abschluss dieses Moduls die Prozesse und Normforderungen zur Implementierung der Normen ISO 27001 und ISO 27002 in einem Unternehmen und können diese praktisch anwenden. Sie verfügen über die Basis, um eine ständige Verbesserung des ISM-Systems zu gewährleisten.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

ISMP – 1 Tag, 09–17 Uhr – Psychologische Grundlagen: Von Mitarbeiter*innen-Motivation bis zu Konfliktfähigkeit

LEHRGANG

Die Einführung neuer Systeme stößt mitunter auf Widerstände – außer man beherrscht die hohe Schule der Psychologie. Dieses eintägige Seminar vermittelt Ihnen die Grundlagen, um das erworbene Fachwissen erfolgreich im Umfeld eines Unternehmens umsetzen zu können. Dazu gehören Soft Skills wie Moderations-, Team- und Konfliktfähigkeit, interdisziplinäres Zusammenarbeiten oder auch Wissen über Beziehungsmodelle, gruppendynamische Prozesse und Motivationstechniken. Auch das Selbstverständnis eines Managers bzw. einer Managerin gehört zu den entscheidenden Erfolgsfaktoren.

ZIEL

Die Teilnehmenden werden in die Lage versetzt, die Unternehmensziele mit möglichst geringen Reibungsverlusten auf der Beziehungsebene erfolgreich durchzusetzen. Sie lernen auch, Projektteams zu bilden, zu führen und zu motivieren.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

ISMR – 1 Tag, 09–17 Uhr – Rechtsgrundlagen für Information Security Manager*innen: Compliance-Anforderungen erkennen und kompetent umsetzen

LEHRGANG

In diesem Lehrgang werden Ihnen vier Schwerpunkte vermittelt:

- Datenschutz & Datensicherheit: Dieser Block liefert Informationen über schützenswerte Daten, Wege der Datenverwendung, das Datengeheimnis, die Rechte von Betroffenen, Strafen und Schadenersatz.
- Wettbewerbsrecht: Dieser Teil vermittelt Grundsätzliches über E-Mail-Werbung, Internet-Links, Markenschutz und Werbeverbote.
- E-Commerce: Dieses Kapitel behandelt die E-Commerce-Richtlinie, den Fernabsatz und das Signaturgesetz.
- Urheberrecht, Domain-Namen: Der letzte Ausschnitt widmet sich dem Marken-, Namens- und Kennzeichenschutz.

ZIEL

Die Teilnehmenden kennen die für Informationssicherheit relevanten Gesetze und können die wichtigsten Regelungen selbständig anwenden.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

ISM-P – 1 Stunde – PRÜFUNG Information Security Manager*innen

LEHRGANG PRÜFUNG

Die Prüfungsinhalte beziehen sich auf die CIS-Lehrgänge „Die ISMS-Normen ISO 27001 und ISO 27002“, „Psychologische Grundlagen für Information Security Manager*innen“ und „Rechtsgrundlagen für Information Security Manager*innen“.

DURCHFÜHRUNG

Die schriftliche Prüfung (Single Choice) dauert 1 Stunde.

ZERTIFIKAT **Information Security Manager**

GÜLTIGKEITSDAUER DES ZERTIFIKATS 3 Jahre

VERLÄNGERUNGSKRITERIEN

- Nachweis (z. B. Bestätigung durch Arbeitgeber*in, Interimszeugnis, Eigenerklärung) über 3-jährige Berufspraxis im Bereich Informationssicherheitsmanagement.
- Eine CIS-Weiterbildungsveranstaltung in 3 Jahren.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

Information Security Auditor*in nach ISO 27001

BERUFSBILD

Als Information Security Auditor*innen sind Sie im Unternehmen die „Oberste Instanz“ für ISMS. Sie beurteilen die Informationssicherheit auf ihre Normkonformität hin und arbeiten Verbesserungspotenziale heraus, bevor einem Unternehmen das CIS-Zertifikat für den bestmöglichen Standard an Sicherheit nach ISO 27001 verliehen oder eine Verlängerung ausgestellt wird. Interne Audits bewähren sich als mächtige Instrumente, um die Rentabilität und Wirksamkeit von ISMS nachhaltig zu steigern. Als erste Organisation in Österreich wurde die CIS für die Personenzertifizierung akkreditiert. Damit entsprechen die durch die CIS ausgestellten Personenzertifikate staatlich und international anerkannten Dokumenten.

ISATE-P — 2 Stunden — Technische Einstiegsprüfung: Garant für ein hohes Ausbildungsniveau

LEHRGANG PRÜFUNG

Teilnahmevoraussetzung für den Information Security Auditor*innen Lehrgang ist das Zertifikat „Information Security Manager“. Das Absolvieren der technischen Einstiegsprüfung ist eine weitere Voraussetzung, um am Lehrgang teilzunehmen.

INHALTE

Die Prüfungsinhalte werden im Selbststudium erarbeitet und umfassen rund 1.000 Fragen und Antworten.

DURCHFÜHRUNG

Die Prüfung ist schriftlich abzulegen. Die Prüfung besteht aus Auswahlfragen (Single Choice) und dauert 2 Stunden.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

ISAP — 2 Tage — 09–17 Uhr — Psychologische Grundlagen: Zwischen Prüfendem und Developer. Systemisch denken, wirksam kommunizieren.

LEHRGANG

Auditor*innen sind bei einem Audit doppelt gefordert: Einerseits haben sie als sachkundige Prüfende zu fungieren, andererseits als vorausschauende Development Agents, die wichtige Impulse für die Weiterverbesserung des ISM-Systems setzen. Auditor*innen stehen sowohl in Kontakt mit der obersten Führungsebene als auch mit dem operativen Management. Neben Expertenwissen benötigen Auditor*innen eine hohe soziale Kompetenz, die Fähigkeit vernetzt zu denken und abteilungsübergreifende Systemzusammenhänge zu erkennen sowie Einblicke in die Grundregeln der Kommunikation. Theorie und Praxis ergänzen sich bei diesem Seminar in ausgewogener Weise: Der zweite Ausbildungstag ist vor allem dem Training durch Rollenspiele mit Video-Feedback gewidmet.

ZIEL

Die Teilnehmenden üben das Denken in Systemzusammenhängen, kennen die Kompetenzen eines Auditors bzw. einer Auditorin und beherrschen die Grundregeln der Kommunikation in Theorie und Praxis.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

STRUKTUR DER LEHRGANGSREIHE

ISATE-P → ISAT → ISAP → ISA-P

Die aktuelle Teilnahmegebühr für die gesamte Lehrgangsreihe inklusive Prüfung und Zertifikat finden Sie online. Preise für einzelne Lehrgänge auf Anfrage. Kontaktieren Sie uns gerne unter trainings@cis-cert.com

ISAT — 1 Tag — 09–17 Uhr — Audittechniken: Interne Audits als mächtiges Instrument für die Systemverbesserung

LEHRGANG

Die gesamte Praxis zur Durchführung interner und externer Audits ist Inhalt dieses Lehrgangsmoduls. Die verschiedenen Auditarten für unterschiedliche Typen von Organisationen gehören ebenso dazu wie die verschiedenen Arbeitsschritte: Vorbereitung des Audits, Anwendung der Auditfragen, Vorab-Prüfung, Vor-Ort-Audit, Auditanalyse (mit Methoden) und Erstellung des Auditberichts. Ein wichtiger Schwerpunkt ist auch die Bestimmung von Korrektur- und Verbesserungsmaßnahmen. Die Umsetzung der Theorie wird anhand möglichst praxisnaher Fallbeispiele geübt.

ZIEL

Die Teilnehmenden können interne und externe Audits planen und durchführen, sowie deren Ergebnisse analysieren und etwaige Schwachstellen und Verbesserungspotenziale erkennen und bewerten.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

ISA-P — 1 Stunde — Prüfung Information Security Auditor*in

LEHRGANG PRÜFUNG

Die Prüfungsinhalte beziehen sich auf die CIS-Lehrgangsmodule „Psychologische Grundlagen“ und „Audittechniken“.

DURCHFÜHRUNG

Die schriftliche Prüfung (Single Choice) dauert 1 Stunde.

ZERTIFIKAT **Information Security Auditor**
(bei fehlendem Praxisnachweis mit dem Zusatz „Anwärter“)

GÜLTIGKEITSDAUER DES ZERTIFIKATS 3 Jahre

VERLÄNGERUNGSKRITERIEN

- Nachweis über 3 Jahre Berufspraxis im Informationssicherheitsmanagement. Nachweis über 4 durchgeführte IS-Audits mit mind. 20 Audittagen
- Eine CIS-Weiterbildungsveranstaltung (Refresher) innerhalb von 3 Jahren.

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

Seminare/Refreshings/Webinare

1 Tag
09–17 Uhr

SEMINAR: Datenschutz nach ISO 27701 für Informationssicherheits-manager*innen

SEMINAR

Das Aufbautraining für Informationssicherheitsmanager*innen führt in die Zusatzanforderungen eines ISO 27701 konformen Datenschutz- und Informationssicherheitsmanagementsystems ein.

ZIELGRUPPE

Informationssicherheitsmanager*innen

INHALT

- Informationssicherheit und Datenschutz: Gemeinsamkeiten und Unterschiede
- Kernelemente der Datenschutzgrundverordnung 2016/679 u. a. Datenschutzbestimmungen
- Grundsätze der Verarbeitung; Rechte und Pflichten; Rollen
- Zusatzforderungen und Aufbau der ISO 27701
- Reflexion

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

3 Tage
09–17 Uhr

SEMINAR: ISO 27701 Das Informationssicherheits- und Datenschutz-managementsystem

SEMINAR

Das Seminar führt in die Wirkungsweise und die Anforderungen an ein Informationssicherheitsmanagementsystem nach der ISO 27001 ein, und zeigt darauf aufbauend die effiziente und nachhaltige Umsetzung eines ISO 27701 konformen Datenschutz- und Informationssicherheitsmanagementsystems auf.

ZIELGRUPPE

Geschäftsführung, Führungskräfte, betriebliche Beauftragte, Systemmanager*innen, Auditor*innen und andere Interessierte an Informationssicherheit und Datenschutz

INHALT

- Bedeutung von Informationssicherheit und Datenschutz für Ihr Unternehmen
- Informationssicherheit und Datenschutz: zwei Seelen in einer Brust – Gemeinsamkeiten und Unterschiede
- Kernelemente der Datenschutzgrundverordnung 2016/679 u. a. Datenschutzbestimmungen
- Kernelemente der ISO 27001, ISO 27701, ISO 27002; Analyse der Anforderungen und Verarbeitungen
- Risikoanalyse und Notfallmanagement
- Sicherheitsmaßnahmen, Organisation und Prozesse

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

1 Tag
09–17 Uhr

SPEZIALTRAINING: ISO 27001 und Cyber Security für Software-entwickler*innen

SEMINAR

Dieses individuelle Spezialtraining vermittelt den Teilnehmenden die Grundlagen der Norm ISO 27001/IS0 27002 – das Fundament für moderne Informationssicherheitsmanagementsysteme (ISMS).

ZIELGRUPPE

Softwareentwickler*innen

INHALT

- ISO 27001
- Implementierungsleitfaden ISO 27002 mit allen wichtigen Teilbereichen wie Risikomanagement, Business Continuity Planning, internes Auditing und insbesondere die technischen Controls des Annex A
- Bereiche der Norm, die in der Softwareentwicklung eine wichtige Bedeutung haben.
- Praxisorientierter Erfahrungsaustausch

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

2 Tage
09–17 Uhr

REFRESHING für IS-Manager*innen und IS-Auditor*innen

REFRESHING

Praxisnahe Fallbeispiele und Anforderungen gemäß ISO 27001 aus dem eigenen Arbeitsbereich werden zielgerichtet diskutiert. Der Refresher-Kurs für Informationssicherheitsmanager*innen und -Auditor*innen umfasst demgemäß neben Wissensaktualisierung auch Erfahrungsaustausch und Tipps für die Praxis – bringen Sie „Ihr Unternehmen“ mit!

ZIELGRUPPE

IS-Manager*innen und IS-Auditor*innen, die die Aufrechterhaltung ihres Personenzertifikats und eine Kompetenzentwicklung anstreben

INHALT

- Weiterentwicklung von ISMS nach ISO 27001/ISO 27002
- Normforderungen und ihre effektive Umsetzung in der Praxis
- Neue Subnormen, neue Norminhalte im Rahmen der Normenreihe ISO 27000
- Neue Methoden und Erkenntnisse aus der internationalen Community
- Interne und externe Audits: Synergien und Systemoptimierung durch strukturiertes Vorgehen
- Strategie- und Organisationsentwicklung

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

2 Tage | **VDA QMC Lizenztraining (in Kooperation mit ÖQA): VDA ISA im eigenen Unternehmen umsetzen**

SEMINAR

In der zweitägigen Schulung lernen Sie an einigen zentralen VDA ISA-Anforderungen beispielhaft, wie Sie im eigenen Unternehmen Maßnahmen für ein erfolgreiches TISAX® Assessment umsetzen können.

TISAX® ist eine eingetragene Marke der ENX Association.

ZIEL

Sie lernen Entscheidungsgrundlagen zu bilden und eine Roadmap zur Umsetzung im Unternehmen zu entwickeln. Sie verstehen die notwendigen Abläufe und Maßnahmen für ein erfolgreiches TISAX® Assessment. Sie kennen unterschiedliche Werkzeuge, um entsprechende Maßnahmen im eigenen Unternehmen umzusetzen.

WEITERE INFORMATIONEN

www.austriaguetezeichen.at/ausbildung

60 Minuten | **WEBINAR: Erfolgsfaktor Informationssicherheit und Datenschutz**

Ein Datenschutz- und Informationssicherheits-Managementsystem fördert nachhaltig, effizient und effektiv das Sicherheits- und Datenschutzbewusstsein und stärkt das Vertrauen der Stakeholder. Wenn Sie an diesem Thema interessiert sind und einen ersten Überblick über die Norm ISO 27701 und deren Nutzen erhalten wollen, besuchen Sie unser kostenfreies CIS Webinar in Zusammenarbeit mit der Quality Austria.

INHALT

- Erfolgsfaktor Informationssicherheit und Datenschutz
- Zwei Seelen in einer Brust
- ISO 27701: Informationen zum Managementsystem
- Nutzen und Vorteile

WEITERE INFORMATIONEN www.cis-cert.com/alle-termine

Service

WIR HELFEN IHNEN GERNE WEITER. KONTAKTIEREN SIE UNS!

CIS NEWSLETTER

Der CIS Newsletter liefert Ihnen topaktuelle News rund um die Themen Informationssicherheit, Datenschutz, Cloud Computing, IT-Services, Business Continuity Management u. v. m. 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

Besuchen Sie unsere Social Media Kanäle auf LinkedIn, Twitter und XING. News und Trends aus der Branche warten auf Sie – vernetzen Sie sich mit Gleichgesinnten und verpassen Sie keine Updates mehr.

Like, Share, Follow - let's connect! **#bepartofit #besecure**

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

qualityaustria
Erfolg mit Qualität

WIR UNTERSTÜTZEN SIE BEI DER AUSRICHTUNG AUF LANGFRISTIGE ZIELE

Die CIS – Certification & Information Security Services GmbH ist eine 100%ige Tochter der Quality Austria – Trainings, Zertifizierungs und Begutachtungs GmbH.

www.qualityaustria.com

SECURE YOUR BUSINESS

CIS
Certification & Information Security Services GmbH

www.cis-cert.com

office@cis-cert.com
Salztorgasse 2/6/14,
1010 Wien, Austria
Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89

Hinweis
Alle personenbezogenen Bezeichnungen in dieser Broschüre beziehen sich in gleicher Weise auf Frauen und Männer. Die CIS 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 2023

Dok.nr.: CIS-M002_Portfolio_202308 | Ausgabe: 08/2023