Zertifizierung von Managementsystemen

Informationssicherheit nach ISO/IEC 27001

IT-Service-Management nach ISO/IEC 20000

Vom Detail zum System:
Prozessmanagement
nach ISO-Standards

CIS - Secure Your Business

Inhalt

Impressum

Herausgeber: CIS - Certification & Information Security Services GmbH
Für den Inhalt verantwortlich: Erich Scheiber, CIS-Geschäftsführung
Konzept und Text: Galley Public Relations
Grafik: powerhouse.at
Stand: Mai 2011

Fußnoten

[1] **Rechtsanwalt Dr. Markus Frank, Wien**
[2] **Rechtsanwalt Dr. Orlin Radinsky, Wien, Kanzlei Brauneis Klauser Prändl**

CIS - Secure Your Business

Als akkreditierte Zertifizierungs- und Ausbildungsorganisation gehört CIS zu den Global Playern

Als weltweit tätige Zertifizierungs- und Ausbildungsorganisation ist die CIS - Certification & Information Security Services GmbH auf Informationssicherheit nach ISO/IEC 27001 sowie IT-Service-Management nach ISO/IEC 20000 spezialisiert. In rund 30 Ländern bietet CIS über Tochter- oder Partnerorganisationen Certification Services und Trainings auf höchstem Niveau. Das hohe Ansehen von CIS-Zertifikaten im In- und Ausland, bei **Behörden und Kunden**, gilt als Vorteil im Wettbewerb. Grund dafür ist die Qualität der CIS-Akkreditierung durch das BMWFJ sowie der **erprobte Zertifizierungsablauf**. Denn mit einer CIS-Zertifizierung erhalten Sie eine unabhängige Überprüfung des Managementsystems nach ISO 27001 oder ISO 20000, wobei CIS-Auditoren ihr profundes Fachwissen in der Vorbereitungsphase einbringen. Mächtige Instrumente dafür sind das Stage-Review und das Stage-One-Audit (S. 6). So sind Unternehmen optimal vorbereitet – für die Motivation der Mitarbeiter ist es wichtig, die Zertifizierung im ersten Anlauf zu erreichen. Als etablierter Zertifizierungspartner bietet CIS wichtige Vorteile:

- **Mehrwert:** Vorsprung bei Ausschreibungen
- **Vertrauen:** Hohes Ansehen der CIS-Zertifikate
- **Know-how**: Profunde Expertise & IT-Spezialisierung
- **Impulse:** Auditbericht mit Stärken/Schwächen-Analyse
- **Synergien:** bis zu 30% Ersparnis durch Kombi-Audits
- **Global:** CIS-Services aus einer Hand in 30 Ländern

Mit einem CIS-Zertifikat sind Unternehmen auf der sicheren Seite. CIS ist als unabhängige Zertifizierungsorganisation **staatlich akkreditiert**. Regelmäßig wird die CIS nach gesetzlich vorgeschriebenen **Standards für Zertifizierer** durch das BMWFJ überprüft und erfüllt damit die strengen Auflagen der internationalen Normen ISO 17021 für die Systemzertifizierung sowie ISO 17024 für die Personenzertifizierung. CIS-Zertifikate entsprechen staatlichen Dokumenten und sind international bei Behörden, Kunden sowie vor Gericht anerkannt.

Erich Scheiber
CIS-Geschäftsführung

CIS-Leistungen im Überblick:

- **Zertifizierung von Unternehmen**
- **Stage-Reviews**
- **Ausbildungen mit Zertifikat**
- **Inhouse-Trainings**

...passen für Unternehmen jeder Größe und Branche: Managementsysteme nach ISO-Standards

Informationssicherheit mit System

Mehr als IT-Security: Durch ISO 27001 werden auch Mitarbeiter-Awareness, Gebäudeschutz und Umgebungssicherheit abgedeckt

Am Markt ist es heute zunehmend erforderlich, betriebliche Informations- und Datensicherheit explizit nachzuweisen. Zudem benötigen Unternehmen für die immer komplexeren Security-Anforderungen ein Prozessmanagementsystem, mit dem sich höchste Sicherheit nicht nur erreichen, sondern auch **messen, kontrollieren** und verbessern lässt: Nach dem KVP-Modell Plan-Do-Check-Act.
Der Standard ISO/IEC 27001 für Informationssicherheit verbucht weltweit einen wachsenden Anwenderkreis aus allen Branchen, von KMU bis zu Multinationals. Inhaltlich geht ISO 27001 **je nach Bedarf** weit über die reine IT-Sicherheit hinaus. Auch Faktoren wie Mitarbeiter-Awareness, Einhaltung gesetzlicher Verpflichtungen sowie Infrastruktur-, Gebäude- und Umgebungsaspekte vom Brandschutz bis zu Zutrittskontrollen werden abgedeckt. Organisationen mit sensiblen Daten und Anforderungen an Hochverfügbarkeit nutzen den erprobten Standard.

Vertraulichkeit – Integrität – Verfügbarkeit
Ein Managementsystem für Informationssicherheit (ISMS) nach ISO 27001 gewährt durch sein Framework für technische und organisatorische Maßnahmen mit Wirksamkeitskontrolle sowie Optimierungsschleifen:

- **höchsten Schutz von Daten und Informationen,**
- **Hochverfügbarkeit von IT-Services,**
- **Haftungsminimierung vor Gericht.**

Gleichzeitig steigert eine Zertifizierung nach ISO 27001 den **Business Value von IT-Diensten**. Geprüfte Informationssicherheit ermöglicht das Anbieten hochwertiger Services – intern wie extern. Zudem gilt das ISO-27001-Zertifikat als schlagendes Wettbewerbskriterium. So wird Datensicherheit ohne aufwendige Einzelnachweise effizient belegbar:

- **bei Ausschreibungen,**
- **bei Behörden,**
- **für die Interne Revision.**

Foto: Raiffeisen Informatik GmbH

Good Practice: Profitieren, von den Erfahrungen anderer ...

Raiffeisen Informatik GmbH;
Michael Ausmann, Chief Security Officer:
„Mit dem Fokus der Norm ISO 27001 auf „Informationssicherheit" wird das Thema ganzheitlich betrachtet: Es werden alle im Lebenszyklus der Informationen relevanten Faktoren berücksichtigt – nicht nur die IT-Komponente."

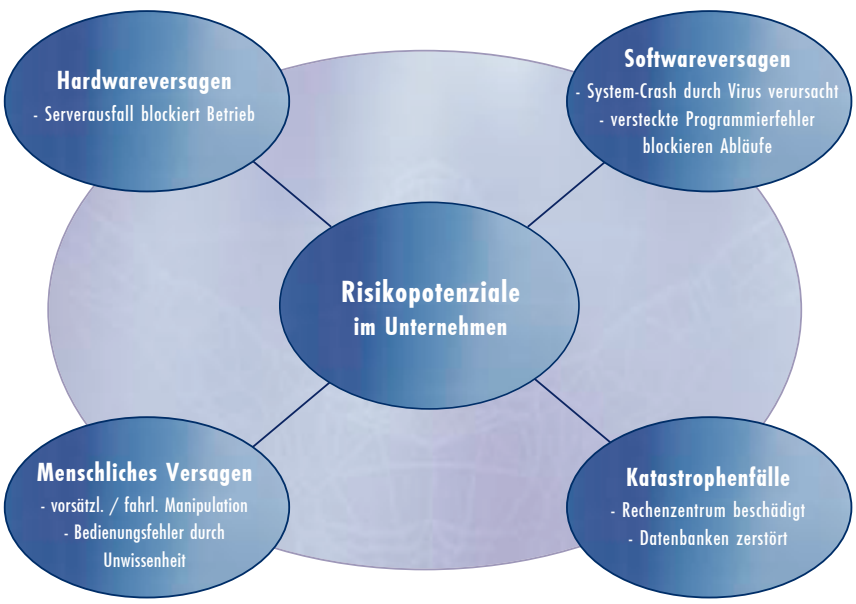
Risiken (er)kennen und bewerten

Die Risikoanalyse nach ISO 27001 bringt verborgene Gefahren ans Licht

Ist das Sicherheitsniveau des Unternehmens angemessen? Gibt es Schwachstellen in Bezug auf Datensicherheit und -verfügbarkeit oder in der Legal Compliance? Welche **Sicherheitsmaßnahmen** sind wirksam und rentabel? Risikoanalysen nach ISO/IEC 27001 liefern wichtige Erkenntnisse zur **Bewertung des Sicherheitsniveaus** einschließlich Restrisiken und ermöglichen die Erstellung effizienter Maßnahmenkataloge. Risikomanagement zur Wahrung der Business Continuity ist eine zentrale Forderung in der Informationssicherheit. Diesem Ansatz ist die gute Skalierbarkeit des Standards zu verdanken: ISO 27001 eignet sich für KMU genauso wie für Konzerne, da die anfängliche Risikoanalyse den individuellen Sicherheitsbedarf aufzeigt.

Reduzierung des Haftungsrisikos

Medien berichten immer wieder über verlorene oder veröffentlichte Kundendaten mit Schadenersatzklagen in Millionenhöhe. Ein zertifiziertes Managementsystem für Informationssicherheit minimiert Sicherheitslücken systematisch und reduziert das Haftungsrisiko.[1] Denn **in Gerichtsverfahren** hängt der Prozessausgang häufig von der **Nachweisbarkeit** „sorgfältiger Leistungserbringung“ ab. Aufgrund der unabhängigen Überprüfung durch einen Zertifizierer wird für den Richter nachvollziehbar, dass Mitarbeiter nach festgelegten, dem Stand der Technik entsprechenden Richtlinien arbeiten. Resultat einer kontinuierlichen ISO-27001-Zertifizierung ist eine Minimierung des Haftungsrisikos für Unternehmen und ihre Führungskräfte.[2]



„50 % aller Firmen, die wichtige Daten verloren haben, konnten sich nie davon erholen. 90 % jener Firmen mussten innerhalb von zwei Jahren ihre Geschäftstätigkeit aufgeben.“

Center for Research on Information Systems, University of Texas

IT Service Management

Von ITIL zu ISO: Zertifikat nach ISO 20000 macht ITIL-Compliance gegenüber Kunden nachweisbar

Service-Qualität steigern, Kosten senken. ISO/IEC 20000 ist der weltweit erste zertifizierbare Standard für IT-Service-Management und fokussiert Qualitätsverbesserung, Effizienzsteigerung und **Kostentransparenz** von IT-Diensten. Die internationale Norm beschreibt einen integrierten Satz von Management-Prozessen für die Erbringung von IT-Services und baut inhaltlich auf der erfolgreichen IT Infrastructure Library auf. Eine ISO-20000-Zertifizierung ist für Personen möglich – ISO 20000 Auditor, ISO 20000 Practitioner – ebenso aber auch für Organisationen oder Abteilungen. So wird der Wettbewerbsvorsprung gegenüber Kunden nachweisbar.

Einen Investitionsschutz bietet die Zertifizierung nach ISO 20000 aufgrund des implementierten Managementsystems. Statistisch zeigt sich, dass Investitionen ohne kontinuierliche Verbesserung nur kurzzeitige Erfolge bringen. Durch regelmäßige Überwachungsaudits wird dem effektiv entgegen gewirkt. Aufgrund der Begutachtung durch eine unabhängige Zertifizierungsorganisation können Abweichungen von Vorgaben sichtbar gemacht und Korrekturmaßnahmen eingeleitet werden. **Kernstück des Standards** ist das Modell zur Prozessverbesserung Plan-Do-Check-Act, welches zu einem kontinuierlichen Optimierungsprozess mit höherer Qualität und Effizienz von IT-Diensten führt. Der **Einsatz von Kennzahlen** wie „Kundenzufriedenheit“ oder „Service-Verfügbarkeit“ erweist sich als mächtiges Steuerungsinstrument. Aufgrund seiner Flexibilität ist ISO 20000 für alle Unternehmensgrößen und Branchen geeignet.

„Transparenz“ durch ISO 20000

“Die Bearbeitungsdauer von Vorfällen ging seit der ISO-20000-Zertifizierung um 20 % zurück. Incidents aufgrund von Release-Einsätzen reduzierten sich um 40 %.”

Raiffeisen Rechenzentrum Süd
Dipl.-Ing. Markus Hefler,
ITS Continuity Manager

Profitieren, durch ISO-20000-Zertifizierung:

- Messbare Einsparungen
- Qualität durch Optimierung
- Produktivität steigt wesentlich
- Weltweit anerkannter Standard
- Zertifikat macht Vorsprung sichtbar
- Benchmarking durch Standardisierung

Von der Implementierung zum Zertifikat

In drei Projektphasen sicher an das Ziel

Der Ablauf eines Zertifizierungsprojektes für ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001 (ISMS) oder ein IT-Service-Managementsystem nach ISO/IEC 20000 (ITSMS) teilt sich in drei Projektphasen. Dieser Ablauf gilt auch für Integrierte Managementsysteme mit zeit- und kostensparenden Kombinations-Audits.

"Keep it secure and simple: So wirksam wie möglich, aber trotzdem einfach in der Handhabung."

Mag. Krzysztof Müller, Leiter Information Security, A1 Telekom Austria

- **Information:** Ein Erstgespräch mit CIS liefert Details über den Zertifizierungsprozess. Es folgen Registrierung und Projektplanung.
- **Analyse:** Evaluierung von individuellen Anforderungen und Bewertung vorhandener Maßnahmen durch das Unternehmen. CIS als unabhängige Prüfstelle ist nicht involviert.
- **Implementierung:** Einführung von Maßnahmen nach ISO 27001 und/oder ISO 20000. CIS als unabhängige Prüfstelle ist nicht involviert.

- **CIS-Stage-Review (freiwillige Vorbeurteilung):** Auf Wunsch überprüft CIS projektbegleitend die Zweckmäßigkeit und Effizienz der implementierten System-Elemente.
- **CIS-System-&-Risk-Review (Vorbegutachtung):** CIS begutachtet die Umsetzung der Normforderungen sowie die Dokumentation. Mängel und Verbesserungspotenziale werden in einem Kurzbericht festgehalten. Diese Vorbegutachtung dient als „Generalprobe" vor dem Zertifizierungsaudit.
- **CIS-Certification-Audit:** Der CIS-Auditor überprüft das Managementsystem durch multiple Stichproben auf allen Ebenen der Organisation. Ein Abschlussbericht zeigt künftige Verbesserungspotenziale auf.

- **CIS-Licence:** Mit der „Certificate Issuance & Right to Use Licence" erwerben Sie das 3 Jahre gültige CIS-Zertifikat, welches die Prozessqualität des ISMS und/oder ITSMS für Ihre Kunden sichtbar macht.
- **CIS-Surveillance-Audit:** Das einmal pro Jahr durchgeführte Surveillance-Audit überprüft die Effektivität des gesamten Managementsystems sowie seine ständige Verbesserung.
- **CIS-Recertification-Audit:** Nach 3 Jahren kann das abgelaufene Zertifikat erneuert werden.

„Vertrauensbonus bei Kunden“

Aufgrund der guten Skalierbarkeit sind ISO/IEC 27001 sowie ISO/IEC 20000 branchen- und größenunabhängig einsetzbar

Durch ihre Flexibilität und Technologieunabhängigkeit stellen die ISO-Standards der Reihen 27000 und 20000 ein umfassendes Rahmenwerk dar, das von Unternehmen und Organisationen aller Größenklassen in allen Geschäftsbereichen individuell umgesetzt werden kann.

Marcus Grausam, Director Operation:

„Als führendes Telekommunikationsunternehmen legen wir besonderen Wert auf Informationssicherheit. Mit dem ISO-27001 -Zertifikat untermauern wir das Bestreben, unseren Kunden bestes Service und höchste Sicherheit zu bieten. Periodische Audits belegen unsere kontinuierliche Weiterentwicklung.“

A1 Telekom Austria in Wien ist Österreichs größter Anbieter von Telekommunikation, Internet- und IT-Services.

Dipl.-Ing. Roland Jabkowski, MBA, Geschäftsführer:

„Unser Security-System umfasst neben IT-Sicherheit auch organisatorische und bauliche Aspekte. Diese komplexen Zusammenhänge werden durch ein ISMS nach ISO 27001 messbar und kontrollierbar. Die laufende Weiterentwicklung unserer Sicherheitsprozesse wird jährlich mittels Zertifikat bestätigt.“

Das Bundesrechenzentrum in Wien ist IT-Dienstleister und marktführender E-Government-Partner der österreichischen Bundesverwaltung.

Mag. Dr. Franz Semmernegg, Vorstand:

„Durch die unabhängige Begutachtung der CIS werden mögliche verborgene Mängel an unserem Sicherheitssystem erkannt und behoben. Das primäre Ziel unserer Zertifizierung nach ISO 27001 sehen wir jedoch darin, unseren Kunden einen international anerkannten Sicherheitsstandard zu bieten.“

Kapsch BusinessCom gehört zu den führenden Anbietern von Kommunikations-, Netzwerk- und IT-Lösungen in Österreich.

Michael Rösch, Chief Technical Officer:

„Unsere ASP-Lösung POOL4TOOL bildet ITIL-Prozesse ab. ISO 20000 ermöglicht es, die ITIL-Konformität mittels Zertifikat nachzuweisen. Daher plant Selected Services ergänzend zur ISO-27001-Zertifizierung auch die Zertifizierung nach ISO 20000. Als Vertrauenssignal an unsere Kunden.“

Selected Services ist ein Saas-Spezialist im SAP-Umfeld mit Standorten in Österreich, Deutschland, USA und Singapur.

durch ISO-Zertifikat

Dipl.-Ing. FH Dietmar Schlar, Geschäftsführer

„Durch Neuausrichtung des RRZ Süd auf den externen Markt war die Implementierung eines durchgängigen IT-Servicemanagements inklusive Kennzahlensteuerung wichtig. Mit der ISO-20000-Zertifizierung wird unsere organisationsweite Prozessorientierung in einer messbar gesteigerten Service-Qualität sichtbar.“

Die Raiffeisen Rechenzentrum Süd GmbH ist Spezialist für IT-Dienstleistungen in der Steiermark.

Dr. Gustav Jung, Qualitätsmanager

„Da die EDVG Millionen von Personendaten für Mitgliederorganisationen verwaltet, sind Datensicherheit und Service-Qualität geschäftskritische Erfolgsfaktoren. Informationssicherheit nach ISO 27001 und Service Mgmt nach ISO 20000, besiegelt durch das Zertifikat einer akkreditierten Prüforganisation, steigert den Business Value unserer Leistungen.“

Die EDV Elektronische Datenverarbeitung Service GmbH betreut als etablierter IT-Dienstleister namhafte Mitgliederorganisationen.

CIS-Zertifikate machen das hohe Niveau der Informationssicherheit oder Service-Qualität für Kunden sichtbar.

Security & Services in einem System

Integrierte Managementsysteme vereinen Informationssicherheit, IT-Services, Qualität, Umwelt oder übergeordnete Prozesse wie Planung und Strategiefindung in einem Gesamtsystem.

Immer mehr Unternehmen **nutzen die Synergien** zwischen den verschiedenen ISO-Standards und fassen **Managementthemen wie** Informationssicherheit, IT-Service-Management, Qualität oder Umwelt zu einem einheitlichen integrierten Managementsystem für das gesamte Unternehmen zusammen. **Die Vorteile sind:**

- Vereinfachtes Handling, Übersichtlichkeit, Transparenz
- Kombinierte Audits / Reviews entlasten Führungsebenen
- *Eine* Dokumentation für Management- & Businessprozesse
- Kosten- & Zeitersparnis durch Nutzung von Synergien

Die Standards für Informationssicherheit (ISO 27001), IT-Service-Management (ISO 20000), Qualitätsmanagement (ISO 9001) sowie Umweltmanagement (ISO 14000) **weisen ähnliche Strukturen auf** und stellen in vielen Punkten dieselben Anforderungen, wie zum Beispiel in der

- Verantwortlichkeit des oberen Managements,
- Zielsetzung der ständigen Verbesserung,
- Wartung und dem Betrieb der Systeme,
- Systematik der Dokumentation,
- Einhaltung der Vorgaben.

CIS bietet effiziente **Kombinationsaudits** für Integrierte Managementsysteme: „Alles aus einer Hand" durch Kooperation mit **quality**austria.

EDV Elektronische Datenverarbeitung Service GmbH, Dr. Gustav Jung, Qualitätsmanager:
„ISO 9001, ISO 27001 und ISO 20000 haben identische Elemente in der Organisation. Reviews, Gremienmeetings, Überwachungs- und Rezertifizierungsaudits werden bei uns integriert durchgeführt – mit rund 20 Prozent Zeitersparnis."

Brennercom AG; Christian Weithaler, Qualitäts- und IS-Manager:
„Wir haben die Standards für Informationssicherheit und Qualitätsmanagement zusammengelegt. Bei beiden geht es um eine effiziente Organisation unter Einbindung des Managements. Die Ergebnisse geben uns Recht!"

System-Check für das Unternehmen

Stage Reviews geben ein Plus an Sicherheit – in der Einführungsphase von Managementsystemen

Auf welchem Niveau befindet sich das implementierte Managementsystem und welche relevanten Aspekte sollten verbessert werden? Für Unternehmen, die sich in einem Zertifizierungsprozess nach ISO/IEC 27001 oder ISO/IEC 20000 befinden, erweist sich ein Stage-Review als Meilenstein auf dem Weg. Aber auch generell liefert dieses **mächtige Instrument** eine aussagekräftige **Statusbestimmung** für die Wirksamkeit von Managementsystemen mit ihren Policies, Prozessen, Kennzahlen und Maßnahmen.

Als freiwillige Vorbegutachtung im Rahmen einer Zertifizierung zeigt ein CIS-Stage-Review detailliert Stärken, Schwächen und Verbesserungspotenzial eines Informationssicherheits- oder IT-Service-Managementsystems auf. Denn sowohl ein Zuwenig als auch ein Zuviel an umgesetzten Maßnahmen kann unrentabel werden.

Das CIS-Stage-Review eignet sich daher gut als objektive **Projekt-Fortschrittsüberwachung**. Zur Durchführung einer Ist-Analyse nach ISO 27001 oder ISO 20000 werden die individuellen Anforderungen abhängig von Firmengröße und Branche, die **implementierten Prozesse** ebenso wie organisatorische Maßnahmen evaluiert und dem Anforderungsprofil des Standards gegenübergestellt. Das Ergebnis ist ein Auditbericht mit Stärken-Schwächen-Profil und gezielten Optimierungsmöglichkeiten. Ein CIS-Stage-Review umfasst drei Elemente:

Das CIS-Stage-Review

- **Auditplanung:** garantiert eine ökonomische Abwicklung
- **Audit:** Evaluierung von Anforderungen, Stärken und Schwächen im Unternehmen
- **Auditbericht:** mit Stärken/Schwächen-Analyse und Verbesserungspotenzial

Ing. Johannes Mariel,
Leitung Sicherheit und Qualität, Bundesrechenzentrum:
„Beim Aufbau eines Managementsystems bietet das Stage-Review dem Projektteam geplante Kontrollpunkte, an denen die Angemessenheit der Maßnahmen geprüft wird. Diese Zwischenbeurteilung steigert die Motivation und liefert zusätzliche Anregungen."

Ein Zuwenig oder ein Zuviel an Maßnahmen kann unrentabel werden

Personenzertifikat: Ein Schachzug für die Karriere

Praxisnahes Wissen „aus erster Hand" – direkt vom Zertifizierer: mit international anerkanntem Zertifikat

Für jene Unternehmen, die ein Managementsystem nach ISO/IEC 27001 und/oder ISO/IEC 20000 einführen, bietet die CIS normkonforme Lehrgänge mit Personenzertifikat. CIS-Trainer sind hauptberuflich in der Informationssicherheit oder im IT-Service-Management tätig und fungieren als Auditoren bei der Systemzertifizierung.

Wissen und Erfahrung fließen in die Lehrgangsinhalte ein. So garantieren Top-Trainer praxisnahe Ausbildungen auf höchstem Niveau. Aufgrund der CIS-Akkreditierung für ISO-27001-Ausbildungen durch das BMWFJ sowie für ISO-20000-Ausbildungen durch APMG, gelten Personenzertifikate als offiziell und international anerkannte Dokumente. Ein Schachzug für die Karriere.

Strategisches Zeugnis: Absolventen erhalten das offiziell anerkannte CIS-Zertifikat

INHOUSE, die Formel für den persönlichen Erfolg: INput = Highest OUtput + Secret + Efficient

Inhouse-Training: Ausbildung nach Maß

Die effizienteste Ausbildungsmöglichkeit ist Lernen im eigenen Haus, im Kreis von Kollegen und Vorgesetzten, **anhand der Fallbeispiele** aus dem eigenen Arbeitsbereich. Daher werden alle CIS-Lehrgänge – „Information Security Manager nach ISO 27001", „Information Security Auditor nach ISO 27001", „ISO 20000 Practitioner", „ISO 20000 Auditor" – auch als Inhouse-Training angeboten, wobei auch einzelne Module gebucht werden können. Darüber hinaus bietet die CIS auf Wunsch Trainings zu ausgewählten Themen aus der Informationssicherheit oder dem IT-Service-Management an.

Secret & Efficient

Inhouse-Lehrgänge sind eine attraktive Ausbildungsalternative. Vor allem für größere Unternehmen kann dies kostengünstiger und effektiver sein. Gleichzeitig wird gewährleistet, dass **Firmen-Know-how** nicht nach außen gelangt. Customizing wird bei der Inhouse-Ausbildung groß geschrieben: Die Inhalte werden auf individuelle Anforderungen zugeschnitten und während des Trainings kann gezielt auf betriebliche Fragestellungen eingegangen werden. So vermitteln Inhouse-Trainings anwendungsnahes Wissen, das unmittelbar im Arbeitsumfeld einsetzbar ist.

CIS-Lehrgangsreihe

Information-Security-Manager nach ISO 27001

Informationssicherheitsmanager nehmen jene zentrale Position im Unternehmen ein, in der **Führungs- und Technologiekompetenz** gefragt sind. Sie betreuen den Aufbau, die Implementierung sowie die ständige Verbesserung des Informationssicherheits-Managementsystems (ISMS) und fungieren als **Schnittstelle zwischen** Führungsebene und operativen Bereichen. Diese CIS-Lehrgangsreihe vermittelt kompakt und anwendungsorientiert die Kernelemente der ISO/IEC 27001 für Informationssicherheit sowie eine korrekte **Interpretation und Umsetzung**. Der Lehrgang umfasst die Module:

- Die Normen ISO 27001 / ISO 27002
- Psychologische Grundlagen
- Rechtsgrundlagen
- Abschlussprüfung

Der erfolgreiche Abschluss der Prüfung wird mit dem staatlich anerkannten **CIS-Personenzertifikat** bescheinigt, das auch international gültig ist.

Die ISMS-Normen ISO 27001-27002
2 Tage

Psychologische Grundlagen für IS-Manager
1 Tag

Rechtsgrundlagen für IS-Manager
1 Tag

Prüfung IS-Manager
1 Stunde

Zertifikat IS-Manager

CIS-Lehrgangsreihe

Information-Security-Auditor nach ISO 27001

Das interne Audit gilt als mächtiges Instrument für die Weiterentwicklung von Managementsystemen. Diese CIS-Lehrgangsreihe vermittelt systemische Techniken, um betriebliche Gegebenheiten nach unterschiedlichen Aspekten analysieren zu können, um Schwachstellen oder Doppelgleisigkeiten zu erkennen und **Optimierungspotenzial** zu eruieren. Erprobte Audit-Techniken werden geübt: Auditarten, Auditprinzipien und die **Auditvorbereitung** gehören ebenso dazu, wie das Erstellen von Audit-Dokumenten oder **Checklisten**, die Durchführung des Vor-Ort-Audits, der Auditbericht sowie Korrekturmaßnahmen. Die Module sind:

- Technische Einstiegsprüfung
- Psychologische Grundlagen*
- Audittechniken
- Abschlussprüfung

Ein gültiges IS-Manager-Zertifikat ist Teilnahmevoraussetzung. Die Ausbildung schließt mit dem staatlich anerkannten **CIS-Personenzertifikat** ab.

Technische Einstiegsprüfung

*Psychologische Grundlagen für IS-Auditoren**
2 Tage

Audittechniken
1 Tag

Prüfung IS-Auditor
1 Stunde

Zertifikat IS-Auditor

* Dieser Teil ist durch eine Ausbildung zum Auditor / Fachauditor gemäß ISO 19011 abgedeckt.

CIS-Lehrgang

ISO 20000 Practitioner

Beziehung ISO 20000 / IT-Service-Management
Certification Readiness Assessments und Audits
Applicability, Eligibility and Scoping
Statusanalyse, Improvement, Implementation Plan
Continual Improvement Processes
Vorbereitung auf ISO-20000-Zertifizierung
3 Tage

Prüfung ISO 20000 Practitioner
2 Stunden

Zertifikat Practitioner ISO/IEC 20000

Implementieren, steuern, verbessern: Der ISO-20000-Practitioner verbindet Technologie- und Managementwissen gleichermaßen. Implementierung, Zieldefinition, Scoping, der kontinuierliche Verbesserungsprozess und die Vorbereitung auf Audits gehören zu den im Lehrgang vermittelten Kompetenzen. Absolventen sind in der Lage die Anforderungen der ISO/IEC 20000 in einer Organisation umzusetzen, auf die Zertifizierung vorzubereiten und das Managementsystem effizient zu steuern sowie auch weiter zu entwickeln. Diese Qualifikationen befähigen dazu, Systemverantwortung zu tragen. Inhalte des 3-tägigen Lehrgangs: siehe Grafik.

Teilnahmevoraussetzung ist ein ITIL Foundation Certificate. Die Ausbildung schließt mit Prüfung und anerkanntem **Personenzertifikat** ab.

CIS-Lehrgang

ISO 20000 Auditor

Anforderungen, Ziele, Anwendung der ISO 20000
Prinzipien des IT-Service-Management
Eligibility und Scoping
Anwendung / Relevanz von ISO 20000-2 bei Audits
Pre-Audits, Zertifizierung, Surveillance Audits
2 Tage

Prüfung ISO 20000 Auditor
1 Stunde

Zertifikat Auditor ISO/IEC 20000

Mit einschlägiger praktischer Erfahrung und tiefgehendem Normwissen fungiert ein ISO-20000-Auditor als oberste Instanz für ITSM-Systeme. Der CIS-Lehrgang befähigt zur Durchführung von Audits und Assessments. Absolventen erkennen Normkonformität, Abweichungen sowie Optimierungspotenziale und sind qualifiziert, um neben der Durchführung interner Audits auch als Auditor für akkreditierte Zertifizierungsorganisationen oder als Berater mit dem Fokus auf Audits und Assessments nach ISO/IEC 20000 zu arbeiten. TN-Voraussetzung: Qualifizierter Auditor nach ISO 9000 / 27001, TickIT, IRCA, CISA und 3 Jahre Auditerfahrung. Inhalte des 2-tägigen Lehrgangs: siehe Grafik.

Teilnahmevoraussetzung: gültige Auditor-Qualifikation. Die Ausbildung schließt mit Prüfung und anerkanntem **Personenzertifikat** ab.

Zehn Gründe...

...warum sich „Management mit System“ rechnet

Informationssicherheit nach ISO/IEC 27001
und IT-Service-Management nach ISO/IEC 20000:

- vermeiden Fehlerquellen von Einzelmaßnahmen
- bieten Investitionsschutz durch kontinuierliche Verbesserung
- bringen Wettbewerbsvorteile durch das anerkannte ISO-Zertifikat
- bewirken eine ständige Verbesserung von Prozessen und Maßnahmen
- machen die Wirksamkeit von Maßnahmen messbar, steuerbar, vergleichbar
- lassen sich mit anderen ISO-Standards in einem integrierten System abbilden
- sind anwendbar für jede Unternehmensgröße und Branche
- basieren auf internationalen Good-Practice-Methoden
- bringen verborgene Mängel ans Licht
- minimieren die Haftung vor Gericht

CIS - Secure Your Business

Management mit System

nach ISO 27001 und ISO 20000...

...passt für Unternehmen
jeder Größe und Branche

CIS - Secure Your Business

CIS - Certification & Information Security Services GmbH
A-1010 Wien . Salztorgasse 2/6/14 . T: (+43)-1-532 98 90 . F: (+43)-1-532 98 90 109
E-Mail: office@cis-cert.com . Web: www.cis-cert.com . FN 206298 f beim HG Wien . DVR: 1077864