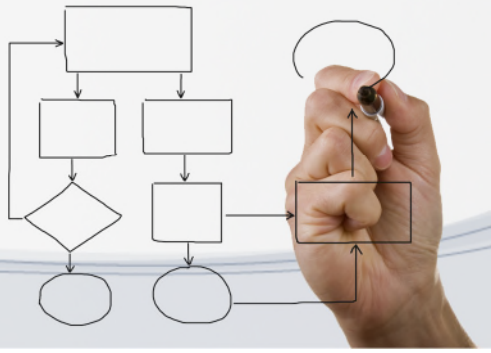
Geschäftsbereich **Betrieb und Service**



ISMS-Zertifizierung für die Dr. Glinz COVIS® GmbH

Erfolgreicher Aufbau und Zertifizierung eines Information Security Management Systems (ISMS) nach ISO 27001.

Mit viel Euphorie gestartet, wurde dem ISO 27001-Projektteam schon nach relativ kurzer Zeit klar, dass der Aufbau eines Managementsystems der Informationssicherheit nach ISO 27001:2013 mal nicht so nebenbei zu realisieren ist und das Unternehmen vor einer großen Herausforderung steht. Und ohne externe Unterstützung war dies auch nicht zu bewerkstelligen. Die entsprechende Unterstützung beim Aufbau des dazu notwendigen Information Security Management Systems (ISMS) fand COViS mit der socos GmbH. Aufbauend auf der Kompetenz und Erfahrung der externen Berater ist es der Dr. Glinz COViS GmbH jetzt erstmals gelungen die Zertifizierung zu erlangen.

Über COViS

Ihr Full-Service IT Dienstleister für agile Lösungen

Die Dr. Glinz COViS® GmbH ist ein unabhängiges und inhabergeführtes IT–Dienstleistungsunternehmen mit Sitz in Düsseldorf.

Die Dr. Glinz COViS® GmbH bietet IT-Lösungen aus einer Hand. Von IT-Beratungsleistungen im Bereich Prozess- und Projektmanagement, über Analyse, Design und Entwicklung von Softwarelösungen, bis hin zu deren Test, Qualitätssicherung und Betrieb, stellen wir seit über 30 Jahren kontinuierlich ein vollständiges Leistungsspektrum über die gesamte Wertschöpfungskette bereit.

Mit weit über 150 erfolgreichen Projekten im In- und Ausland und der langjährigen Erfahrung ihrer Mitarbeiter gehört die Dr. Glinz COViS® GmbH zu den etablierten Anbietern im Markt für individualisierbare Softwarelösungen. Zu unseren Kunden zählen neben großen Konzernen auch mittelständische Unternehmen. Wir bedienen auf der Basis unserer Softwaremodule Projekte unterschiedlichster Größenordnung - von der Standardlösung bis hin zur hochindividualisierten Plattform.

Als Full-Service IT-Dienstleister mit eigenem Rechenzentrumsstandort in Düsseldorf decken wir mit unserem End-to-end-Portfolio den gesamten Wertschöpfungsprozess von Beratung & Design über Entwicklung bis hin zur Integration und Betrieb der Systeme ab.

Der Bereich Betrieb und Service bietet folgende Leistungen an:

- Server Housing: Bereitstellung, Betrieb und Betreuung von Webservern, Datenbanken und Storage-Systemen
- Managed Services: System-Management, Monitoring sowie Sicherung und Wiederherstellung von Daten, Analysen und Performance Engineering
- Co-Location: Stellfläche für Racks und Höheneinheiten zur Unterbringung und Netzanbindung von Kundenservern
- Hosting: Bereitstellung von Domains, Webspeicher, Webdatenbanken, Statistiken, E-Mail-Hosting für Websites
- Storage-Virtualisierung für optimale Absicherung vor Datenverlust
- Security von höchstem Anspruch durch Systeme von F5, CheckPoint und Cisco, redundante Firewall-Systeme
- Datenbanksysteme wie MS SQL2008-2014, Mongo DB und ElasticSearch
- Abgestimmte Serviceprozesse nach ITIL 2011-Standard
- Umfangreiche Zugangskontrollen und Videoüberwachung
- Löschanlagen nach modernstem Stand der Technik
- Betrieb von Backup- oder redundanten Systemen in verschiedenen Brandabschnitten
- Permanentes 24/7-Monitoring der Zugriffe auf alle Systeme
- Fortlaufende Überarbeitung unserer Sicherheitskonzepte durch eigenen zertifizierten Security-Manager
- Green Engineering mit Ökostrom

Unser COViS® Hochleistungs-Rechenzentrum in Düsseldorf ist schon seit 2012 nach ISO 9001 und ISO 27001 zertifiziert.

Ausgangslage

Alle Mitarbeiter im Betrieb und Service der Dr. Glinz COViS® GmbH kommen täglich mit sensiblen Daten von Kunden in Kontakt. Dem angemessenen Schutz dieser Informationen kommt eine große Bedeutung zu. Mithilfe von rund 25 Mitarbeitern werden dabei folgende Dienstleistungen und Produkte erbracht:

- Managed Services
- Hosting
- Betrieb und Pflege von Management-Systemen

Informationen können vorliegen:

- in Form digitaler Daten (Festplatten, Bänder, optische Datenträger, USB-Sticks etc.), die über Netzwerke übertragen werden können
- in Papierform, ausgedruckt oder handschriftlich, die über postalische Sendungen oder Fax Nachrichten weitergeleitet werden können
- in sprachlicher Form als mündliche Konversation oder per Telefon weitergegeben.

Informationssicherheit ist integraler und essentieller Bestandteil aller Geschäftsprozesse der Dr. Glinz COViS® GmbH. Sie dient der Wahrung der nachfolgenden Grundeigenschaften von Informationen:

- Vertraulichkeit

Informationen oder Funktionen dürfen nur dem berechtigten Personenkreis zur Verfügung stehen.

- Integrität

Die Unversehrtheit von Informationen ist jederzeit sicherzustellen. Informationen müssen korrekt und vollständig sein, Funktionen müssen korrekte Ergebnisse liefern. Dabei muss auch die Vertrauenswürdigkeit der jeweiligen Informationsquellen sichergestellt sein.

- Verfügbarkeit

Die Nutzung von Informationen oder Funktionen muss dem berechtigten Personenkreis in dem benötigten Zeitraum mit der erforderlichen Güte möglich sein.

Darüber sollte ein weiteres Ziel der Informationssicherheit des Unternehmens sein, die betriebliche Geschäftskontinuität zu gewährleisten. Dabei sollen potentiell auftretende Schäden für das Unternehmen minimiert werden, indem durch zeitnahe und angemessene Korrekturen sowie Vorbeugungs- und Korrekturmaßnahmen die Auswirkungen von Sicherheitsvorfällen jeglicher Art so gering wie möglich gehalten werden.

Dies gelingt nur, wenn:

- wertvolle oder sensible Informationen vor unbefugtem Zugriff geschützt werden
- die Richtigkeit und Vollständigkeit von Informationen vor unbefugter Änderung bewahrt werden
- die Verfügbarkeit von Informationen und vitalen Diensten sichergestellt ist, sobald sie benötigt werden

Neben den organisationseigenen Standards der Dr. Glinz COViS® GmbH sind normative, rechtliche, vertragliche und organisatorische Anforderungen zu erfüllen.
Aus diesem Grund hat sich Dr. Glinz COViS® GmbH im Januar 2014 entschieden, nach dem Rechenzentrum nun den Betrieb und Service nach dem internationalen Sicherheitsstandard ISO/IEC 27001 zertifizieren lassen.

Das Projekt

Verantwortlich für die Implementierung, Pflege sowie wirksame Aufrechterhaltung des ISMS der Dr. Glinz COViS® GmbH ist die Leitung Betrieb und Service mit seinen Mitarbeitern.

Als Grundlage für den Aufbau des ISMS wurden die Dokumente “Leitlinie zu Informationssicherheit“ und “Anwendungsbereich des ISMS der Dr. Glinz COViS® GmbH“ erstellt.

Die Geschäftsführung und -leitung der Dr. Glinz COViS® GmbH unterstützte und genehmigte die wirksame und dauerhafte Implementierung eines ISMS nach ISO/IEC 27001:2013 im Rahmen des ausgewiesenen Anwendungsbereichs.

Das Projektteam führte anhand einer an die ISO 27001 Anhang A angelehnte "Orientierungsliste" eine Ist-Analyse im Unternehmen durch, die Nichtkonformitäten gegenüber der ISO-Norm aufdeckte. Parallel dazu wurde mit den Prozesseigentümern eine Bewertung der Risiken bezüglich der Informationssicherheit vorgenommen.

Jede Nichterfüllung und jedes Risiko wurden dabei in ihrer Auswirkung auf die eigentlichen Geschäftsvorfälle der Dr. Glinz COViS® GmbH bewertet. Hieraus wurde ein Maßnahmenkatalog abgeleitet, der bei der Geschäftsleitung vorgestellt wurde.

In Abstimmung mit dieser wurden Maßnahmen zur Umsetzung beschlossen, die den Kern des Projektauftrages für das Projektteam bildeten. Die Priorisierung der Maßnahmen erfolgte wiederum unter dem Aspekt der Kritikalität der im Scope stehenden Geschäftsvorfälle.

Das Projektteam

Das Projektteam, bei Übergabe des Zertifikates, von links nach rechts: Jörg Crämer - IT Security und Datenschutzbeauftragter, Jens Heinen - QS Manager, Klaus Ruschel - Projektleiter und Leiter Betrieb und Service, Enrico Endruschat - Leiter IT und Loran Rajic - Servicemanager

Die Umsetzung

Zu Beginn des Projektes wurde in einem Workshop mit der Geschäftsleitung und dem Projektteam der Scope definiert und die Projektplanung abgestimmt.

Wesentlich für den Erfolg des Projektes war in allen Phasen die Unterstützung der Geschäftsleitung, die durch klare Zielsetzung und die Genehmigung der Leitlinien den Mitarbeitern die Sicherheit und Motivation gab, die für einen Projekterfolg enorm wichtig sind.

In zahlreichen Workshops, begleitet durch kompetente Unterstützung der socos GmbH, wurden die Themen aus dem Maßnahmenkatalog behandelt.

Bereits am Anfang wurde klar, dass neben der Kenntnis des Sicherheitsmanagements auf der Basis des BSI IT-Grundschutzes, insbesondere die Kenntnis aller zur IT-Infrastruktur gehörenden Objekte und die Analyse des tatsächlichen Schutzbedarfs von immenser Bedeutung sind.

Eine Vielzahl von Informationen und Daten ergaben, dass die Abbildung der Infrastruktur in Anlehnung an den BSI IT-Grundschutz und die Bewertung von Maßnahmen nur toolgestützt erfolgen kann. Die Auswahl fiel auf den Microsoft System Center Service Manager, welcher bereits als Ticket-Tool im Einsatz war. Im Rahmen der Erweiterung wurden nun das ISMS und die CMDB (Configuration Management Database) in das Tool integriert.

Dieser ganzheitliche Ansatz und die zielorientierte Arbeitsweise führten bereits nach kurzer Projektlaufzeit zu sichtbaren Ergebnissen und damit zu der Möglichkeit, zahlreiche Verbesserungen in den Prozessen aufzuzeigen.

Durch die Einbindung aller Mitarbeiter der Dr. Glinz COViS® GmbH, also auch die der Bereiche Entwicklung und Projektmanagement, durch Schulungsmaßnahmen und Informationsveranstaltungen, konnte das Projekt eine hohe Akzeptanz im Unternehmen erreichen.

Mit dem Aufbau eines ISMS gemäß ISO 27001, sowie der dazu notwendigen Organisation inklusive der Einbindung in bestehende Managementsysteme, wird COViS den Anforderungen an die Informationssicherheit gerecht.

Im Rahmen des umfangreichen Maßnahmenpaketes, wurde die professionelle Erweiterung der bestehenden Sicherheitsorganisation, die komplette Überarbeitung der internen Weisungen zum Schutz von Informationen und Informations- und Kommunikationstechnik Systemen (IKT-Systeme) durchgeführt.

Des Weiteren erfolgte eine Klassifizierung aller relevanten Informationen, Applikationen, ICT-Systeme, Informationsverarbeitungsprozesse und Lokalitäten.

Im Zuge der Erfüllung bestehender Compliance-Forderungen, als auch von Anforderungen des Qualitätsmanagements, wurde ein Notfall- und BCM-Handbuch erstellt. Insgesamt wurden im Rahmen des Projektes weit über 100 Dokumente neu erstellt oder überarbeitet. Entsprechende Notfallübungen wurden festgelegt und zum Teil schon durchgeführt.

Nebenbei konnten für die komplette Belegschaft der Dr. Glinz COViS® GmbH Verbesserungen in Sachen Arbeitsschutz, wie zum Beispiel Austausch der gesamten Arbeitsplatz-Bildschirme, erreicht werden.

Die Einhaltung der Anforderungen aus der ISO 27001 wurde im Rahmen eines umfangreichen Audits durch die akkreditierte Zertifizierungsstelle BSI bestätigt. Nach Erstellung des Auditberichts, der nur geringfügige Verbesserungspotentiale aufzeigte, konnten die Auditoren ein positives Gesamtvotum geben. Im Oktober 2015 wurde das Zertifikat, nach eingehender Prüfung des Auditberichts, durch das BSI schließlich der Dr. Glinz COViS® GmbH verliehen.

Mit der Zertifizierung nach ISO/IEC 27001:2013 liefert die Dr. Glinz COViS® GmbH den Nachweis, dass sie mit den ihr anvertrauten Informationen sicher umgeht und Informationssicherheit ein zentrales Element der täglichen Arbeit ist.

Im Jahr 2016 wird das erste Überwachungsaudit durchgeführt, für eine Re-Zertifizierung ist die Dr. Glinz COViS® GmbH gewappnet. Der Aufwand hat sich nach Überzeugung aller Verantwortlichen gelohnt. Das Projekt hat konsequente Sicherheitsprozesse und ein durchgängiges, hohes Sicherheitsniveau etabliert.

In allen Phasen der Zertifizierung war die aktive Einbindung der Geschäftsleitung gegeben. Die Audittätigkeiten wurden durch das Management auf vorbildliche Weise unterstützt. Die Überprüfung durch die unabhängigen externen Berater der socos GmbH wurde als äußerst hilfreich empfunden.

Die Geschäftsführung und -leitung der Dr. Glinz COVIS® GmbH bekennt sich zum Betrieb und zu einer kontinuierlichen Verbesserung eines ISMS, sowie der Einhaltung anwendbarer rechtlicher, vertraglicher sowie organisationseigener Vorgaben, um den Erwartungen interessierter Parteien an die Informationssicherheit auf einem hohen Stand zu entsprechen.

Um diesen Anforderungen gerecht zu werden, sieht die Geschäftsführung und -leitung die Umsetzung und Erhaltung des ISMS-Programms als eine Verpflichtung im Rahmen der laufenden Geschäftsprozesse an.

Dank sagt das Projektteam den Mitarbeitern der Dr. Glinz COViS® GmbH, insbesondere der IT Operation, für viele Überstunden und die konstruktive Unterstützung bei der Umsetzung der Maßnahmenpakete.

Klaus Ruschel

Düsseldorf, den 10.02.2016