

ISO 27001 der Standard für Sicherheit und Vertrauen

Jedes Geschäft braucht Vertrauen. Mit einer Zertifizierung Ihrer Informationssicherheit nach dem internationalen Standard ISO/IEC 27001 schaffen Sie Vertrauen bei Ihren Kunden. Nutzen auch Sie diesen Vorteil. Wir wissen, wie Sie dieses Ziel erreichen können - vielleicht einfacher als Sie meinen.

Was ist die DIN ISO/IEC 27001

So wie die bekanntere Norm ISO 9001 für Qualitätsmanagement steht, ist die DIN ISO/IEC 27001 der maßgebliche internationale Standard für Informationssicherheit. Sie ist Teil der Normenfamilie ISO 27000 ff die Anforderungen und Maßnahmen für ein Informationssicherheits-Managementsystem (ISMS) beschreibt. Die ISO 27001 beschreibt die Kriterien und Voraussetzungen für eine Zertifizierung.

Welche Vorteile bietet eine Zertifizierung

Das Vertrauen der Kunden ist äußerst wichtig für alle Unternehmen, in denen Informationen verarbeitet werden. Aus der Sicht des Kunden ist es schwierig die Informationssicherheit und damit Vertrauenswürdigkeit Ihrer Firma zu beurteilen. Mit einer Zertifizierung nach der international anerkannten Norm ISO 27001 weisen Sie den hohen Stand Ihrer Informationssicherheit nach.

Gesetzliche Anforderungen

- Als Geschäftsführer weisen Sie durch die Implementierung eines Informationssicherheitsmanagements gemäß ISO 27001 nach, dass Sie Ihren Verpflichtungen aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sowie dem Aktiengesetz (AktG) und dem GmbH-Gesetz (GmbHG) nachgekommen sind.
- Als Cloud-Dienstleister können Sie aufwendige Audits durch Kunden im Rahmen der Auftrags-Datenverarbeitung nach Vorgabe des Datenschutzgesetzes (BDSG) vermeiden.
- Die Bundesregierung hat einen Gesetzesentwurf (IT-Sicherheitsgesetz, KRITIS) beschlossen, das nach Verabschiedung Provider kritischer Infrastrukturen (z.B. Telekommunikation) verpflichtet die IT-Sicherheit ihrer Infrastruktur nachzuweisen.
- Der Sicherheitskatalog gem. § 11 Abs. 1a EnWG verpflichtet zukünftig Energieversorger zu einer Zertifizierung nach DIN ISO/IEC 27001 unter Berücksichtigung der DIN SPEC 27009. .
- Als Unternehmen im Bereich der Finanzwirtschaft erfüllen Sie mit einer Zertifizierung die *Mindestanforderungen an das Risikomanagement - MaRisk* der Bafin.

Wie kann die Süd IT Sie unterstützen

Unsere erfahrenen Mitarbeiter, die selbst ausgebildete Auditoren sind, helfen Ihnen Ihr Ziel schnell und mit möglichst geringen Kosten zu erreichen.

Den Weg zu einem Informationssicherheits-Managementsystem nach ISO 27001 gehen wir Schritt für Schritt mit Ihnen gemeinsam, so dass Sie jederzeit die volle Kontrolle über die Kosten und den Überblick über den Projektfortschritt behalten.

ISO 27001 - der Standard für Sicherheit und Vertrauen

Schritt 1 - Kompaktanalyse:

Die Kompaktanalyse erfolgt anhand von Checklisten und einer Besichtigung Ihrer Infrastruktur. Als Ergebnis der Kompaktanalyse erhalten Sie eine Beurteilung der Informationssicherheit Ihres Unternehmens und einen Überblick über die Aufwände, die für eine Zertifizierung erforderlich wären.

Auch wenn Sie noch keine Zertifizierung planen, kann die Durchführung einer Kompaktanalyse sinnvoll sein, um eine unabhängige Beurteilung des Status Ihrer Informationssicherheit zu erhalten.

Schritt 2 - Planung und Umsetzung eines ISMS

Unsere erfahrenen Mitarbeiter wissen genau, was zu tun ist. Zielsicher erarbeiten sie mit Ihnen die für Sie passenden Prozesse und Dokumente. Sie stellen sicher, dass die Forderungen der Norm ohne unnötigen Ballast erfüllt werden.

Wir können Ihnen als "Bergführer" den Weg zeigen, oder als "Sherpa" einen Großteil der Last tragen. Die Aufteilung der Arbeiten passen wir dabei ganz Ihren Wünschen, Ihrem Budget und Ihrem Zeitplan an.

Schritt 3 - Pflege und Verbesserung

Die kontinuierliche Pflege und Verbesserung muss naturgemäß im Rahmen des täglichen Geschäftes erfolgen. Gerne unterstützen wir Sie bei der Planung und Umsetzung eines kontinuierlichen Verbesserungsprozesses und/oder unterstützen Sie auch kontinuierlich mit kompetenten Mitarbeitern.

Schritt 4 - Interne Audits

Die geplante Durchführung von internen Audits ist Teil der Norm-Forderungen und soll durch externe Mitarbeiter erfolgen. Unabhängig von den vorhergegangenen Schritten führen wir interne Audits durch, mit denen Sie optimal auf eine Zertifizierung vorbereitet werden.

Schritt 5 - Begleitung bei der Zertifizierung

Unsere Berater sind selbst Auditoren und kennen die Anforderungen genau. Gerne beraten wir Sie bei der Auswahl eines Zertifizierers und nehmen begleitend und unterstützend am Zertifizierungs-Audit, z.B. durch den TÜV, teil.

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontaktaufnahme

Dr. Stefan Krempf
089 461 3505 12
krempf@sued-it.de
ISO 27001 Auditor, Datenschutzbeauftragter

