



# ISO/IEC 27001

Informationssicherheit mit System – effizient, preiswert und toolunterstützt

Wenn Sie nach der ISO-Norm 27001 zertifiziert sind, dann erfüllt Ihr Unternehmen die Anforderungen an ein funktionsfähiges IT-Sicherheits-Management. Gerade Unternehmen mit sensiblen Kundendaten, wie z. B. Versicherungskonzerne wollen ihren Kunden zeigen, dass sie keine Angst vor Datenmissbrauch haben müssen. Automobilzulieferer dagegen müssen aktiv zur Sicherheit entlang der Wertschöpfungskette beitragen. Sie sorgen mit dafür, dass bei der Produktentwicklung die Risiken minimiert werden und geraten so positiv in den Fokus der Automobilhersteller.

## **SICHERHEIT GEGEN DATENMISSBRAUCH UND ENTLANG DER WERTSCHÖPFUNGSKETTE**

Sie erhalten mit der ISO/IEC 27001 einen Prozessansatz „was“ zu tun ist, um die Qualität der Informationssicherheit einer Organisation zu verbessern, nicht jedoch „wie“ dies im Detail technisch durchzuführen ist. Ihr Information Security Management Systems (ISMS) erfährt eine eingehende Überprüfung für alle Bereiche. Der Kern des Standards sind die Themengebiete Risikoanalyse und Risikomanagement. Nur eine sorgfältig durchgeführte Analyse der Sicherheitsrisiken ermöglicht ein kosteneffizientes Management von Risiken und Gefährdungen. Das Ergebnis der Risikoanalyse zeigt, wo der Schuh am meisten drückt und welche IT-Sicherheitsmaßnahmen umgesetzt werden sollten und welche weniger wichtig sind.

## **GEFAHREN FÜR FIRMEN UND GESCHÄFTSFÜHRER**

Nicht nur der Bereich der klassischen IT-Sicherheit birgt Gefahren für Firmen und Geschäftsführer. Auch der Verstoß gegen eine Vielzahl von gesetzlichen Vorgaben (Compliance-Anforderungen) kann schwerwiegende Folgen haben, wie unzählige Verstöße gegen das Bundesdatenschutzgesetz zeigen. Allein bei der privaten Nutzung von E-Mail am Arbeitsplatz kommt eine Vielzahl von Paragraphen zum tragen, die im Einzelfall zu bösen Überraschungen führen können. Mit ISO/IEC 27001 werden auch Compliance-Anforderungen in die Risikobetrachtung mit einbezogen und ermöglicht so ein prozessorientiertes, ganzheitliches und transparentes Management der operativen Risiken einer Organisation.

## **EIN STANDARD, DER FÜR ALLE ORGANISATIONEN WICHTIG IST**

Insbesondere dann, wenn es um den Datenschutz geht, wird die ISO/IEC 27001 relevant. Besonders im Finanz- und Gesundheitswesen, im öffentlichen Dienst oder IT-Sektor ergeben sich Schwerpunkte. Unternehmen, die von ihren Kunden persönliche Daten anvertraut bekommen, werden großen Nutzen aus der ISO/IEC 27001 ziehen. Die Kunden gewinnen durch die Zertifizierung die Gewissheit, dass ihre Daten geschützt sind. Sie müssen Ihren Kunden gegenüber also nachweisen, dass Sie Ihre Informationssicherheit „im Griff“ haben. Dazu müssen Sie ein ISO/IEC 27001 konformes Information Security Management Systems zumindest im Aufbau haben. Ihren Kunden gibt es Gewissheit darüber, dass ihre Daten bei Ihnen gut aufgehoben sind. Dazu müssen Sie Vertrauen und Verlässlichkeit schaffen. Ihrem Unternehmen hilft die Zertifizierung nach ISO/IEC 27001 dabei, lebensnotwendige Informationen zu verwalten und zu schützen.

## **MINIMIERUNG DER HAFTUNGSRISIKEN DURCH EIN ZERTIFIZIERTES ISMS**

Das erste Ziel muss es sein, die Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen zu kennen, die dann an die Besonderheiten der einzelnen Organisationen angepasst werden. Damit haben Sie die Möglichkeit geeignete und angemessene Sicherheitskontrollen auszuwählen. Diese Sicherheitsmechanismen dienen dem Schutz sämtlicher Werte in der Wertschöpfungskette. So schaffen Sie die Voraussetzungen für den systematischen Aufbau eines prozessorientierten Managementsystems.

Schon die erste Stufe der Risikoanalyse reduziert die Haftungsrisiken für Geschäftsführer. Nachdem die Risiken bekannt sind, schließt sich in der Folge die Risikobehandlung, das Risikomanagement und der Aufbau der ISMS-Dokumentation an. Wenn Sie schon ein Qualitätsmanagementsystem nach DIN EN ISO 9001 oder ITIL im Einsatz haben, dann lässt sich ein ISMS nach ISO 27001 kostengünstig darauf aufbauen.

**Unsere Experten prüfen für Sie mögliche staatliche Förderungen der Länder und beraten Sie.**

## VERTRAUENS BASIS SCHAFFEN

Ganz eindeutig bauen Sie mit einer Zertifizierung Vertrauen gegenüber Ihren Kunden auf. Bescheinigt durch unabhängige Auditoren, weisen Sie nach, dass Ihre Informationen geschützt und sicher sind. Durch unsere Beratungsleistung ergeben sich für Sie folgende Mehrwerte:

- Kosteneffizienz durch potentielle staatliche Fördermittel
- Reduzierung von Kosten und Risiken des Projektes durch ein Festpreis-Angebot
- Transparenz Ihrer IT-Risiken und deren Schäden
- Planungssicherheit in welche Schutzmaßnahme Sie wann investieren sollten
- Übersichtlichkeit und Nachvollziehbarkeit Ihrer Prozesse
- Gesetzeskonformer Betrieb Ihrer IT– BDSG, GDPdU, StGB, TKG usw. sind keine Bedrohung mehr für Sie
- Neukundengewinnung durch Vertrauensbildung

## WIR BEREITEN SIE AUF DIE ZERTIFIZIERUNG VOR

Niemand kennt Ihre Firma besser als Sie und Ihre Mitarbeiter. Deshalb bieten wir Ihnen mit unseren erfahrenen Beratern eine gemeinsame Vorbereitung auf eine ISO/IEC 27001 Zertifizierung. Ein Dienstleistungs- und Softwareangebot kann Ihren Wünschen entsprechend flexibel gestaltet werden und gerne zum Festpreis erfolgen. Vielleicht ist aber auch schon unser Gesamtpaket oder das Zwei-Tage-Paket für Sie interessant:

### Gesamtpaket:

- Workshop zur Einführung in die Vorgehensweise
- Toolgestützte Risikoanalyse nach einem internationalen Standard
- Toolgestützte Implementierung Ihres Information Security Management Systems
- Beratung und Betreuung bei der Erstellung von Policies und Dokumenten
- Vorbereitung auf das Zertifizierungsaudit

Förderung durch die Landesregierung möglich, wie z. B. in Baden-Württemberg.

Gerne besprechen wir gemeinsam mit Ihnen Ihre Anforderungen in einem ersten unverbindlichen Gespräch.

### Zwei-Tage-Paket:

- Analyse Ihrer Informationssicherheit nach ISO/IEC 27001
- Bericht über die Ist-Situation
- Empfehlungskatalog

## Zertifizierte Berater

Unsere Berater belegen ihre Kompetenz durch Zertifikate nach den etablierten Standards. Dazu gehören Zertifikate der IT Infrastructure Library (ITIL), des Examination Institute for Science (EXIN), des Bureau Veritas Quality International (BVQI) und nach ISO 9001 / 2000. Sie sind qualifizierte Berater als Sachverständige für IT-Security / IT-Sicherheit.



Hamburg  
T +49 40 675968-0

Frankfurt  
T +49 69 6607680-0

München  
T +49 89 925191-0

Zürich  
T +41 52 62008-80

Düsseldorf  
T +49 211 577996-0

Stuttgart  
T +49 7195 92255-0

Wien  
T +43 1 5222015 -10

[kontakt@voquz.com](mailto:kontakt@voquz.com)  
[www.voquz.com](http://www.voquz.com)