

ISO Standard 27001

Compliance vs. pragmatische
Orientierung am Standard



ISO Standard 27001 - Compliance vs. pragmatische Orientierung am Standard

Jedes Unternehmen benötigt IT-Sicherheit. Das eine mehr - das andere weniger. Gesagt getan: Aber wie bewahre ich mein Unternehmen vor dem Schlimmsten, ohne dabei mehr Aufwand zu betreiben als notwendig ist? In dieser Kurzübersicht zeigen wir Ihnen, wie es geht und wie Sie die Sicherheit erzielen, die Ihr Unternehmen benötigt: Auf den Punkt!

DAS MASS ENTSCHIEDET

In der IT-Sicherheit kommt es entscheidend auf das passende Maß an. Denn während ein Zuviel an IT-Sicherheit weder praktisch in der Anwendung noch wirtschaftlich vertretbar ist, kann ein Zuwenig an IT-Sicherheit fatale Folgen haben.

WAS RECHT UND BILLIG IST

In erster Linie sind es die finanziellen Aspekte, die das Maß an IT-Sicherheit in Unternehmen motivieren und weniger die rechtlichen. Prinzipiell ist das sogar auch OK so. Denn die Gesetzgebung fordert zu einer den Umständen eines Unternehmens entsprechenden Risikovorsorge auf, bei der natürlich auch die finanzielle Ausstattung eine Rolle spielt. Dabei gilt die Faustformel: Je mehr Einfluss Elemente auf die Ausführung geschäftskritischer Prozesse besitzen, desto höher ihr Schutzbedarf. Weniger relevante Bereiche sollen demnach gar nicht mit erhöhtem Aufwand angegangen werden. Folglich kann das Ziel nur lauten: **Die Risiken durch den Einsatz der IT mit angemessenen Maßnahmen auf ein tragbares Niveau zu reduzieren.**

RESTRISIKEN

IT-Risiken komplett ausschalten zu wollen bedeutet, mit Kanonen auf Spatzen zu schießen. Im Sinne einer Angemessenheit und Tragbarkeit dürfen und sollen Restrisiken also durchaus bestehen bleiben. Der Gesetzgeber erwartet allerdings, dass sie nachvollziehbar sind und soweit entschärft werden, dass sie den Geschäftsbetrieb im Eintrittsfall nicht maßgeblich gefährden.

KEINE VERNÜNFTIGE SICHERHEIT OHNE METHODIK

Wer sich seiner IT-Risiken bewusst werden will, muss sie methodisch analysieren. Nur so lassen sich alle Problemfelder organisiert, arbeitsökonomisch und vor allem kosteneffizient identifizieren, bewerten und beseitigen. Natürlich erfordert dies einen gewissen Aufwand: Sie können sich allerdings sicher sein, dass Sie so nicht nur die sichtbare Spitze des Eisberges bearbeiten, sondern auch das, was Ihnen auf den ersten Blick verborgen blieb und worauf sie eventuell niemals gekommen wären. Und genau darauf kommt es doch auch an.

Auf der rechten Seite dieser Kurzübersicht stellen wir Ihnen zwei praxisbewährte Methoden mit allerdings recht unterschiedlichen Ansprüchen vor. Die Grundideen beider Varianten verdeutlichen wir vorab an einem Beispiel.

BEISPIEL:

Im Bereich der KFZ-Versicherungen wird über die Haftpflichtversicherung hinaus zum Beispiel auch ein Schutzbrief sowie eine Insassen-, Teil- oder Vollkaskoversicherung angeboten.

Die sich stellenden Fragen lauten: Was brauche ich wirklich? Was ist finanziell machbar bzw. sinnvoll? Welche Risiken gehe ich bei Verzicht ein? Genau um diese Fragen dreht es sich auch bei der IT-Sicherheit.



WAS MAN WEISS HAT MAN SICHER, WAS MAN SICHER HAT WEISS MAN JEDOCH NIE.

MARTIN GERHARD REISENBERG

1 COMPLIANT ZU ISO STANDARD 27001: INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM

Bei Informationssicherheits-Managementsystemen (ISMS) handelt es sich um ein Bündel an Verfahren und Werkzeugen, die eine anzustrebende Informationssicherheit nachvollziehbar messen und steuern. Der Clou: ISMS ermöglichen die Zertifizierung nach ISO Standard 27001, der derzeit einzigen international gültigen Norm zum IT-Sicherheitsmanagement.

"ISO 27001 auf Basis von IT-Grundschutz" etwa ist eine solche international gültige Zertifizierung. Sie ersetzt das vormalige "Grundschutzzertifikat" des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) und testiert bzw. zertifiziert individuell angemessene IT-Sicherheitsniveaus.

Gewiss aber steht die Zertifizierung der IT-Sicherheit nicht im Fokus eines jeden Unternehmens. Denn damit ist die gleichermaßen konsequente Abarbeitung aller Aspekte eines Standards verbunden - unabhängig davon, ob sie im Einzelfall relevant erscheinen oder nicht. Dennoch empfehlen wir auch den Unternehmen, die keine Zertifizierung anstreben, IT-Sicherheit organisiert anzugehen: jedoch auf pragmatischem Weg durch eine "*Orientierung am Standard*" anstatt durchgängig streng "*nach Standard*".

2 PRAGMATISCHE IT-SICHERHEIT ORIENTIERT AN ISO 27001

Gerade wenn ohne Bedarf an formaler IT-Zertifizierung der Wunsch nach einer besonders aufwandsarmen, zeitnahen und passenden Sicherheitslösung besteht, ist ein praxisbewährtes, pragmatisches Vorgehen zweckmäßiger und auch objektiv sinnvoller. Entscheidend ist hierbei die veränderte Perspektive: Im Sinne der Effektivität und Zweckdienlichkeit geht es hier nicht darum "streng nach Standard" zu verfahren, sondern unter Berücksichtigung der Umstände und Anforderungsprioritäten eines Unternehmens eine individuell sinnvolle "*Orientierung am Standard*" anzuwenden. Der Vorteil liegt klar auf der Hand: Sie sparen deutlich an Zeit und Invest und erhalten mit diesem Vorgehen ein Optimum aus Methodik, Aufwand, Investitionsschutz und Sicherheitsgewinn.

IT-SICHERHEIT MIT NETWORKERS

Networkers unterstützt Unternehmen bei der Herstellung einer individuell passenden IT-Sicherheit. Dabei stehen Ihnen unsere Security-Teams rund um unsere lizenzierten BSI-Auditoren im Bereich IT-Grundschutz und ISO Standard 27001 in allen Fragen zur Verfügung. Exakt nach Ihren Zielsetzungen, Anforderungen und Rahmenbedingungen erarbeiten wir genau die für Sie passende IT-Sicherheit: Sei es revisionsicher "nach ISO Standard 27001" im Hinblick auf die Zertifizierung Ihrer IT-Infrastruktur oder aber pragmatisch "orientiert am Standard" mit Blick auf eine besonders aufwandsarme Erreichung eines tragbaren IT-Sicherheitsniveaus.

LEISTUNGSÜBERBLICK IT-SICHERHEIT AUF DEN PUNKT:

- Planung, Aufbau und Betrieb von IT-Sicherheitsumgebungen
- Coaching von IT-Security-Teams
- Security-Awareness-Workshops
- Schutzbedarfsfeststellungen (BSI)
- Basis-Sicherheitschecks (BSI)
- IT-Sicherheits-Audits:
White-Box, Black-Box, und Penetrationstests
- IT-Sicherheits-Revisionen
- Security-Policies / Security-Richtlinien
- Risikomanagement
- Vorbereitung zu Zertifizierungen und Testierungen (IT-Grundschutz, ISO 27001)
- Auditierung nach ISO 27001
- Eskalationspläne
- Wiederanlaufpläne
- IT-Notfallvorsorgekonzepte
- Kryptokonzepte
- Datensicherungskonzepte
- Schulungskonzepte
- Virenschutzkonzepte
- Berechtigungskonzepte
- Ereignis- und Krisenvorsorge
- IT-Security-Dokumentation ... und viele weiteres mehr



Networkers AG
Bandstahlstraße 2
58093 Hagen

fon: 0 23 31 . 80 95 0
fax: 0 23 31 . 80 95 499

email: info@networkers.de
web: www.networkers.de