

„ISO 27001 auf der Basis von IT-Grundschutz“

Die Norm ISO 27001 ist eine internationale Zertifizierungsnorm für Informationssicherheits-Managementsysteme. Bei einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz wird neben dem IT-Sicherheitsmanagement auch die konkrete Umsetzung von IT-Sicherheitsmaßnahmen auf der Basis von IT-Grundschutz geprüft. Mit den anerkannten BSI-Standards und den IT-Grundschutz-Katalogen werden die sehr allgemein gehaltenen Anforderungen der ISO 27001 für die Praxis konkretisiert und helfen den Anwendern mit vielen Hinweisen, Hintergrundinformationen und Beispielen. Detaillierte Step-by-Step-Anleitungen zeigen, wie ein Informationssicherheits-Managementsystem im Unternehmen eingeführt werden kann.

Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz zeigt, dass in der jeweiligen Institution IT-Sicherheit ein anerkannter Wert ist, ein IT-Sicherheitsmanagement vorhanden ist und außerdem ein definiertes IT-Sicherheitsniveau nachgewiesen wurde.



Vorbereitung auf die Zertifizierung nach ISO 27001

Für die Informationssicherheit im Gesundheitswesen wird weniger getan, als die informationstechnischen Systeme tatsächlich erfordern. Störungen und Ausfälle belegen, dass die Verfügbarkeit der Systeme, die Vertraulichkeit und die Integrität der Informationen nicht ausreichend gewährleistet sind. Die Ursachen: Die hohe Abhängigkeit der Geschäftsprozesse von der Informationstechnik und die mangelnde Sensibilisierung der Mitarbeiter im Umgang mit vertraulichen Daten machen die Institutionen anfälliger denn je. Das Wissen um die organisatorischen und technischen Schwachstellen und um die Anforderungen von internationalen Informations-Sicherheitsstandards ist noch zu gering.

Der Weg zu mehr IT-Sicherheit

Der Aufwand für Sicherheitsmaßnahmen ist je nach Institution recht unterschiedlich (je nach Größe der Institution und deren IT, Anzahl der Systeme und Schutzbedarf der verarbeiteten Informationen).

Es ist sinnvoll, zunächst kleinere Teilverbände zu bilden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit seinem IT-Grundschutz-Ansatz einen pragmatischen Weg, die Anforderungen der ISO 27001 umzusetzen. Als ersten Schritt empfiehlt es sich, mit einem Workshop zur IT-Sicherheitsanalyse zu beginnen. Hierbei wird der Umfang des Untersuchungsgegenstandes festgelegt, eine Schutzbedarfsanalyse durchgeführt und festgelegt, welche Maßnahmen umgesetzt werden müssen. Anschließend sollten erfahrene Security-Experten den Ist-Zustand ermitteln. Mit einer IT-Risikoanalyse werden die ermittelten Schwachstellen bewertet und Vorschläge für die Planung und Einrichtung geeigneter IT-Sicherheitslösungen gemacht. Ein Zertifikat nach ‚ISO 27001 auf der Basis von IT-Grundschutz‘ ist schließlich der offizielle Beleg für ein etabliertes und gelebtes Informationssicherheits-Managementsystem (ISMS).



DS DATA SYSTEMS ist spezialisiert auf Beratung und Organisation der IT-Sicherheit in Unternehmen und Institutionen. Das Unternehmen besitzt im Gesundheitsbereich langjährige Erfahrung bei den Themen Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz und IT-Risiko Management.