

Neuer Service

PFI zertifiziert Informationssicherheits- Managementsysteme

*Seit September ist das PFI durch die DAkKS für die Zertifizierung von Informationssicherheits-
Managementsystemen nach ISO/IEC 27001 akkreditiert. Informationen sowie die Prozesse,
Systeme und Netzwerke, mit denen sie be- und verarbeitet werden, sind die Grundlage der
Aktivitäten vieler Unternehmen und Organisationen. Ihr Schutz ist ein brisantes Thema und wird in Zu-
kunft sogar noch wichtiger. Viele Unternehmen entscheiden sich daher für ein Informationssicherheits-
Managementsystem, denn es unterstützt sie in Belangen der Sicherheit von Informationen sowie dabei,
die diesbezüglichen rechtlichen Anforderungen zu erfüllen und nötige Aktualisierungen umzusetzen.*

Ein Informationssicherheits-Managementsystem (ISMS) definiert Regeln, Verfahren, Maßnahmen und Instrumente, mit denen sich die Informationssicherheit in einer Organisation definieren, steuern, kontrollieren und dauerhaft verbessern lässt. Sein Zweck ist, die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen jederzeit zu gewährleisten und die Risiken, die der Einsatz von Informationstechnologie birgt, identifizierbar und beherrschbar zu machen. Ein ISMS betrachtet nicht nur digitale Daten, sondern beschreibt ein umfassendes Sicherheitsmanagementsystem, das auch Unterlagen in Papierform und nicht zuletzt die Mitarbeiter einbezieht.



Gerade für kleine und mittelständische Unternehmen, die nicht in der IT-Branche tätig sind und nur kleine IT-Abteilungen haben, sind die Anforderungen der Informationssicherheit eine Hürde. Ein ISMS bietet wertvolle Unterstützung und erleichtert die Implementierung von Maßnahmen zur Informationssicherheit erheblich.

Die Verantwortung für ein ISMS liegt bei der Unternehmensführung. Der Top-Down-Ansatz ermöglicht, die erstellten Sicherheitsrichtlinien (die so genannten *Security Policies*) auf allen Unternehmensebenen umzusetzen. Das Management darf die Detailausarbeitung und Umsetzung der Richtlinien zur Informationssicherung jedoch an Mitarbeiter übertragen.

Die Zertifizierung nach der Norm ISO/IEC 27001 erfolgt gemäß der Normenreihe ISO/IEC 2700x. ISO/IEC 27002 enthält Maßnahmen, wie ein System nach ISO/IEC 27001 gestaltet werden kann. ISO/IEC 27003 bietet Hilfestellungen zur Umsetzung der ISO/IEC 27001. Die Integration eines ISMS in eine bestehende Zertifizierung (beispielsweise gemäß ISO 9001 oder ISO 13485) ist möglich.

Weitere Fragen beantwortet gerne:

Marc Dauber, Zertifizierungsstelle des PFI

Tel.: +49 6331 2490 809

E-Mail: marc.dauber@pfi-germany.de