Bundesamt
für Sicherheit in der
Informationstechnik

ISO 27001 Zertifizierung auf Basis von IT-Grundschutz

Die BSI-Standards enthalten Methoden und Vorgehensweisen zu den unterschiedlichsten Themen aus dem Bereich der Informationssicherheit und stellen mit dem IT-Grundschutz-Kompendium einen De-Facto-Standard für IT-Sicherheit dar.

Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Mit dem BSI-Standard 200-2 zur IT-Grundschutz-Methodik kann ein solides ISMS aufgebaut werden. Dabei steht mit der Standard-Absicherung die bewährte IT-Grundschutz-Vorgehensweise zur Verfügung. Sie wird ergänzt durch die Basis-Absicherung, die eine grundlegende Erst-Absicherung in der Breite ermöglicht, sowie durch die Kern-Absicherung, die sich dem Schutz der besonders schützenswerten Daten einer Institution widmet. Der BSI-Standard 200-3 zum Risikomanagement enthält alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.

Das IT-Grundschutz-Kompendium enthält die IT-Grundschutz-Bausteine, in denen jeweils Gefährdungen und Sicherheitsanforderungen für ein Thema der Informationssicherheit übersichtlich auf rund zehn Seiten erläutert werden. Die IT-Grundschutz-Bausteine sind in zehn thematische Schichten aufgeteilt.

Eine ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz ist sowohl für die Standard-Absicherung, als auch für die Kern-Absicherung möglich. Für den Nachweis einer erfolgreichen Umsetzung der Basis-Absicherung bietet das BSI ein Testat an.

Allerdings dürfen die Testate nur von einem beim BSI zertifizierten Auditoren vergeben werden.

Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-Grundschutz-Auditors gehört eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Auditberichts. Für die Vergabe eines ISO 27001-Zertifikats muss dieser Auditbericht zur Überprüfung dem BSI vorgelegt werden. Auf der Grundlage des Auditberichts wird durch das BSI über die Ausstellung eines Zertifikats entschieden.
