

Die Themen

- ➔ **Begrüßung**
Motivation zur Einführung eines Informationssicherheits-Management-Systems (ISMS) nach ISO27001
- ➔ **ISO27000-Familie**
Aufbau, Inhalte und Lesensart der ISO27001: Managementgebiete, Maßnahmenziele und Controls. Zusammenhang mit den anderen Normen der Normenreihe.
- ➔ **Definition des Scope**
Es wird im ersten Schritt der Scope festgelegt, für den das spätere ISMS Gültigkeit haben soll. Dieses können auch ggf. Teilbereiche eines Unternehmens sein.
- ➔ **Risikomanagement**
Die Grundlage der ISO27001 ist ein Risiko-orientierter Ansatz. Dazu muss vor der Einführung eines ISMS ein qualifiziertes IT-Risikomanagement etabliert sein.
- ➔ **Prozessgedanke**
Die ISO27001 ist stark prozessorientiert. Es wird in diesem Teil des Workshops der "PDCA"-Lebenszyklus eines Management-Prozesses nach Deming vermittelt, der in den relevanten IT-gestützten Geschäftsprozessen umgesetzt sein muss.
- ➔ **Anforderungen an die Dokumentation**
In diesem Punkt wird eine Übersicht über die Dokumente vorgestellt, die für eine Erfüllung der Anforderungen der ISO27001 notwendigerweise erstellt werden müssen, sofern die geforderten Aspekte nicht bereits in anderen Managementsystemen beschrieben sind.
- ➔ **Controls, SOA**
Zur Erfüllung des normativen Anhangs der ISO27001 müssen die dort aufgeführten Controls umgesetzt sein. Dazu wird im Statement of Applicability (SOA) erfasst, welcher Umsetzungsgrad bzgl. der einzelnen Controls bereits erreicht wurde.

Einführung eines ISMS:

Ausrichtung der Unternehmensprozesse nach der internationalen Norm ISO27001

In diesem Workshop werden die Anforderungen der internationalen Informationssicherheits-Norm ISO27001 vermittelt. Es werden Möglichkeiten aufgezeigt, die Vorgaben aus der Norm und aus den Controls des normativen Anhangs umzusetzen und in ein evtl. existierendes übergeordnetes Managementsystem (z.B. Qualitätsmanagement) zu integrieren.

Durch die Erfüllung dieser Anforderungen wird ein Informations-Sicherheits-Management-System (ISMS) etabliert, welches eine anschließende Zertifizierung nach ISO27001 ermöglicht.

ISO27001-Auditoren führen die Teilnehmer durch diesen Workshop.

Zielgruppe: Management, CIO, CISO, IT-Sicherheits- und Datenschutzbeauftragte, IT-Koordinatoren, QM

Vorkenntnisse: keine

Dauer: 1 Tag