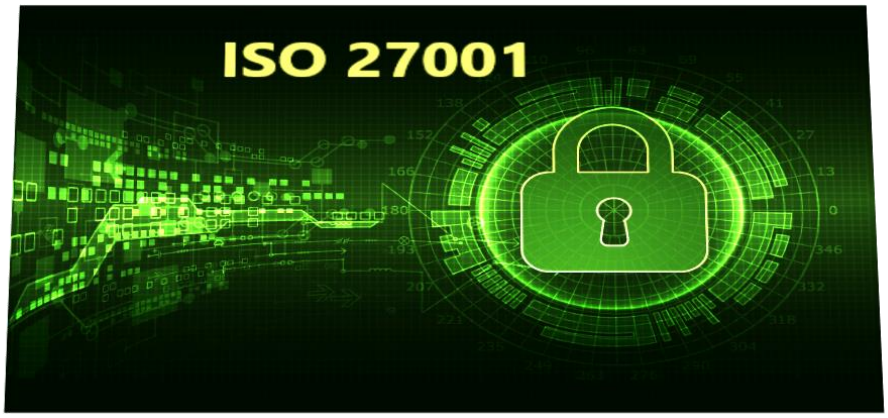
PRAXIS
Unternehmensberatung



Die ISO 27001 ist eine Norm zur Sicherstellung der Informationssicherheit in Unternehmen und Organisationen. Die Ziele, die mit der Einfürhung dieser Norm verfolgt werden, sind:

- Ein **einheitliches** und zentral gesteuertes **Informationssicherheits-Managementsystem**
- **Schutz immaterieller Unternehmenswerte** (Kundendaten, Know-how, Betriebsgeheimnisse)
- Effektives Monitoring und Steuern von Informationssicherheits-Risiken
- **Vereinfachung des Risikomanagements**
- **Sicherheitsnachweis** gegenüber dem Gesetzgeber, Kunden, Partnern, Versicherungen und Lieferanten durch Zertifizierung durch eine unabhängige akkreditierte Zertifizierungsstelle
- **Sicherung aller Geschäftsprozesse** durch eine etablierte Sicherheitsorganisation

Mit einer optimal eingeführten ISO 27001 haben Sie bereits auch viele Anforderungen der EU-Datenschutzgrundverordnung in Ihrem Unternehmen erfüllt!

Welche Unternehmensbereiche werden in einem Informationssicherheits-Managementsystem nach ISO 27001 betrachtet?

- Risiko Management im Bereich der Informationssicherheit
- Unternehmensweite Sicherheitspolitik (Security-Policy)
- Aufbauorganisation des Sicherheitsmanagement-Systems
- Identifizierung, Klassifizierung und Prüfung der Unternehmenswerte
- Sicherheit von Personal & Einrichtungen
- Management von Information & Kommunikation des Geschäftsbetriebes
- Zugangskontrolle & IT Berechtigungen
- Incident- & Problem-Management
- Disaster & Recovery Prozeduren

Die aktuelle Fassung der ISO 27001 wurde bereits in der High-Level-Structure aufgebaut, nach der auch die Normen ISO 9001:2015 und ISO 14001: 2015 aufgebaut sind. Daher können diese Normen leicht in einem gemeinsamen Managementsystem abgebildet werden.

PRAXIS
Unternehmensberatung

Ein wesentlicher Aspekt der Norm ist noch, dass Sie das Schutzbedürfnis Ihrer Werte und Prozesse selbst definieren können. Grundregel: Je höher das Schutzbedürfnis, desto höher der Aufwand bei Kontrolle und Sicherung Ihrer Werte!

Vereinfachter Ablaufplan zur Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001:2015

Voraussetzung für eine erfolgreiche Einführung der ISO 27001 ist eine ausreichende Managementunterstützung für das ISMS:

Phase 1		**Erfassung der IST-Situation**
	Schritt 1	Definition des Geltungs- und Anwendungsbereichs des ISMS
	Schritt 2	Definition der IT-Prozesse und der Geschäftsprozesse mit IT-Unterstützung
	Schritt 3	Definition der Aufbaustruktru des ISMS, Grundschulung für die Mitarbeiter
Phase 2		**Organisations- und Risikoanalyse**
	Schritt 4	Erstellung eines Netzplans
	Schritt 5	Definition der Unternehmenswerte
	Schritt 6	Bewertung der Unternehmenswerte (Darstellung der Gefährdungslage
	Schritt 7	Abschluss der Risikoanalyse, Erstellung eines Maßnahmenkataloges für die Umsetzungsphase
Phase 3		**Umsetzung**
	Schritt 8	Umsetzung der Maßnahmen aus dem Maßnahmenkatalog
	Schritt 8	Umsetzung der Maßnahmen aus dem Maßnahmenkatalog
	Schritt 9	Einführung eines laufenden Verbesserungsprozesses und der Notfallvorsorge
	Schritt 10	Einführung und Schulung der Mitarbeiter in das eingeführte ISMS
	Schritt 11	Erstellung der übergeordneten ISMS-Dokumente (ISMS-Sicherheitspolitik, Handbuch, ISMS-Sicherheitsziele
	Schritt 12	Durchführung eines Internen Audits nach ISO 27001
	Schritt 13	Bewertung des ISMS, Vorbereitung auf das Zertifizierungs-audit nach ISO 27001
Erfolgreiche Zertifizierung		