Informationssicherheitsmanagement

ISO/IEC 27001 im Überblick:

Anforderungen ISO/IEC 27001:

- Risiken erkennen/Risikobehandlungsplan erstellen
- Definition einer Informationssicherheitsleitlinie
- Risikoakzeptanz definieren (messbare Werte)
- Selbstbewertung (internes Audit inkl. Maßnahmenliste)
- Ständige Verbesserung/Weiterentwicklung des ISMS

Ziele:

- Mehr Transparenz im Umgang mit Informationen durch international anerkanntes Konzept
- Risiken aufdecken, analysieren, beherrschen

Die Kapitel der Norm:

0 Einleitung

0.1 Allgemeines
0.2 Kompatibilität mit anderen Normen für Managementsysteme

1 Anwendungsbereich

2 Normative Verweisungen

3 Begriffe

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems
4.4 Informationssicherheitsmanagementsystem

5 Führung

5.1 Führung und Verpflichtung
5.2 Politik
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Chancen
6.2 Informationssicherheitsziele und Planung zu deren Erreichung

7 Unterstützung

7.1 Ressourcen
7.2 Kompetenz
7.3 Bewusstsein
7.4 Kommunikation
7.5 Dokumentierte Information

8 Betrieb

8.1 Betriebliche Planung und Steuerung
8.2 Informationssicherheitsrisikobeurteilung
8.3 Informationssicherheitsrisikobehandlung

9 Bewertung der Leistung

9.1 Überwachung, Messung, Analyse und Bewertung
9.2 Internes Audit
9.3 Managementbewertung

10 Verbesserung

10.1 Nichtkonformität und Korrekturmaßnahmen
10.2 Fortlaufende Verbesserung