Die ISO 31000 "Risikomanagement - Grundsätze und Richtlinien" ist eine Leitlinie für das Risikomanagement und kann für jede Art von Risiko, unabhängig von den betroffenen Instanzen bzw. Unternehmenswerten, angewendet werden. Diese Norm empfiehlt, dass Organisationen einen Rahmen entwickeln, umsetzen und laufend verbessern, um den Prozess für die Behandlung von Risiken in die allgemeinen Führungs- (Governance), Strategie- und Planungs-, Management- und Berichterstattungsprozesse, Politik, Werte und Kultur einzubinden.

Die ONR 49001 "Risikomanagement für Organisationen und Systeme, Elemente eines Risikomanagementsystems) des Österreichischen Normungsinstitus (ON) wurde als als ON-Regel herausgegeben und kann als Zertifizierungsgrundlage von Risikomanagementsystemen verwendet werden.

Risiken und Bedrohungen sowie Compliance-Anforderungen müssen genau definiert und Sicherheitskonzepte danach ausgerichtet sein, um sicherstellen zu können, dass wichtige Geschäftsprozesse nicht beeinträchtigt werden und das Unternehmen vor Haftungsansprüchen Dritter geschützt ist. Dies muss auch für bei Auslagerung von IT an externe Provider gewährleistet werden können. Mit dem aktiven Management von Risiken und Compliance-Anforderungen beim Provider, engem und vertrauensvollem Kontakt zu diesem, proaktiver Risikovermeidung und ständiger Dokumentation und Anpassung der Compliance-Anforderungen sowie der Etablierung eines gemeinsamen Prozesses lassen sich auch größte Outsourcing-Projekte in hochsensiblem Umfeld erfolgreich gestalten.

Dazu können Prozesse zur nachhaltigen Reduktion von Risiken in Geschäftsprozessen von Unternehmen nach Vorgaben des Artikelgesetzes zur Kontrolle und Transparenz (KonTraG) dienen.

Inhalte:

- Risikoinventarisierung auf Basis der Gefährdungskataloge und Schutzbedarfsfeststellung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Risikobewertung (Wahrscheinlichkeit des Eintritts, bzw. des Entdeckens; Auswirkungsgrad)
- Definition von Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit, bzw.

Auswirkungsgrad von Einzelrisiken

- Umsetzung von Maßnahmen zur Risikoreduzierung (Risiko-Matrix)
- Überwachung der Risikolage des gesamten Risikoinventars (Review-Meetings)
- Aktualisierung des Risikoinventars