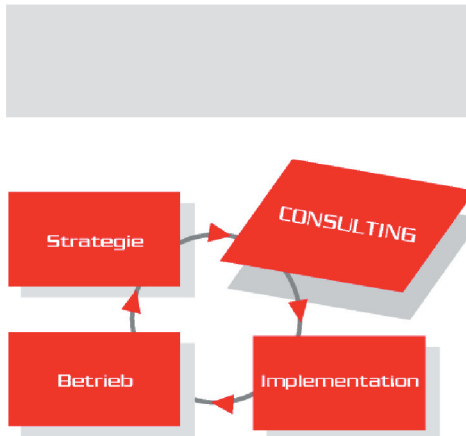


# IT-Risikomanagement

## @-yet Assessments Teil 1 - Risikoanalyse

Ein wichtiges Instrument des IT Risikomanagements. Dient der Feststellung der Risiken, liefert Entscheidungsgrundlagen für das Management sowie die Basis für weitere Verfügbarkeits- und Sicherheitsanalysen.



### Ziel:

Identifizierung, Bewertung der Bedrohungen und deren Auswirkungen auf die Geschäftsprozesse, Bestimmung der IT Risiken.

### Überblick:

#### @-yet Assessments

#### Teil 1 - Risikoanalyse

- ✓ Gefahren identifizieren und bewerten
- ✓ Risikoinventur

#### Teil 2 - Verfügbarkeitsanalyse

- ✓ Richtlinien für Ausfall- und Notfallabsicherung, Infrastruktur setzen und bewerten

#### Teil 3 - Sicherheitsanalyse

- ✓ Richtlinien für Sicherheitsvorkehrungen, Infrastruktur setzen, bewerten und prüfen

#### Datenschutzerklärung

- ✓ @-yet garantiert die Geheimhaltung der Daten durch eine Datenschutzerklärung.

### @-yet Risikoanalyse besteht aus

#### Risiko - Identifikation (Anwendungssicht)

- ✓ erfasst anwendungsbezogen die IT Infrastruktur
- ✓ bewertet die Grundbedrohungen (Verlust der Verfügbarkeit, Integrität und Vertraulichkeit) für geschäftsbedingte IT Services, Anwendungen und Daten

#### Risiko - Bewertung (technische Sicht)

- ✓ bewertet die Bedrohungen und Häufigkeit von Schäden für einzelne Infrastrukturkomponenten
- ✓ bestimmt und klassifiziert die bestehenden Risiken in Bezug auf
  - ✓ Rechenzentrum Infrastruktur
  - ✓ Hardware und Software
  - ✓ Datenträger und Anwendungsdaten
  - ✓ Kommunikation
  - ✓ Betriebsführung und Organisation
  - ✓ Disaster-, Notfallvorsorge, K-Fall
  - ✓ Aufrechterhaltung der Sicherheit

#### Sicherheitsüberprüfung gesetzlich verankert

#### z.B.: § 91 Aktiengesetz (AktG)

- ✓ (2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Verletzung der Organisationspflicht kann zu Schadensersatz führen.

### Ergebnisse einer Risikoanalyse

#### Risk Map und Risikoinventur

- ✓ Erfassung der Risiken
- ✓ Quantitative und Qualitative Bewertung der IT Infrastruktur nach Risikoklassen
- ✓ Beurteilung der Wirksamkeit der bestehenden Vorkehrungen (Organisation und Technologie)
- ✓ Ansatzpunkte für Optimierung und Risikobewältigung (Maßnahmenkatalog)
- ✓ Prioritätenliste

### @-yet-Vorgehen

#### Einführung (Workshop, Ausarbeitung)

- ✓ Abstimmung des Vorgehens
- ✓ Abgrenzung und Festlegung der zu analysierenden Bereiche und Aspekte
- ✓ grobe Aufnahme

#### Beschreibung des Analysebereichs Beschreibung der Bedrohungen und Risiken

- ✓ in Abhängigkeit der IT Services (Anwendungen), Daten, Infrastruktur

#### Analyse und Bestimmung der Risiken

- ✓ Schadenpotentiale (Risikoklassen)
- ✓ Häufigkeit
- ✓ Infrastruktur und Organisation

#### Beschreibung der möglichen Ansätze

#### Aufbereitung der Ergebnisse (Risikoinventur)

- ✓ Entscheidungsgrundlage

#### Präsentation der Ergebnisse