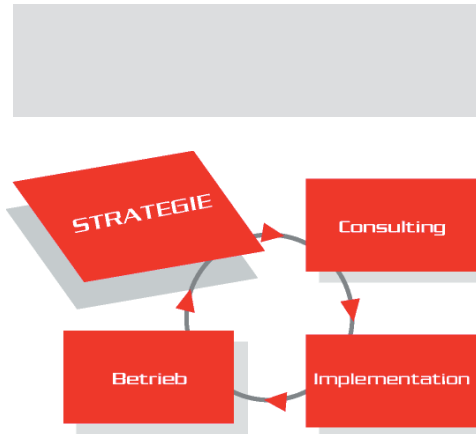


IT-Risikomanagement

@-yet Assessments Teil 3: Sicherheitsanalyse

Die Sicherheit der IT gestützten Geschäftsprozesse/ Services/Anwendungen wird durch viele einzelne Maßnahmen gewährleistet.



Eine Sicherheitsanalyse setzt die Richtlinien für alle IT Bereiche, die der Vertraulichkeit und Integrität der IT Services, Geschäftsprozesse und Daten dienen.

Überblick: @-yet Assessments

Teil 1 - Risikoanalyse

- ✓ Risiken identifizieren und bewerten
- ✓ Risikoinventur

Teil 2 - Verfügbarkeitsanalyse

- ✓ Richtlinien für Ausfall- und Notfallabsicherung setzen und bewerten

Teil 3 - Sicherheitsanalyse

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

@-yet Sicherheitsanalyse

- ✓ stellt Vertraulichkeit und Integrität der Daten und Geschäftsprozesse in den Mittelpunkt
- ✓ vertieft die Ergebnisse einer Risikoanalyse
- ✓ definiert die Richtlinien für Sicherheitsvorschriften wie:
 - ✓ Etablierung der Vorschriften
 - ✓ Umgang mit IT Komponenten
 - ✓ Virenschutz
 - ✓ Datenverschlüsselung
 - ✓ Authentifizierung
 - ✓ Schutz der externen Anbindungen
 - ✓ etc.
- ✓ ist mittel- bis langfristig ausgelegt
- ✓ stellt die Anwendungen, IT Services und deren Abhängigkeiten in Vordergrund (Top/Down Methode)
- ✓ stellt die Basis für detaillierte Planungen (Sicherheitskonzept)
- ✓ dient als Entscheidungs- und Budgetierungsvorlage

@-yet-Vorgehen

Einführungs-Workshop

- ✓ Abstimmung des Vorgehens
- ✓ Abgrenzungsdefinition

Konzept

- ✓ Bedarfsermittlung (Bedarfsmatrix)
- ✓ erste Kostenschätzung

Präsentation der Ergebnisse

Ergebnisse der Sicherheitsanalyse

Richtlinien der organisatorischen Aspekte aus Verfügbarkeitsicht wie z. B.

- ✓ Sicherheitsorganisation
- ✓ Verantwortlichkeiten, Entscheidungswege, Sicherheitsziele, Prinzipien und Verhaltensregeln
- ✓ Aufrechterhaltung der Sicherheit
 - ✓ Security Check und Audits
 - ✓ Überwachung und Optimierung
 - ✓ Regeln für Veränderungen in der IT
 - ✓ abgestimmte und dokumentierte Abnahme und Produktionsfreigabe
- ✓ Richtlinien für einzelne Sicherheitsvorkehrungen wie z. B.:
 - ✓ Zugangsschutz
 - ✓ DMZ
 - ✓ Netzwerkstrukturen
- ✓ Richtlinien und Bedarf (Bedarfsmatrix für Organisation und Infrastruktur)
 - ✓ Regelungen für organisatorische Abläufe
 - ✓ Zugriffskontrolle (Rechteverwaltung, Rechteprüfung)
- ✓ grobe Kostenschätzungen