

# Versuch eines systematischen Überblicks über Organisationsalternativen

Dr. Helmut G. Stiegler  
STI-Consulting GmbH

# Wesentliche Tätigkeiten

Benötigte Instanzen hierfür? Wie arbeiten sie zusammen?

- Zielfestlegung
- Risk-Assessment
- Festlegung der Massnahmen
- Durchführung (in d. Regel stark dezentralisiert)
- Prüfung der Einhaltung, Wirksamkeit
- Erkennen von Schwachstellen und Rückkopplung

# Betroffene IT-Bereiche

Wie werden SLAs definiert? Wer bietet den Service?

- Incident Mgt
- Change Mgt
- Configuration Mgt
- Release Mgt
- Availability Mgt

# Betroffene Non-IT-Bereiche (1)

Wie werden SLAs definiert? Wer bietet den Service?

- Informationssicherheit
- Gebäudesicherheit, Werkschutz
- Anlagenverwaltung
- Personalverwaltung (Arbeitsschutz, Ränge, Rechte, Zuständigkeiten, Verantwortung - auch Personenschutz?)
- Datenschutz
- Q-Mgt
- Finanzverwaltung (Budget-Verwaltung, Risikovorsorge)

# Betroffene Non-IT-Bereiche (2)

- Einkauf (SLAs mit Zulieferern?),
- Verkauf (Sicherheits-Aspekte in zu erfüllenden SLAs)
- Kunden (denen Service geboten wird)
- Auftragnehmer (die als Zulieferer auftreten)

# Organisation der Firma

- Vorstand mit geteilten Verantwortungen
  - Z.B. Gebäudesicherheit getrennt von IT
- Rolle der IT, Mission der Organisation
  - Z.B. nur untergeordneter Service?
- Nationale/internationale Firma
  - Besondere Anforderungen durch spezielle nationale Gesetze
- Grösse der Firma
  - Kleine Firmen z.B.:
    - Weniger interne Struktur und Formalisierung, „da stärker von aussen abhängig“ (nach Zhou Zhiying)
    - Keine Stäbe

# Schutzaspekte von Information

Nach Donn Parker (the „Parkerian Hexad“)

wer ist jeweils dafür zuständig, davon betroffen, daran interessiert?

- Jeder Aspekt kann von einer anderen Instanz verantwortet werden

Confidentiality

Control or Possession

Integrity

Authenticity

Availability

Utility

# Organisation und Zukunftssicherheit

Nach Zhou Zhiying: CMM in uncertain environments, CommACM, August 2003, Vol 46, no 8, p.115-118

Uncertainty and rapid change:

- Wechsel zwischen „Polen“ in der Geschichte: zumindest zwei Formen des Wechsels: langsames/plötzliches Ende
- CMM-Maturity ist nur gut für „stabile Periode“
  - Formalisierung auf Basis von Erfahrung genügt dann nicht mehr
  - Wechsel zu „geringerer Maturity“ dann überlebenswichtig
  - Kleine Firmen müssen viel stärker auf Überraschungen gefasst sein als grosse

*Anm.: Security ist per se für Überraschungen gut*



# Warum „Reife“ nicht immer ein Überlebensvorteil ist

Maturity	Vorteil	Nachteil
Reifer	Vorteile durch Disziplin, Automatisierung und Wiederverwendung	Einschränkungen, bezogen auf Vergangenheit
Weniger reif	Flexibilität und Initiative des Einzelnen	Menschliche Schwächen

# Die Pole organisatorischer Reife

## Normalbetrieb

auch: eher grosse Firmen

Einheitlich

Objektiv

Automatisiert

Regelgesteuert

Inflexibel

Geordnet, beherrschbar

Erfahrungsbasiert

Starr

## Katastrophenfall

auch: eher kleine Firmen

Vielfältig

Subjektiv

Individuell

Fehleranfällig

Flexibel

Unordentlich

Innovativ

Instabil