

Tagung vom 4.6.2003: Informationssicherheit und Recht
Verantwortung von IT-Anbietern und Anwendern für
sichere Informationsverarbeitung

Verantwortung des Unternehmens für sichere IT-Strukturen

Prof. Dr. Rolf H. Weber

Zentrum für Informations- und
Kommunikationsrecht Universität Zürich
Wiederkehr Forster Rechtsanwälte Zürich

Überblick

1. Grundzüge der Unternehmensverantwortung

- Verantwortung von VR/GL
- ICT-Konzept
- Kosten-/Nutzen-Analyse
- Implementation mit klarer Führungsstruktur
- Risikomanagement

Überblick (II)

2. Technische Best Practices

- Infrastruktur
- Prozessabläufe
- Funktionserfordernisse

Überblick (III)

3. Rechtliche Umsetzung des ICT-Konzepts

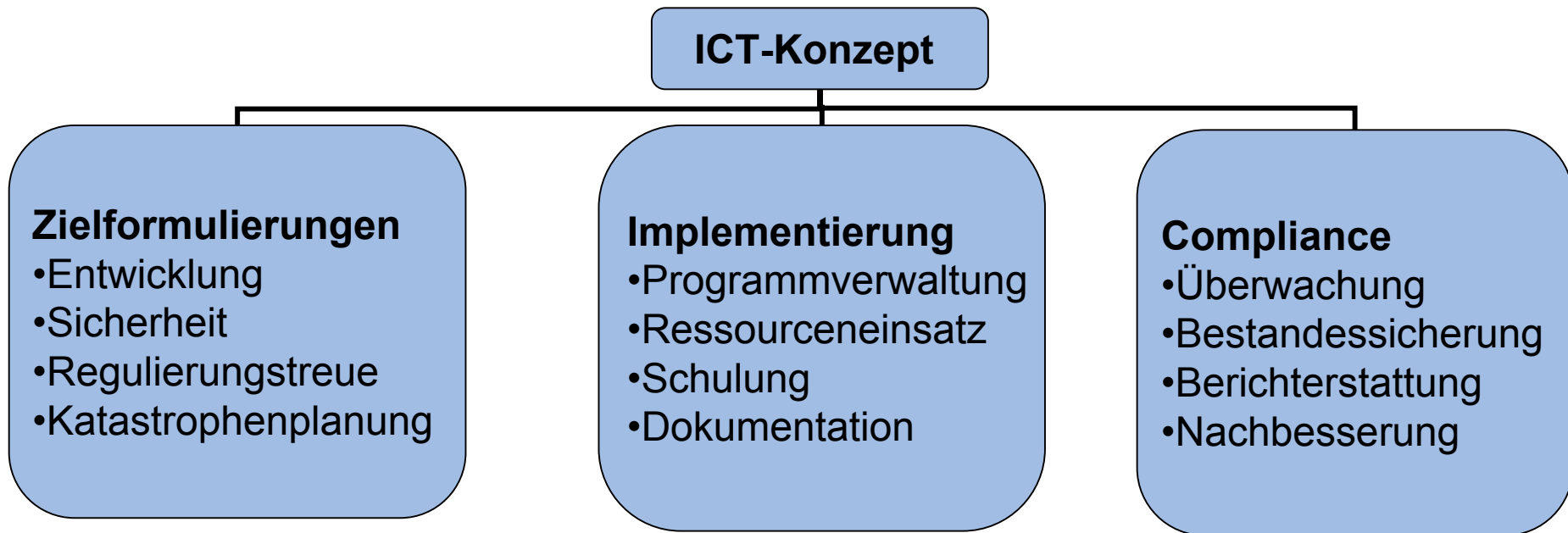
- Einhaltung allgemeiner Standards
- Einhaltung der rechtlichen Rahmenbedingungen
- Sicherheit durch Vertragsmanagement
- Versicherungsschutz

1. Unternehmensverantwortung (E-Governance)

Geteilte Verantwortung von VR/GL

- VR: Oberleitung
 - Grundsätze ICT
 - Führungsinstrument (Management Information System)
 - Corporate Governance
- GL: Projektvorbereitung und Umsetzung

Unternehmensverantwortung (II)



Unternehmensverantwortung (III)

Implementation

- Inventar der Haupt- und Subsysteme (Hard- und Software)
- Festlegung der Prioritätenordnung
- Entwicklung von Lösungsstrategien
- Implementierungen von Änderungen

Unternehmensverantwortung (IV)

Risikomanagement und Kontrolle

- Problemlösungen für technische und operative Risiken
- Compliance-Regulierungen
- Aufbau einer internen Revision
- Disaster Recovery

2. Technische Best Practices

Infrastruktur

- Aggregation vorhandener Informationen
- Einheitlicher Zugang zu Datensammlungen
- Einmalige Datenbeschaffung für alle Zwecke
- Integration der Interface-Stellen mit Dritten
- Monitoring und Erfolgsmessung

Technische Best Practices (II)

Prozessabläufe

- Umschreibung von integrierten ICT-Prozessoren
- Klare Zugangsregelungen für Datensammlungen
- (Benutzerauthentifizierung)
- Vereinheitlichte Regeln mit Bezug auf Datenbedürfnisse
- Aktenführung/Archivierung

Technische Best Practices (III)

Funktionserfordernisse

- Sicherstellen der Datensicherheit
- Automatische Datenerfassung
- Unterstützung von Datensammlungen
- Flexibel gestaltete Bauelemente
- Abstimmung und Plausibilitätsprüfung
- Report und Datenanalyse

3. Rechtliche Umsetzung des ICT-Konzepts

Einhaltung allgemeiner Standards/Themen

- BS 7799 (Information Security Management System)
- ISO/IEC 17799 (Information Security Management)
- ITIL (Best Practice IT Service Management)
- CobiT
- Sektorspezifische Standards (z.B. Basel II)

Rechtliche Umsetzung des ICT-Konzepts (II)

Einhaltung der rechtlichen Rahmenbedingungen

- Technikrecht
- Vertragsrecht
- Schutz von Immaterialgüterrechten
- Datenschutz
- Unlauterer Wettbewerb

Rechtliche Umsetzung des ICT-Konzepts (III)

Sicherheit durch Vertragsmanagement

- Umfassende bzw. isolierte Leistungserbringung
- Klärung der Leistungsziele
- Evaluation von IT-Hardware- und IT-Softwareanbietern
- Grundmuster für Vertragsmanagement
- Checklisten für Vertragsinhalte

Rechtliche Umsetzung des ICT-Konzepts (IV)

Versicherungsschutz

- Sach- und Haftpflichtversicherung
- Versicherte Risiken
- Versicherungsausschluss
- Praktische Durchführungsprobleme