

INFOzMorge

25. Februar 2010

Hotel Schweizerhof, Luzern

Ursula Sury

Rechtsanwältin

Professorin an der Hochschule Luzern

IT Compliance

Definition

to comply with = im Einklang sein mit etwas

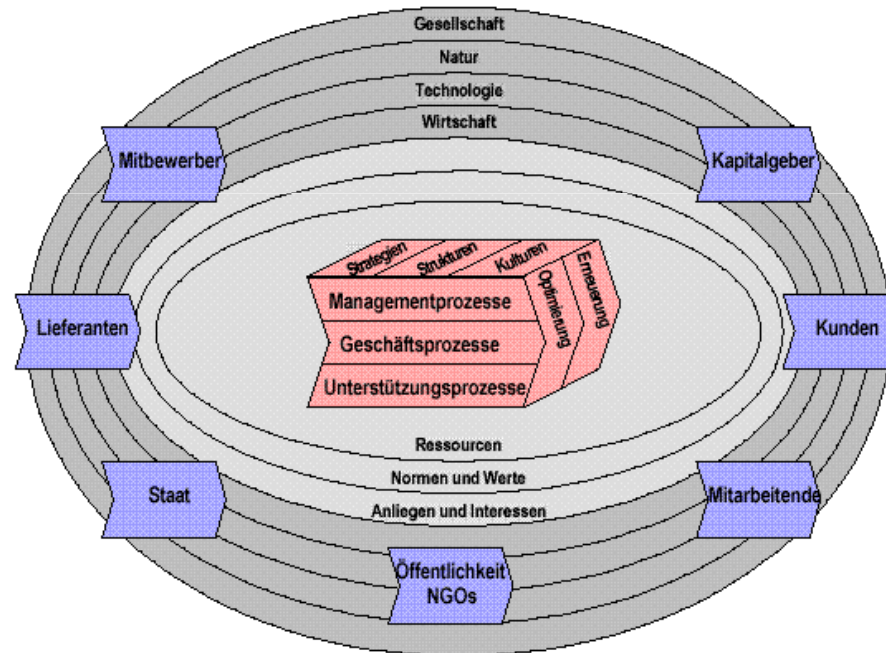
IT oder ICT Informationstechnologie oder
Informations- und
Kommunikationstechnologie

IT oder ICT

IT oder ICT durchdringt sämtliche unternehmerische Bereiche und unterstützt die Kommunikation mit den externen Anspruchsgruppen.

St. Galler Management Modell

St.Galler Management Konzept : Die Unternehmung als dynamisches System



nach Prof. Johannes Rüegg-Stüm, Hochschule St. Gallen

© B.R. Waser

Auf den Punkt gebracht

IT unterstützt Unternehmungen im Erstellen, Bearbeiten, Weiterleiten und Aufbewahren von Informationen.

Informationen

Informationen können personenbezogene Aussagen sein: also Personendaten.

Oder es handelt sich um andere, nicht-personen-bezogene Informationen, wie Texte, Musik, Berechnungsblätter etc.

Recht an Informationen

Informationsrecht	Datenschutz	- Aufbewahrung von Daten - Datenweitergabe
	Archivierungspflichten	
	Internes Kontrollsystem (IKS)	
	Geschäfts- und Fabrikationsgeheimnisse	
	Immaterialgüterrecht	- Urheberrecht, - Patentrecht - Design - Markenschutz
	Etc.	

Datenschutz = Persönlichkeitsschutz

Bearbeitungsgrundsätze
personenbezogener Daten



Wer macht mit **welchen** Personendaten **was** und **warum**?

Wichtige Aspekte

- Datenexport ins Ausland
- Auskunftsrecht und –pflicht
- Outsourcing der Datenbearbeitung

Aktuelle konkrete Anwendungsbereiche

- Versand von E-Mails und Newslettern
- CRM
- Organisation von Businessprozessen
- Datenplattformen
- Cloud Computing

Urheberrecht = Umgang mit urheberrechtlich geschützten Werken

Was gilt als Werk?

Wer ist Urheber?

Was gilt als Werk?

Individuelle, geistige Werke wie z.B.

- Sprachwerke
- Musikwerke
- Bilder

jeglicher Art

Also fast alles, was eine Unternehmung an Dokumenten erstellt

Wer ist Urheber?

- Grundsätzlich die natürliche Person ausser das Urheberrecht sei vertraglich übertragen worden.

 Auch im Arbeitsverhältnis muss das Urheberrecht an den Arbeitgeber übertragen werden!

Konkrete Anwendungsfälle

- Inhalte bei Erstellung von Webseiten
- Inhalte in Social Network-Communities
- Rechte an Computerprogrammen
- Rechte an Marketingunterlagen, Logos etc.

Digitale Signaturen

- Wo braucht man sie?
- Grundsatz der Formfreiheit bei Verträgen
- praktisch sämtliche B2B- und B2C-Verhältnisse sind formlos möglich, Ausnahme z.B. Konsumkreditgeschäfte oder Grundstückkauf

Digitale Signatur

- Digitale Signatur = Gleichstellung mit der eigenhändigen Unterschrift
- Unterschrift mittels eines Zertifikates gemäss ZertEs.
- Zertifikatsgewährer (third trust party) z.B. die Schweizerische Post

Wo will man digitale Signaturen?

Aus Beweiszwecken und für eine provisorische Schuldanererkennung nach SchKG will man praktisch überall eine Unterschrift.

Probleme in der Praxis

- Wer hat ein Zertifikat?
- Wie bringe ich die Thematik in den Businessprozess.

Persönliche Verantwortlichkeit der Unternehmer

- als Organ
- als Mitarbeitender

- zivilrechtlich
- strafrechtlich

Haftung des Verwaltungsrates

OR Art. 716a

2. Unübertragbare Aufgaben

Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;

Haftung des Verwaltungsrates

5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

Der Verwaltungsrat kann die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen. Er hat für eine angemessene Berichterstattung an seine Mitglieder zu sorgen.

Haftung des Verwaltungsrates

OR Art. 754, Abs. 1

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.

Haftung des Verwaltungsrates

OR Art. 759, Abs.1

C. Solidarität und Rückgriff

Sind für einen Schaden mehrere Personen ersatzpflichtig, so ist jede von ihnen insoweit mit den anderen solidarisch haftbar, als ihr der Schaden aufgrund ihres eigenen Verschuldens und der Umstände persönlich zurechenbar ist.

Haftung als Mitarbeitender

OR Art. 321e, Abs. 1 und 2

VI. Haftung des Arbeitnehmers

Der Arbeitnehmer ist für den Schaden verantwortlich, den er absichtlich oder fahrlässig dem Arbeitgeber zufügt.

Das Mass der Sorgfalt, für die der Arbeitnehmer einzustehen hat, bestimmt sich nach dem einzelnen Arbeitsverhältnis, unter Berücksichtigung des Berufsrisikos, des Bildungsgrades oder der Fachkenntnisse, die zu der Arbeit verlangt werden, sowie der Fähigkeiten und Eigenschaften des Arbeitnehmers, die der Arbeitgeber gekannt hat oder hätte kennen sollen.

Strafrechtliche Verantwortung

- Tatbestandsmässigkeit
- Rechtswidrigkeit
- Verschulden

z.B. Urheberrechtsverletzungen, Verletzungen von gesetzlichen Schweigepflichten

Internes Kontroll System IKS

- Der **Verwaltungsrat** muss ein Internes Kontroll-System (IKS) betreiben
- Der **Verwaltungsrat** muss im Anhang zur Jahresrechnung Angaben über die **Durchführung einer Risikobeurteilung** machen
- Die **Revisionsstelle überprüft** das Vorhandensein des **IKS und die Jahresrechnung**
- Dies gilt erstmals für das Kalenderjahr **2008**

Gesetzliche Grundlagen

Art. 728a OR neu

2. Aufgaben der Revisionsstelle

a. Gegenstand und Umfang der Prüfung

1 Die Revisionsstelle prüft, ob:

1. die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;
2. der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinnes den gesetzlichen Vorschriften und den Statuten entspricht;

3. ein internes Kontrollsystem existiert.

2 Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das interne Kontrollsystem.

3 Die Geschäftsführung des Verwaltungsrats ist nicht Gegenstand der Prüfung durch die Revisionsstelle.

Gesetzliche Grundlagen

Art. 663b OR neu

IV. Anhang 1. Im Allgemeinen

Der Anhang enthält:

12. Angaben über die Durchführung einer Risikobeurteilung;

Gesetzliche Grundlagen

Die Bestimmungen über IKS und Risikobeurteilung gelten auch für:

- die GmbH (Art. 801 und 818 OR)
- die Kommandit AG (Art. 764 Abs. 2 OR)
- die Genossenschaft (Art. 906 und Art. 908 OR)
- den revisionspflichtigen Verein (Art. 69b Abs. 3 ZGB)
- die Stiftung (Art. 83a Abs. 2 und 83b Abs. 3 ZGB)

Aufgaben des Verwaltungsrates → IKS

Alter Wein in einem zusätzlichen neuen Schlauch

- Führungsverantwortung impliziert Kontrolle, diese muss systematisch durchgeführt werden.
- Risikomanagement impliziert auch regelmässige Kontrolle, systematisiert werden kann diese mit einem IKS.
- Die Revision prüft, ob ein IKS besteht.
→ **neu**

Aufgaben des Verwaltungsrates → Risikobeurteilung

Alter Wein in einem zusätzlichen neuen Schlauch

- Der Verwaltungsrat hat im Rahmen seiner unübertragbaren Kompetenzen und Verantwortlichkeiten sorgfältig zu handeln.
- Sorgfältiges Handeln impliziert Risikobeurteilung
- Über diese Risikobeurteilung hat der Verwaltungsrat im Anhang der Jahresrechnung Angaben zu machen.
→ **neu**

Risikobeurteilung und IKS

→ **Auswirkungen auf die Informationssicherheit**

- Unklare gesetzliche Grundlage

ABER

- International Tendenz zu umfassendem IKS- und Risikomanagement-Verständnis

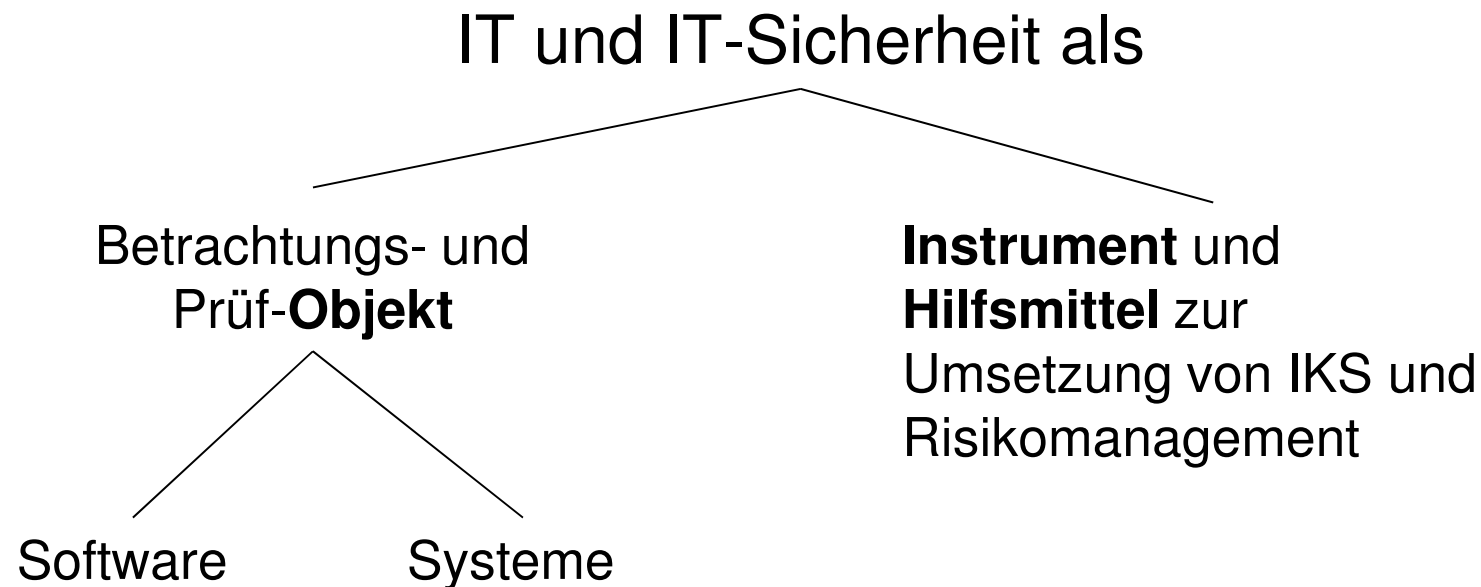
Risikobeurteilung und IKS

→ Auswirkungen auf die Informationssicherheit

- Sicher funktionierende **IT** liefert die für die Geschäftsführung notwendigen **Management-Informationen**
- Sicher funktionierende **IT** ermöglicht in vielen Betrieben erst die Erfüllung/Erstellung des **Geschäftsprozesses**
- Sicher funktionierende **IT** ist das zentrale Element jedes unternehmerischen **Unterstützungsprozesses**

Risikobeurteilung und IKS

→ **Auswirkungen auf die Informationssicherheit**



Sicherheitsanforderungen an IT-Produkte als solche → Objekt

IT-Produkte/Software muss inhaltlich so angelegt sein dass sie

- kein Risiko bilden
- keine Falses generieren (z. B. falsche Management-informationen, falsche Aussagen in der Jahresrechnung o. ä.)
- korrekte Managementinformationen liefern
- korrekten Geschäftserstellungoutput liefern
- keine Gesetze verletzen
- Integrität
- etc.

Risiken beim Einsatz von ganzen IT-Systemen → Objekt

- Ausfallrisiken
- zu weit gehendes Monitoring (Datenschutzverletzung!)
- unsichere Transaktionen
- nicht beweisbare Transaktionen
- falsche Zustellungen
- Datenqualität
- Datensicherheit
- Risiken bei Systemänderungen
- Risiken bei Systemunterhalt
- wie wird die IT eingesetzt?
- wie wird auf Probleme mit IT-Systemen durch die Unternehmen resp. das Management reagiert?
- etc.

Informatik und Informatiksicherheit als Instrumente und Hilfsmittel des IKS

- IT und die IT-Sicherheit von der Unternehmung selber regelmässig überprüft
- Zugriffsregelungen und Authentisierungen
- Verschlüsselungen
- Monitoring
- Anonymisierung
- Pseudonymisierung
- etc.

Ich danke für Ihre Aufmerksamkeit

Hinweise auf Publikationen
www.dieadvokatur.ch

Weiterbildungsmöglichkeiten auch IT-Recht
www.hslu.ch

neues CC Management & Law

Prof. Ursula Sury
Rechtsanwältin
Die Advokatur Sury GmbH
Alpenquai 4
6005 Luzern