
Der Verwaltungsrat in der Verantwortung: Aufgaben in den Bereichen Risikomanagement und Informationssicherheit

Urs E. Zurfluh
Dr. sc. techn. ETH

Verwaltungsrat CSS Versicherung und weitere Mandate
CEO Ad Vantis AG
www.advantis.ch

Inhalt

-
-
- Haftung der Organe
 - Risk Management und die IT
 - Aufgaben des Verwaltungsrates
 - Organisation und Controlling
 - Info-Security Governance
 - Metaaufgaben des Verwaltungsrates
 - Fazit

Haftung der Organe

AD VANTIS

Verwaltungsrat und übrige Organe sind verpflichtet, die ihnen übertragenen Aufgaben der Geschäftsführung mit aller Sorgfalt zu erfüllen und die Interessen der Gesellschaft in guten Treuen zu wahren (Art. 717.1 OR).

Grundlage der Organhaftung nach Art. 754 OR ist die Verletzung der Geschäftsführungspflicht gemäss Art. 716 / 717 OR: Haftung für pflichtwidriges Unterlassen der Organe aufgrund ihrer Garantenstellung.

Die dauernde Verfügbarkeit der notwendigen Funktionalitäten, sowie unveränderte und gegen Zugriff durch Unbefugte angemessen gesicherter Systeme, Programme und Netze und Daten ist eine wesentliche Voraussetzung für die Erhaltung und Mehrung der im Unternehmen verkörperten Vermögenswerte – und für diese Werte sind der Verwaltungsrat und die übrigen Organe zuständig und verantwortlich.

© Ad Vantis AG

Dr. Urs E. Zurfluh

Grundsätze

AD VANTIS

Die primäre Aufgabe des Verwaltungsrates im Bereich der Informations-Sicherheit ist die *strategische Führung*, zusammen mit der Geschäftsleitung.

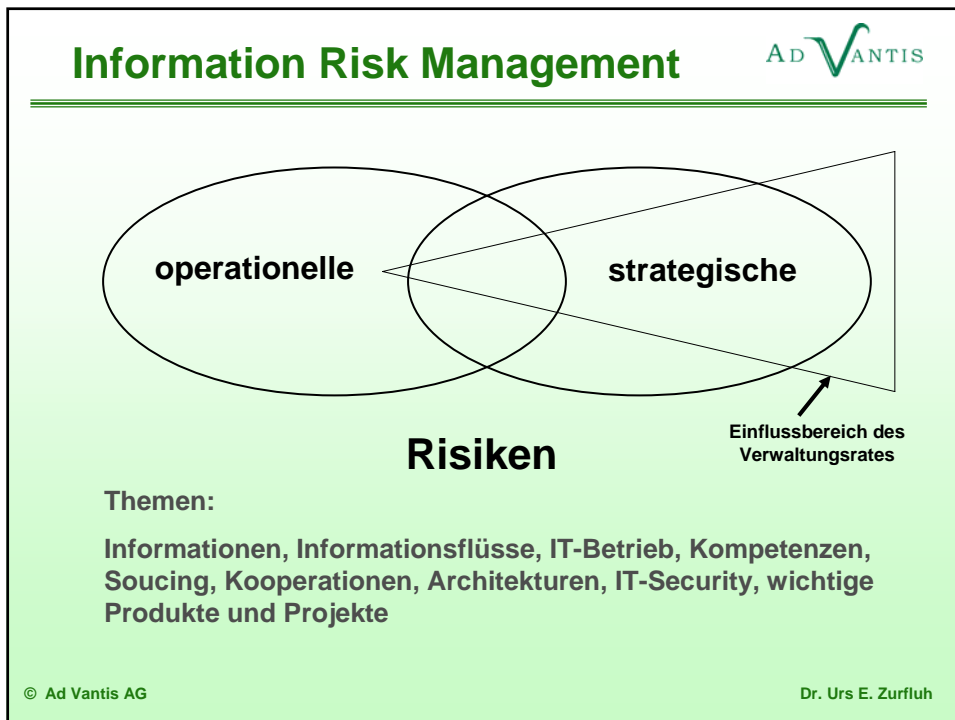
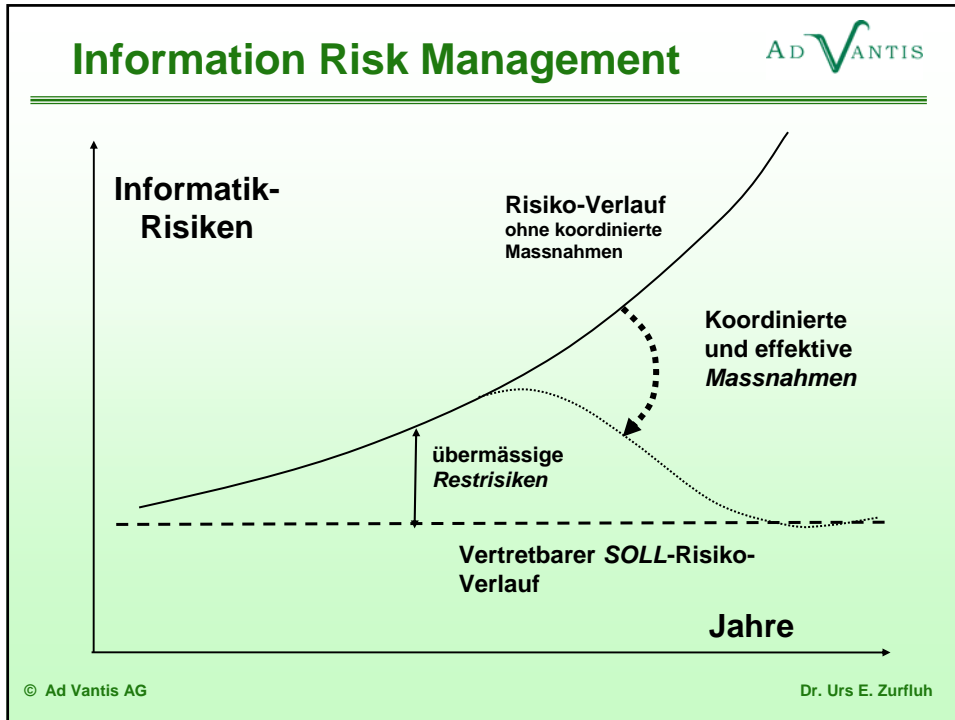
Die Basis bilden das *Risikomanagement*, good Practice, Standards und unternehmerische Intension.

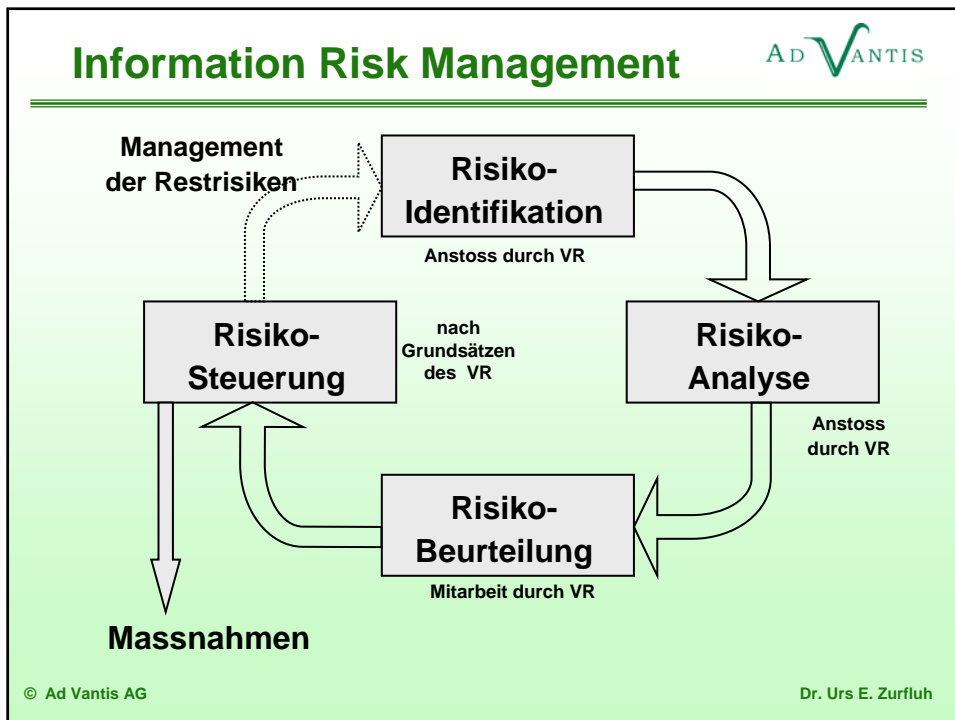
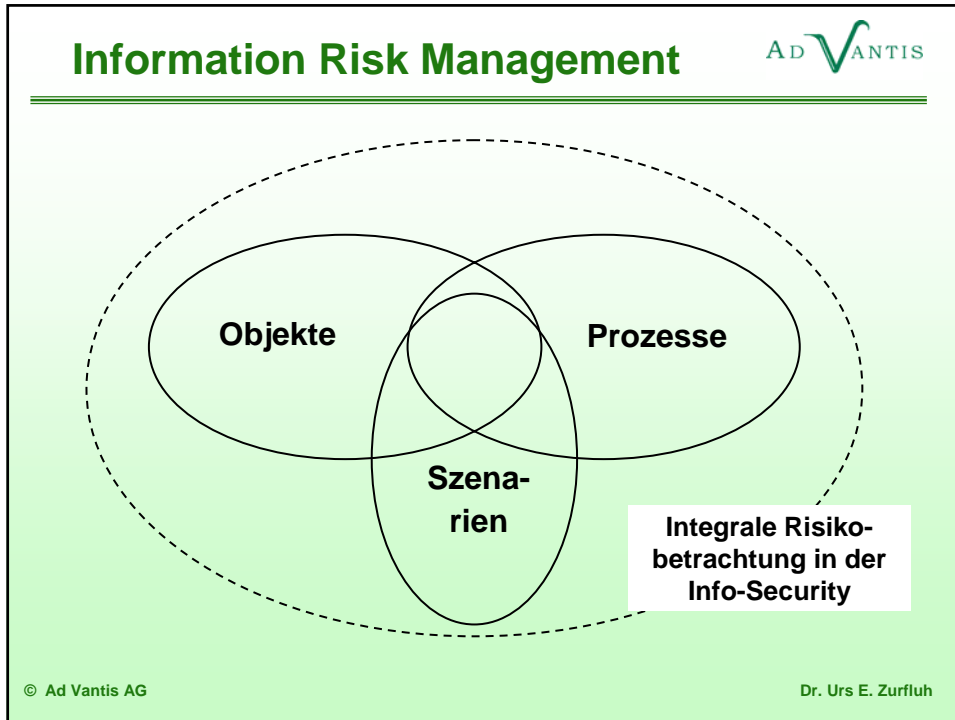
Politik, Strategien und Grundsätze sind die *Führungs-Instrumente*.

Kenngrössen, Rapportierungen und Analysen sind die *Sensoren*.

© Ad Vantis AG

Dr. Urs E. Zurfluh





Aufgaben d. Verwaltungsrates

AD VANTIS

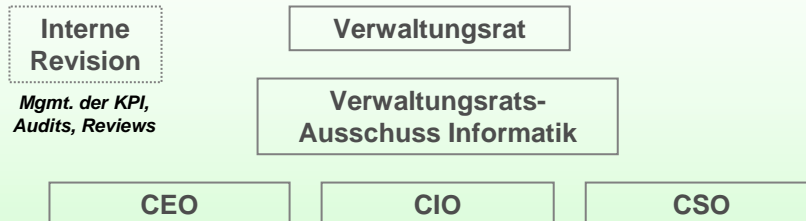
- **Strukturen / Prozesse schaffen**
(zB. Orga., Verfahren, Crisis Mgmt.)
- **Wertesystem entwickeln und abstimmen**
(zB. Politik, Fehlerraten, Vernetzung, Beherrschbarkeit)
- **Inhalte vereinbaren**
(zB. Grundsätze, Architekturen)
- **Abstimmen auf allen Stufen** (.. oder abstimmen lassen)
- **Kulturelle Diskussion führen**

© Ad Vantis AG

Dr. Urs E. Zurfluh

Organisation / Controlling

AD VANTIS

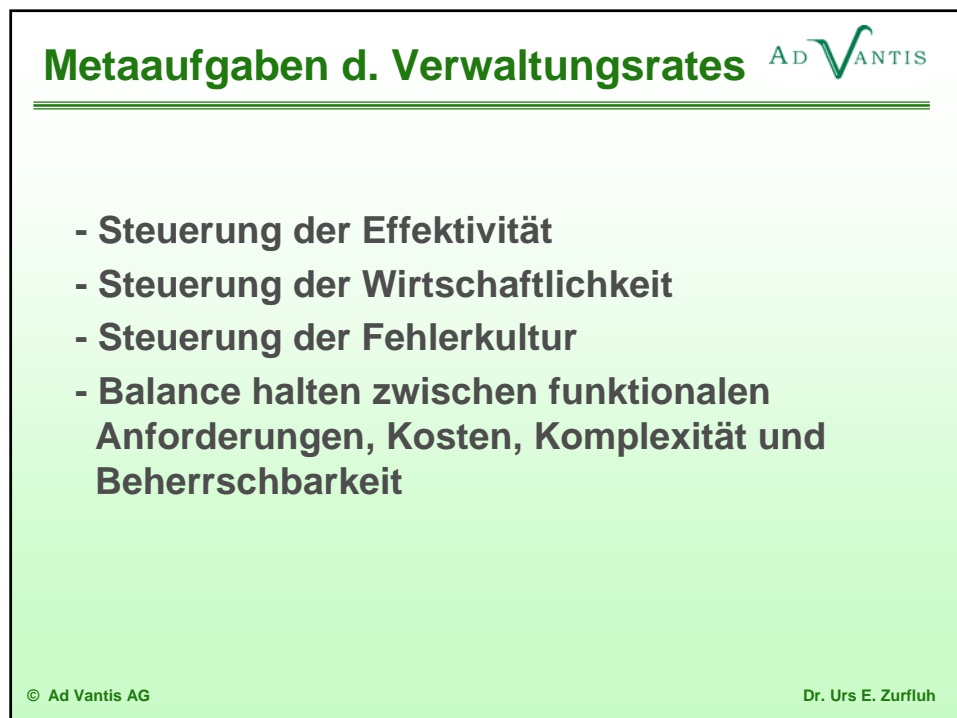
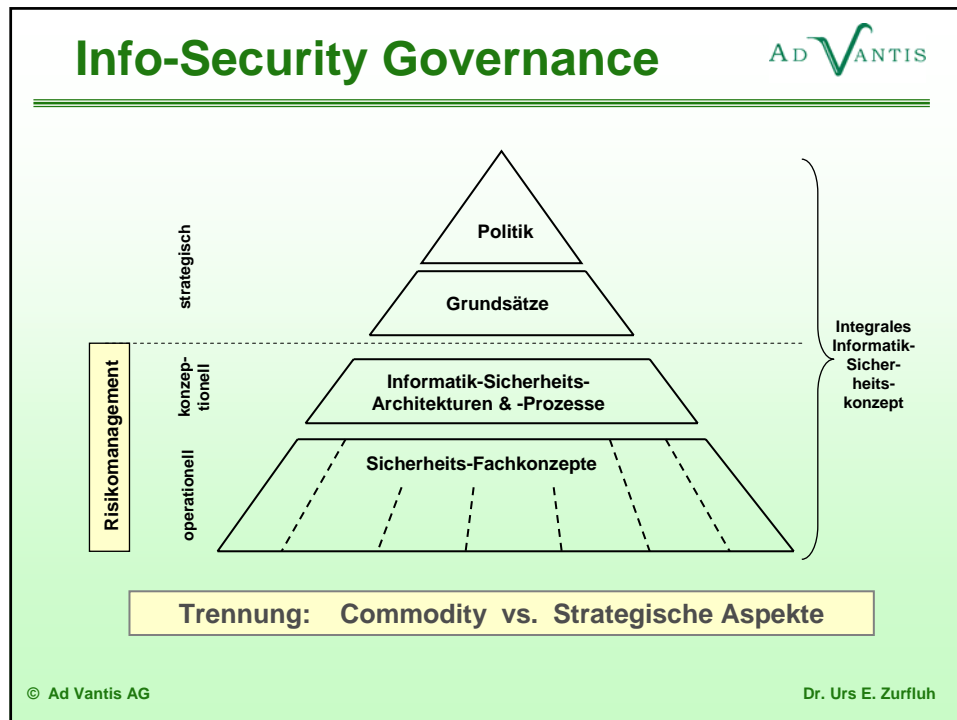


Problem:
VR darf nicht mit CIO
direkt kommunizieren und
Anweisungen geben

Rapportierung:
MIS, Project
Controlling, Crisis
Management

© Ad Vantis AG

Dr. Urs E. Zurfluh



Fazit

AD VANTIS

Info-Security Governance benötigt in der Praxis:

- Bekenntnis zum Thema
- Wille zur Führung
- Wille zur strategischen Koppelung der Informatik
- Toleranz im operationellen Bereich
- Strukturen
- Inhaltliches Know-How
- Durchhaltewillen

© Ad Vantis AG

Dr. Urs E. Zurfluh

Ad Vantis AG

AD VANTIS

Als Beratungsunternehmen mit
Schwergewichten Strategie, Innovation, IT-
Management und Risk Management
unterstützen wir Kunden in der
Implementierung und der Abwicklung von
Governance-Themen.

Kontakt:

Urs E. Zurfluh 044 790 30 00 urs.zurfluh@advantis.ch

© Ad Vantis AG

Dr. Urs E. Zurfluh