Governance, Risk and Compliance (GRC) für die Schweizer Hochschulen

Clemens Gubler, NOVO Business Consultants AG

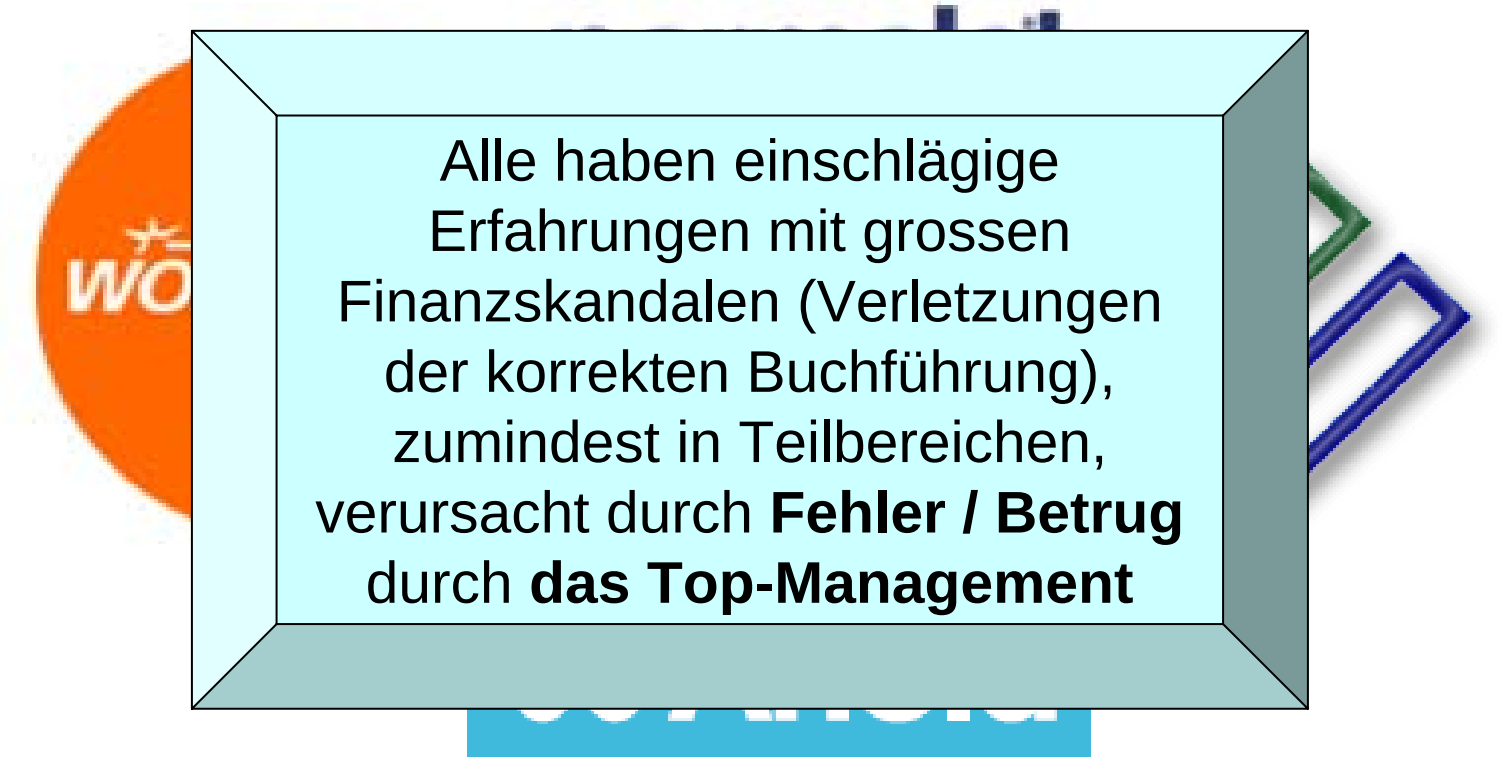
Zürich, 14. November 2007

Agenda

- **Historie**
- Gesetzgebung in der Schweiz
- GRC – Definition des Begriffs
- Handlungsbedarf für Schweizer Hochschulen
- Vorgehensansatz
- Wie können EDV-Systeme im Bereich GRC unterstützen?
- Fragen und Antworten

Welche Gemeinsamkeiten haben diese Unternehmen?

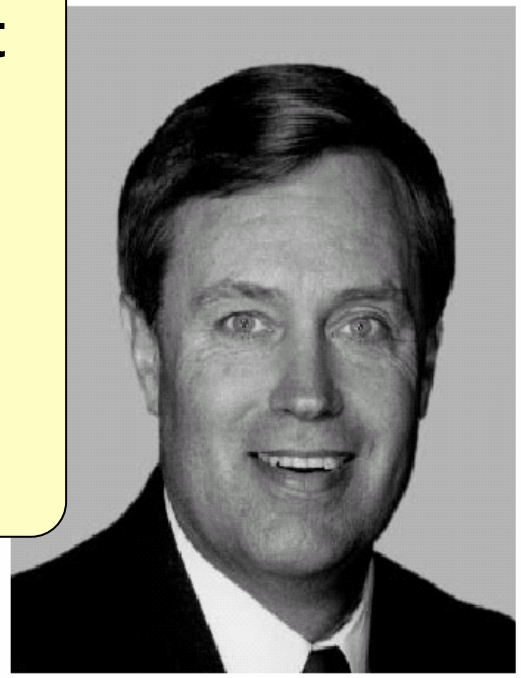
Welche Gemeinsamkeiten haben diese Unternehmen?



Die Reaktion der USA

Sarbanes-Oxley-Act (SOX)

Paul S. Sarbanes
Senator



Michael G. Oxley
Congressman

Agenda

- Historie
- **Gesetzgebung in der Schweiz**
- GRC – Definition des Begriffs
- Handlungsbedarf für Schweizer Hochschulen
- Vorgehensansatz
- Wie können EDV-Systeme im Bereich GRC unterstützen?
- Fragen und Antworten

Reaktion in der Schweiz

- **Sarbanes-Oxley-Act** (SOX) als Vorbote zu Gesetzes-revisionen in Europa und der Schweiz
  → betrifft alle SEC kotierten CH Firmen
- **Ueberarbeitung OR** im Bereich Rechnungslegung führt neu zur expliziten Prüfung des IKS
  → alle Unternehmen mit Buchführungspflicht ab gewisser Grösse
- **Riskmanagement** ist ein „Muss“ *und wird zur undelegier-baren Managementverantwortung*
  → alle Unternehmen mit Buchführungspflicht ab gewisser Grösse
- **Revisionsaufsichtsgesetz** (RAG)
  → Verschärfung der Unabhängigkeitvorschriften des Revisors
  → stellt die Wirtschaftsprüfer unter staatliche Aufsicht
- **Good Governance / Compliance** rückt immer stärker in den Fokus von Anlegern, Kunden, Gesetzgeber und Oeffentlichkeit
  → Führende CH Firmen und öffentliche Verwaltungen lancieren freiwillige Projekte im Bereich Good Governance / Compliance

Neue gesetzliche Anforderungen (Auszug)

- **Internes Kontrollsystem IKS** muss explizit vorhanden und überprüfbar sein (**OR 728a**) d.h. dokumentiert, implementiert und gelebt
- **VR** muss sicherstellen, dass ein **adäquates Risikomanagement** implementiert und die Risiken laufend überwacht (OR 716a) werden; **im Anhang zur Jahresrechnung** müssen explizite Angaben zur Risikobeurteilung ausgewiesen werden
- **Revisor** prüft **Existenz und Zweckmässigkeit des IKS** zusätzlich zur bisherigen Buchprüfung
- **Revisor** erstellt **separaten Bericht an VR mit Feststellungen über das IKS (OR 728b)**
- Der Gesetzgeber richtet den Hauptfokus des IKS auf die **finanzielle Berichterstattung** und die zugrunde liegenden **IT-Systeme**

Gesetzgebung für Schweizer Hochschulen

- **ETH: Gesetzgebung des Bundes**
- **Universitäten/FH: Kantonale Gesetzgebungen**
- **Private Fachhochschule: OR**
- **Abgeleitet aus der Buchführungspflicht**
  → Anforderungen vergleichbar mit dem OR
  → korrekte Buchführung
  → korrekte Finanzberichterstattung
  → Betrugsvorbeugung
  → Prozesssicherheit

Agenda

- Historie
- Gesetzgebung in der Schweiz
- **GRC – Definition des Begriffs**
- Handlungsbedarf für Schweizer Hochschulen
- Vorgehensansatz
- Wie können EDV-Systeme im Bereich GRC unterstützen?
- Fragen und Antworten

Governance, Risk, Compliance

- **Governance** bezeichnet generell das Steuerungs- und Regelungssystem einer politisch-gesellschaftlichen Einheit (Staat, Verband, Unternehmen etc.).
  (www.wikipedia.org)

- **Risk** bezeichnet alle Aktivitäten der Risikoerkennung, -verminderungen und -bewirtschaftung.

- **Compliance** ist die Übereinstimmung mit und Erfüllung von rechtlichen und regulativen Vorgaben.
  (Dr. U. Kampffmeyer)

Agenda

- Historie
- Gesetzgebung in der Schweiz
- GRC – Definition des Begriffs
- **Handlungsbedarf für Schweizer Hochschulen**
- Vorgehensansatz
- Wie können EDV-Systeme im Bereich GRC unterstützen?
- Fragen und Antworten

Konsequenzen für Schweizer Hochschulen

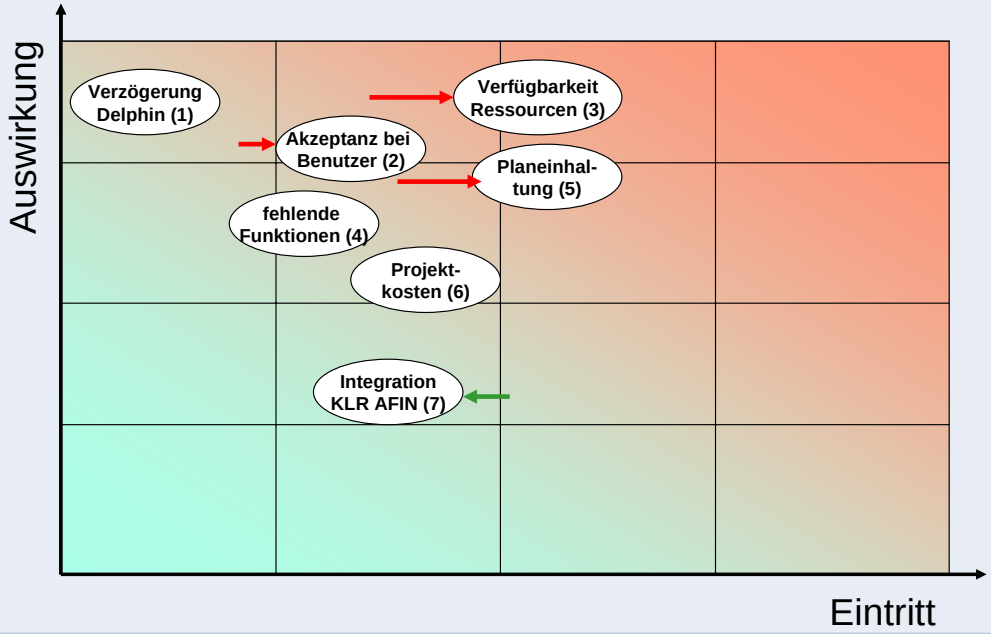
- **Aufbau bzw. Ausbau bestehendes IKS**
  - Aufbau/Anwendung einer IKS-Methode (z.B. COSO / COBIT) & Implementierung eines entsprechenden Control Frameworks
  - Dokumentation aller wesentlichen Geschäftsprozesse *(z.B. Mittelakquisition, (Dritt-)Kreditbewirtschaftung Personalprozess, Reporting etc.)*
  - Definition der internen Schlüsselkontrollen
  - Stufengerechte Schulung über IKS in der Organisation
  - Erstellung von organisatorischen Hilfsmitteln wie
    - Organisationshandbuch
    - Stellenbeschriebe
    - Kompetenz- und Unterschriftenreglemente etc.
  - Aufbau/Ausbau einer pro-aktiven Kontrollumgebung (Verhaltensregelung, etc.), um das Kontrollbewusstsein zu stärken

Konsequenzen für Schweizer Hochschulen (2)

- **Berechtigungssystem und systemunterstützte Kontrollen**
  - Ausgebautes Berechtigungssystem
  - Überprüfung der Berechtigungssysteme
  - Changemanagementprozess
  - Einsatz von Workflows
- **Überprüfung des IKS auf Effektivität**
  - Risikoorientierte Prüfung (Assessments) für alle wesentlichen Einheiten
  - Definition / regelmässiges Monitoring von KPI‘s
  - Prüfung der durchgeführten Kontrollen / Tests

Konsequenzen für Schweizer Hochschulen (3)

- **Aufbau / Ausbau Riskomanagement**
  - Listing aller relevanten Risiken
  - Aktive Bewirtschaftung der Risiken
  - Definition und Umsetzung von Massnahmen
  - Teil des Qualitätsmanagement der Hochschulen



Agenda

- Historie
- Gesetzgebung in der Schweiz
- GRC – Definition des Begriffs
- Handlungsbedarf für Schweizer Hochschulen
- **Vorgehensansatz**
- Wie können EDV-Systeme im Bereich GRC unterstützen?
- Fragen und Antworten

Typische Phase für Compliance Projekte

1 - Unschuld

"Wir haben das beste IKS implementiert. Ich schlafe ruhig!"

2 - Skeptik

"Die Erfüllung der neuen gesetzlichen Anforderungen kann kein Problem sein für uns. Wir haben bereits ein umfangreiches Regelwerk implementiert."

3 - Wut

"Müssen wirklich alle Prozesse dokumentiert werden? Dies sind ja enorm viele!"

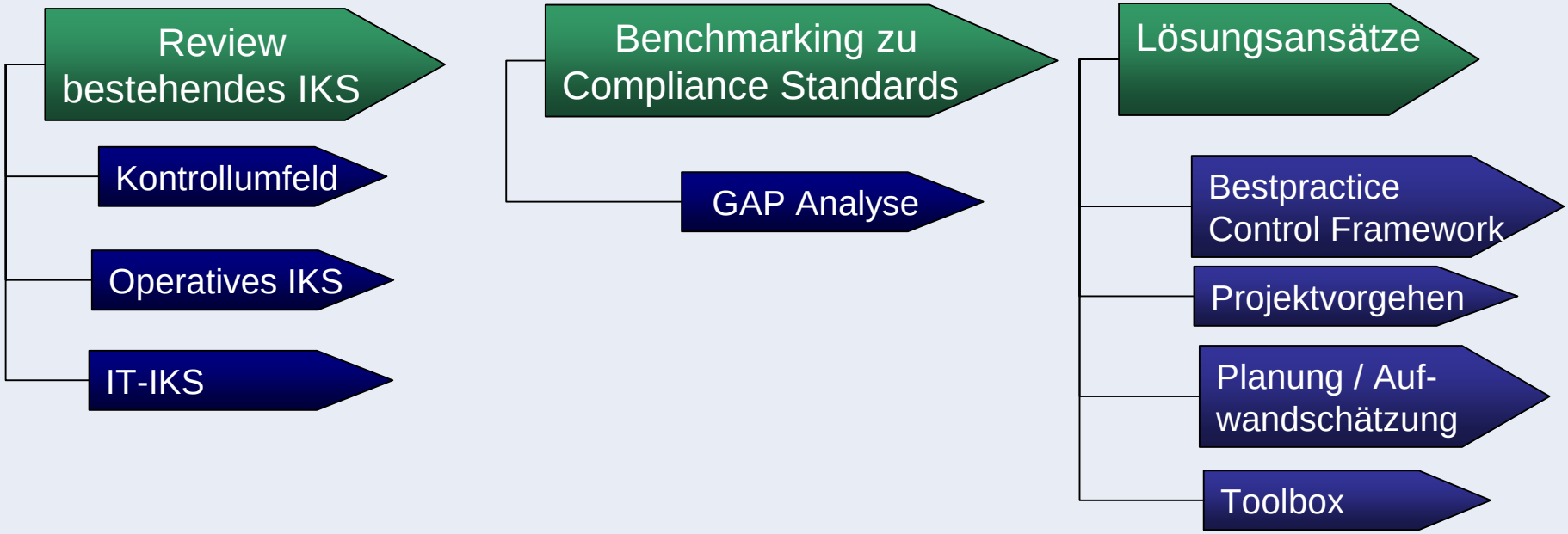
4 - Angst

"Schaffen wir es, zur Zeit bereit zu sein? Wird die externe Revision uns zertifizieren?".

5 - Erkennen des Mehrwertes

"Durch die Dokumentation und die konsequente Umsetzung des IKS konnten die Prozesse optimiert und die Kontrollen verbessert werden. Dadurch reduzierten sich die Fehler markant."

IKS Vorstudie: Vorgehensmodell



Framework

COSO Structure

COSO Component

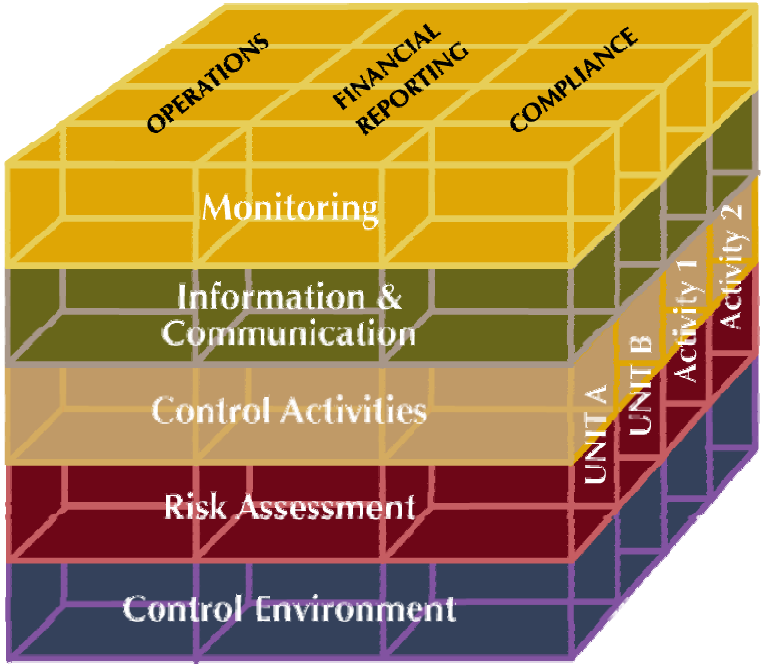
Cycle

Sub Cycle

Risk

Control Objective

Control Activities



Testing

Issue

Action Plan

Agenda

- Historie
- Gesetzgebung in der Schweiz
- GRC – Definition des Begriffs
- Handlungsbedarf für Schweizer Hochschulen
- Vorgehensansatz
- **Wie können EDV-Systeme im Bereich GRC unterstützen?**
- Fragen und Antworten

Berechtigungssysteme

Sprint Phase
(Get Clean)

Risiko-Identifikation & Minderung → **Rollenmanagement** → **Notfalluser**

Marathon Phase
(Stay Clean)

Betrieb Prävention

Workflows:

z.B. Genehmigungsprozess Reisemanagement

Reisender

Name	②	Reisenummer	①
Vorname	②	Kostenstelle	② + ③
Abteilung	②	Kostenträger	③
Nationalität	②	Weiterverrechnung	Kunden ③ / SAS
Destination	④		
Benchmarkpreis	⑤		
Abreisedatum	⑥		
Abreisezeit	⑥	Späteste Ankunftszeit	⑥
Rückreisedatum	⑥	Späteste Ankunftszeit	⑥
SBB ½ Tax	Ja / Nein ⑦	Begründung / Bemerkungen	
Bahnklasse	1. / 2.		
Hotel von	⑧		
bis	⑧		
Mietwagen von	⑧		
bis	⑧		

Reiseantrag

Vorgesetzte

per Workflow

Reise genehmigt: Ja ☐ Nein ☐

Genehmigung

per Workflow

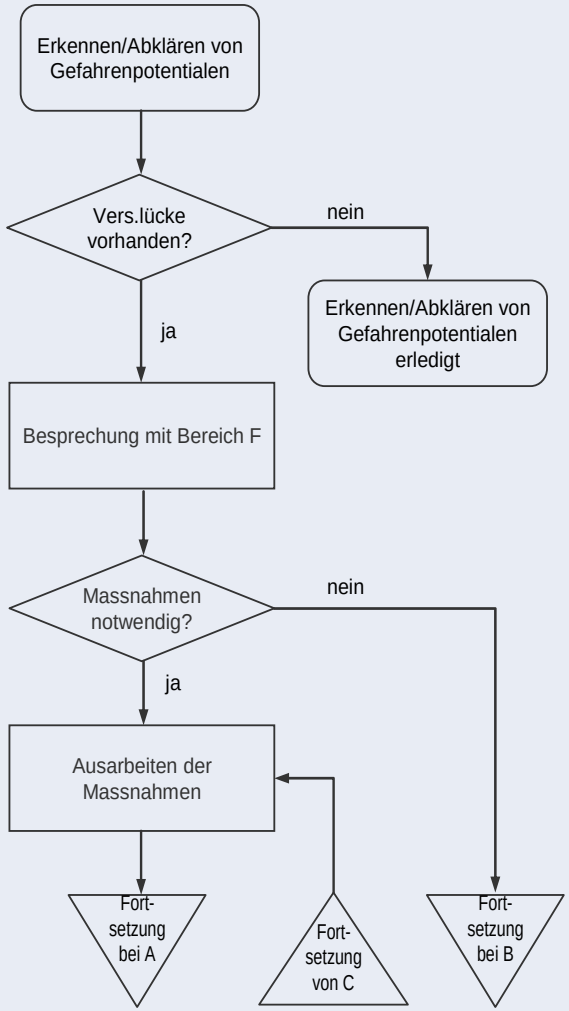
Reisebüro

Reise buchen
Info an Reisenden per E-mail

Qualitätssicherung
Reisebuchung

Prozesssteuerung

- Dokumentation aller relevanten Prozesse
- Definition und Dokumentation der Schlüsselkontrollen
- Risikoassessment und Definition der notwendigen Kontrollen müssen koordiniert ablaufen



Agenda

- Historie
- Gesetzgebung in der Schweiz
- GRC – Definition des Begriffs
- Handlungsbedarf für Schweizer Hochschulen
- Vorgehensansatz
- Wie können EDV-Systeme im Bereich GRC unterstützen?
- **Fragen und Antworten**

Fragen und Antworten

Besten Dank für Ihre Aufmerksamkeit

Kontaktadresse:

Clemens Gubler
Partner
clemens.gubler@novo-bc.ch
+41 79 610 69 80
+41 44 211 88 05

NOVO Business Consultants AG

Talstrasse 20
8001 Zürich

www.novo-bc.ch