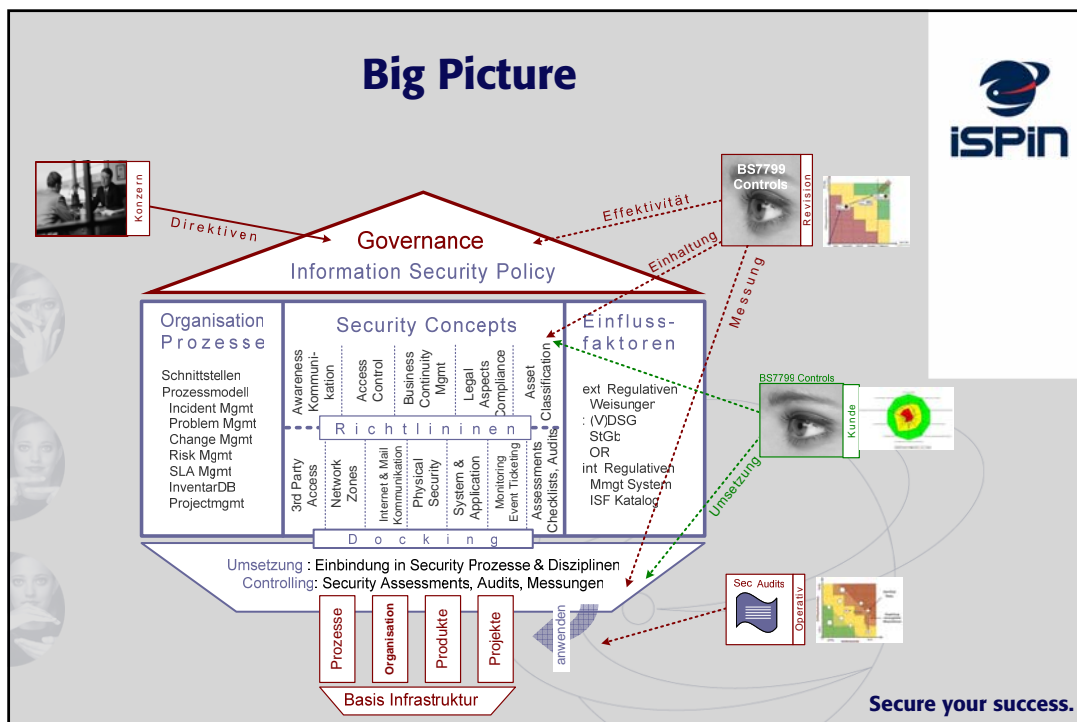


Lebbare und gelebte Informationssicherheit

-

Auswege aus einem Dilemma

10th Symposium on Privacy and Security, 1. September 2005,
Marco Marchesi, CEO ISPIN AG, President ISSA CH,
Vorstand Infosurance, Vorstand Datenschutzforum



Der Verwaltungsrat als Security Officer?

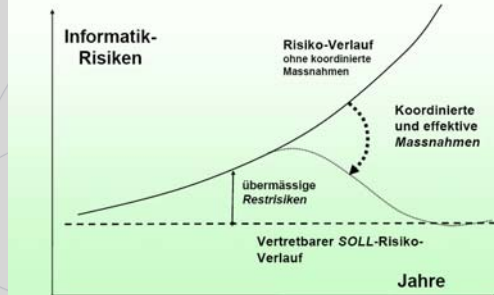


- Aufgabe: Strat. Führung
- Basis: Risikomanagement, Standards, Good Practice
- Keine Null-Fehlerstrategie
- Controlling: Wirksamkeit der Massnahmen sicherstellen



© Ad Vantis AG

Dr. Urs E. Zurlfluh



© Ad Vantis AG

Dr. Urs E. Zurlfluh

Rolle der IT-Security in Compliance Projekten



168 Wörter für \$ 10 – 20 Mrd. !

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.
 (a) **RULES REQUIRED.**—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
 (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
 (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
 (b) **INTERNAL CONTROL EVALUATION AND REPORTING.**—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

- Die jährlichen Kosten für Unternehmen durch den SEC. 404, Sarbanes-Oxley Act werden auf ca. \$ 10 – 20 Mrd. geschätzt.
- Eine Studie der Financial Executives International (FEI) von März 2005 ergab:

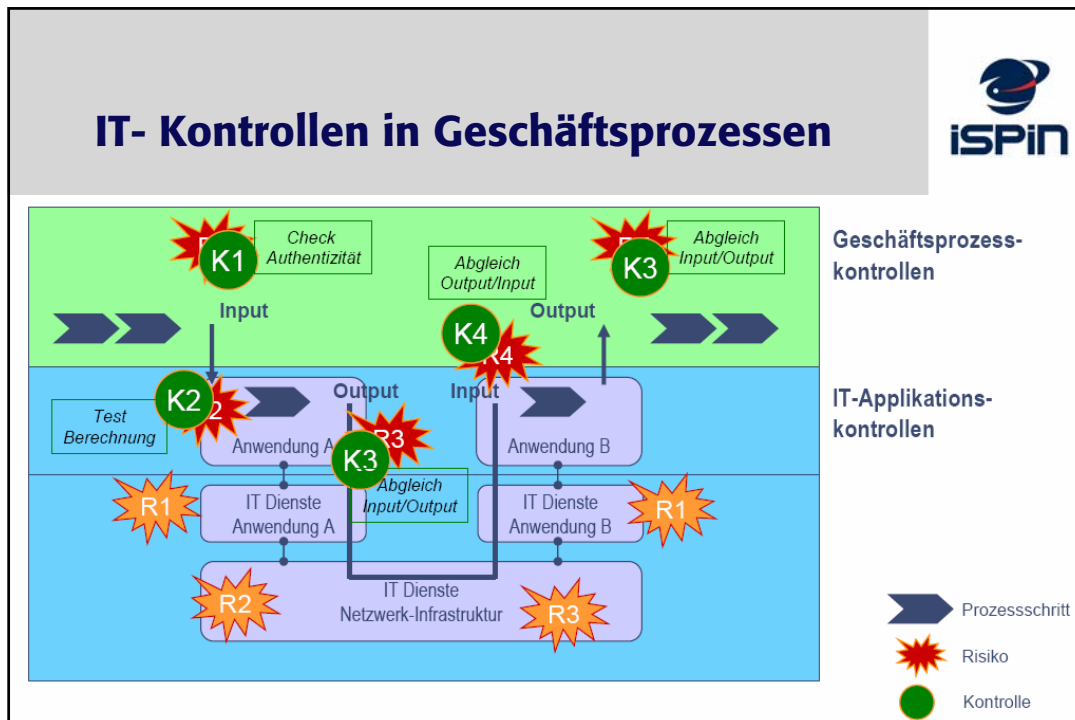
Für 217 Unternehmen mit durchschnittlichem Umsatz von \$ 5 Mrd. betragen die durchschnittlichen Kosten für SEC. 404: \$ 4.36 Mio, d.h. ca. 0.1 % des Umsatzes.

www.fei.executiveboard.com



Trend: Kosten für SOX-Compliance treffen kleinere Unternehmen härter!

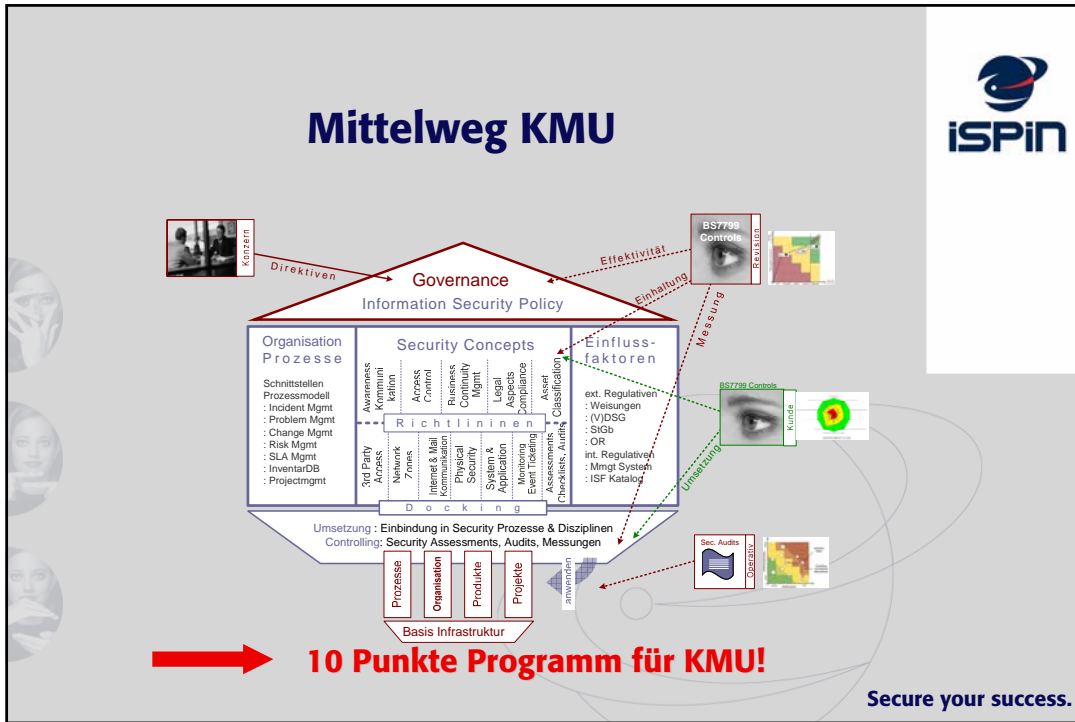
Secure your success.



Schlussfolgerungen zu SOX

- Zunehmende Gleichrichtung von Compliance-Anforderungen durch Gesetze. Gefordert sind ein
 - Formales System zum Management Operationeller Risiken
 - Internes Kontrollsystem zur Sicherung der ordnungsmässigen Geschäftsführung
- Anhand von SOX-Projekten kann man lernen
 - Grundsätzliche Richtung und Massnahmen; Stärken, Schwächen, Chancen und Risiken
- Kombination von **Governance, Risk & Compliance** verspricht Optimierung von Wertschöpfung und Werterhalt

Secure your success.



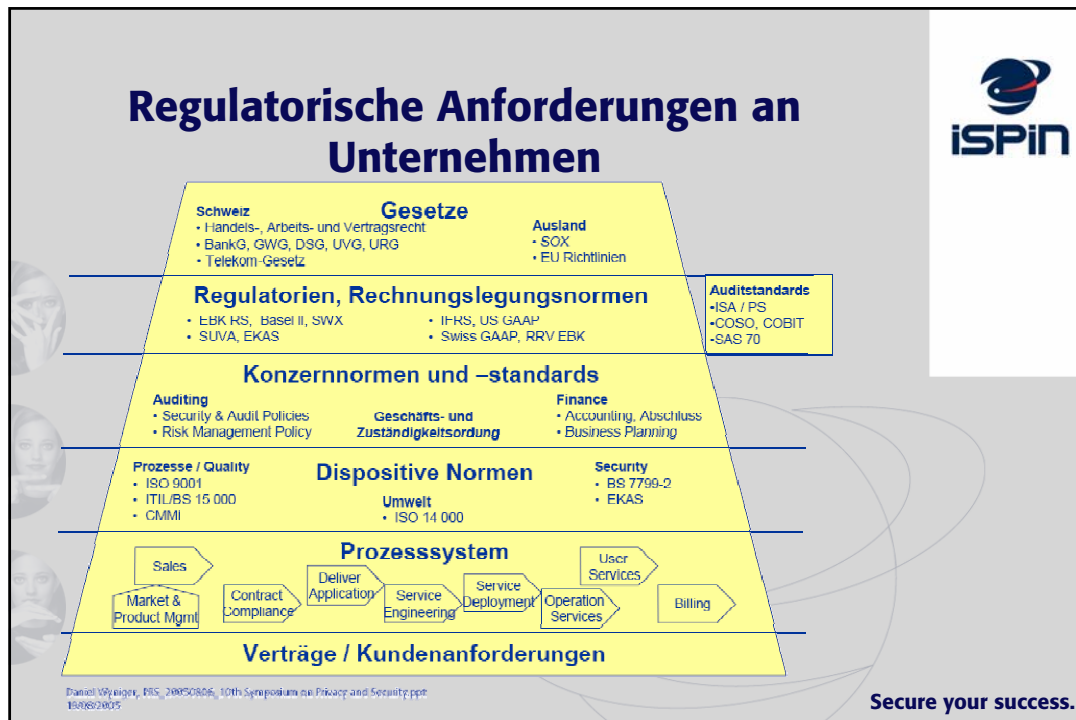
Wo stehen die Schweizer Unternehmen?

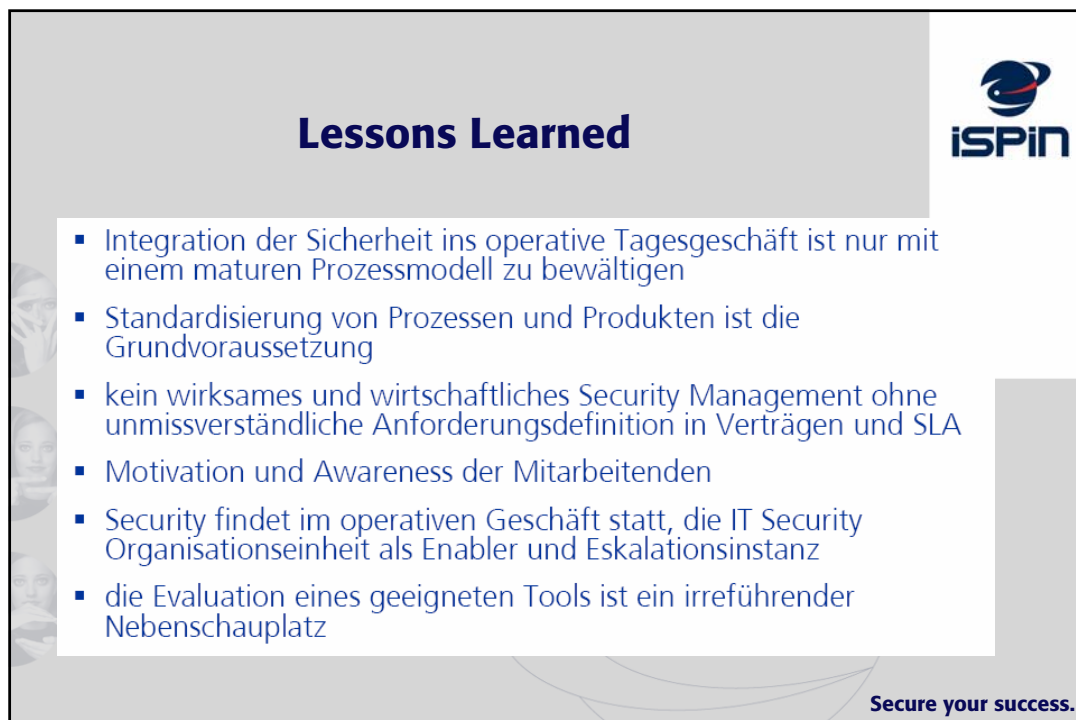
- Neben Standards wird auf eigene Ansätze vertraut
- Gap zwischen Prozessorientierung und eingesetzten Instrumenten

Kategorie	Prozent
Richtlinien und Policies	21,97%
Verantwortungsträger	16,14%
Kontroll- und Messpunkte	10,31%
Risikokataloge	13,45%
Prozessbeschreibungen	35,71%
Managementtools	6,28%
Technische Sicherungs-massnahmen	20,63%

Instrument	Prozent
Eigene Systematik	~45%
BS7799	~28%
BSI Grundschatz	~25%
EBK-Richtlinien	~15%
SOX	~10%
CobIT	~8%
BSI5000	~7%
Good Privacy Datenschutz	~6%
IT_Sec	~4%
ISO 1335	~3%

ISPIN



- ## Lessons Learned
- 
- Integration der Sicherheit ins operative Tagesgeschäft ist nur mit einem maturen Prozessmodell zu bewältigen
 - Standardisierung von Prozessen und Produkten ist die Grundvoraussetzung
 - kein wirksames und wirtschaftliches Security Management ohne unmissverständliche Anforderungsdefinition in Verträgen und SLA
 - Motivation und Awareness der Mitarbeitenden
 - Security findet im operativen Geschäft statt, die IT Security Organisationseinheit als Enabler und Eskalationsinstanz
 - die Evaluation eines geeigneten Tools ist ein irreführender Nebenschauplatz
- Secure your success.**

Fazit



- Risiko-Orientierung als Grundsatz
- Lebbare, dem Schutzbedarf entsprechend, wirtschaftlich tragbare IS aufbauen
- Information Security Organisation nicht in der IT
- IS in täglichen Arbeitsprozessen integrieren
- Keine Tool-Diskussion, sondern Methodik-Diskussion führen

Secure your success.

Mut besteht nicht darin,
dass man Gefahren blind
übersieht, sondern darin, dass man
sie sehend überwindet.

**Unternehmen Sie den ersten Schritt
für eine klare Risikosicht.**

