

# ***Compliance - hype oder real?***

Author: Sascha-A. Beyer

# Compliance

- ↑ Der Begriff Compliance bezeichnet die Gesamtheit aller Maßnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Organisationsmitglieder und seiner Mitarbeiter im Hinblick auf alle gesetzlichen Ge- und Verbote begründen.
- ↑ Darüberhinaus soll die Übereinstimmung des unternehmerischen Geschäftsgebahrens auch mit aller gesellschaftlichen Richtlinien und Wertvorstellungen gewährleistet werden.

(Wikipedia, Internet)

# Compliance ist Teil der IT Industrie

## Buzzword des 21. Jahrhunderts

- Alle Anbieter sind nun “compliance experts”
- Die meisten reduzieren compliance auf eine technische Box Lösung
- Viele versprechen Ihren Kunden Compliance

## Aber

- Nur wenige Anbieter haben echte Fachleute für den Compliance Bereich
- Die meisten nehmen ein Kopie des jeweiligen Standards und übergeben ihn an die Entwicklung: “macht was draus!”
- Nur wenige beachten Anleitungen der Behörden und/oder industriellen Fachgruppen
- Noch weniger haben tatsächlich enge Bindungen zu den relevanten Behörden
- Keine sind staatlich bestätigt



# Compliance Realität

Nach dem Gartner Analysten Robert Handler sind sich alle Experten auf diesem Gebiet einig, daß - obwohl Milliarden ausgegeben werden - 100% Compliance “grundsätzlich unmöglich” ist.

- *InfoWorld* (U.S.), Dezember 2005

Compliance ist ein Risiko Gebiet das Verwirrung und Verzweiflung in Organisationen hervorruft, da es als isoliertes Projekt angegangen wird...eine steigende Belastung wird ...und aufgrund von Fragmentierung zu einem größeren Risiko führt.

- Michael Rasmussen, Forrester, November 2005

# Wie reagieren Unternehmen auf die Standards

- Gar nicht – entweder sind die Anforderungen nicht bekannt oder werden (bewußt) ignoriert
- Moderat – oft mit einem “Schnellschuß” um ein bevorstehendes Audit zu überstehen. Hierbei wird in der Regel die Chance Risiken zu minimieren übersehen! Die Wahl des Standards ist oft nicht fundiert und erhöht den Aufwand.
- Ernsthaft – der oder die Standards werden genutzt um gezielt und pragmatisch Risiken zu minimieren. Und “beiläufig” entsteht eine solide Grundlage um mit wenig Aufwand auch gegenüber zukünftigen Standards compliant zu sein.

# Situation

↑ Unternehmen müssen eine Vielzahl von Standards, Gesetzen und Regularien einhalten

↑ Es gibt über 250 ISO-Normen auf den unterschiedlichsten Gebieten:

- Technische
- Klassifikatorische
- Verfahrensstandards

und eine Vielzahl von anderen Standards, wie z.B. der Sicherheitsstandard BS7799

# Das Problem

↑ Viele Standards werden in Unternehmen schon seit langer Zeit richtig und gut umgesetzt, sofern diese zum Kernwertschöpfungsprozess gehören (z.B. ISO 9000 Qualitätsmanagement oder ISO 14001 Umweltmanagementnorm). Prozessknowhow zum Umsetzen von Standards ist in der Regel vorhanden

# Das Problem

↑ Aber: Informationssicherheit ist nicht die Kernkompetenz der meisten Unternehmen

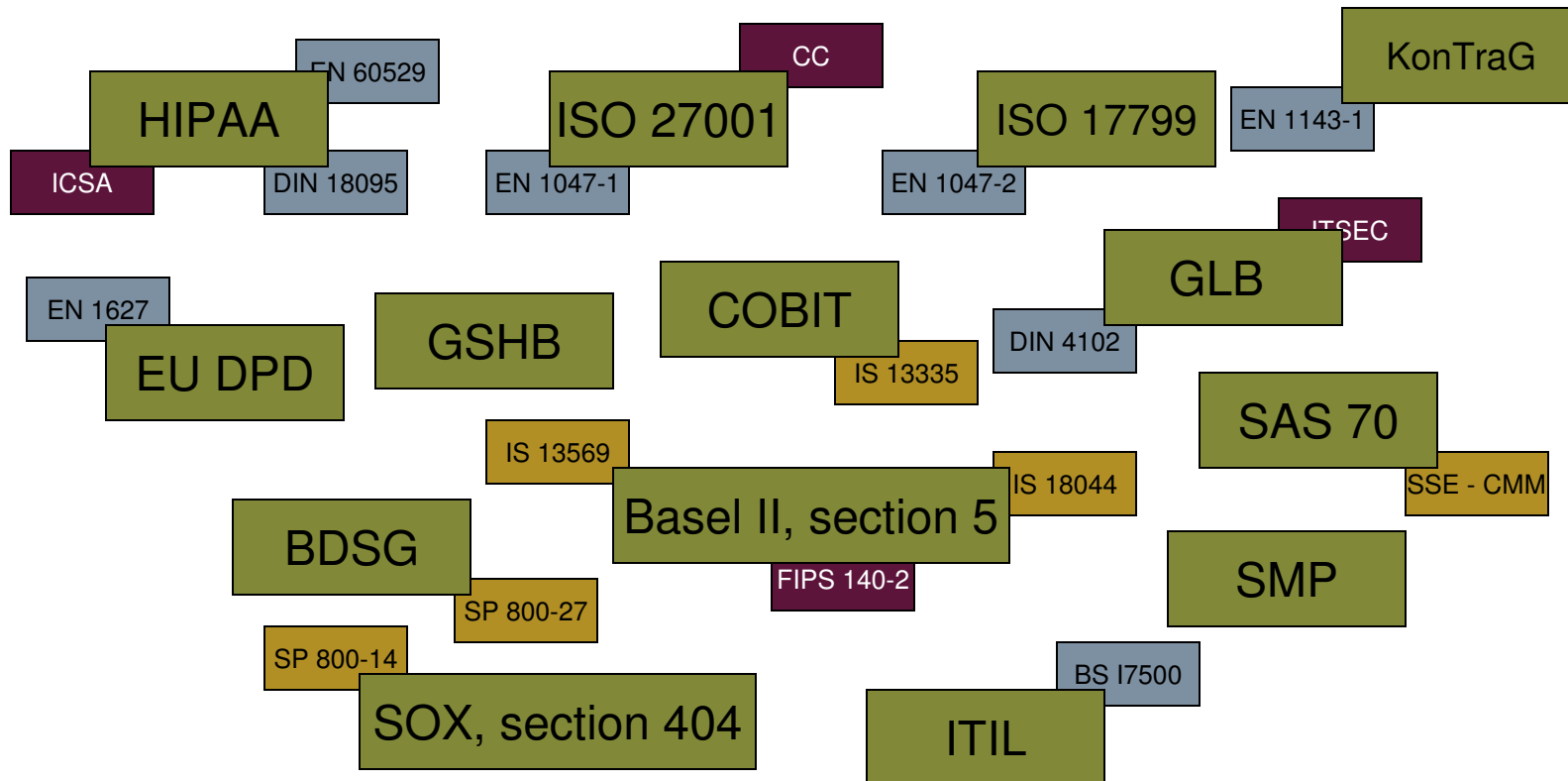
- Welche Sicherheitsstandards gibt es?
- Welcher Sicherheitsstandard ist notwendig oder sinnvoll?
- Wie wird dieser implementiert?
- Wie demonstriere ich compliance?

Bis 2010 werden Unternehmen, die Einzellösungen für ihre Compliance Herausforderungen wählen, 10 mal mehr für den IT Teil der Compliance Projekte bezahlen, als Unternehmen die einen proaktiven und integrierten Ansatz wählen (0.9 Wahrscheinlichkeit)

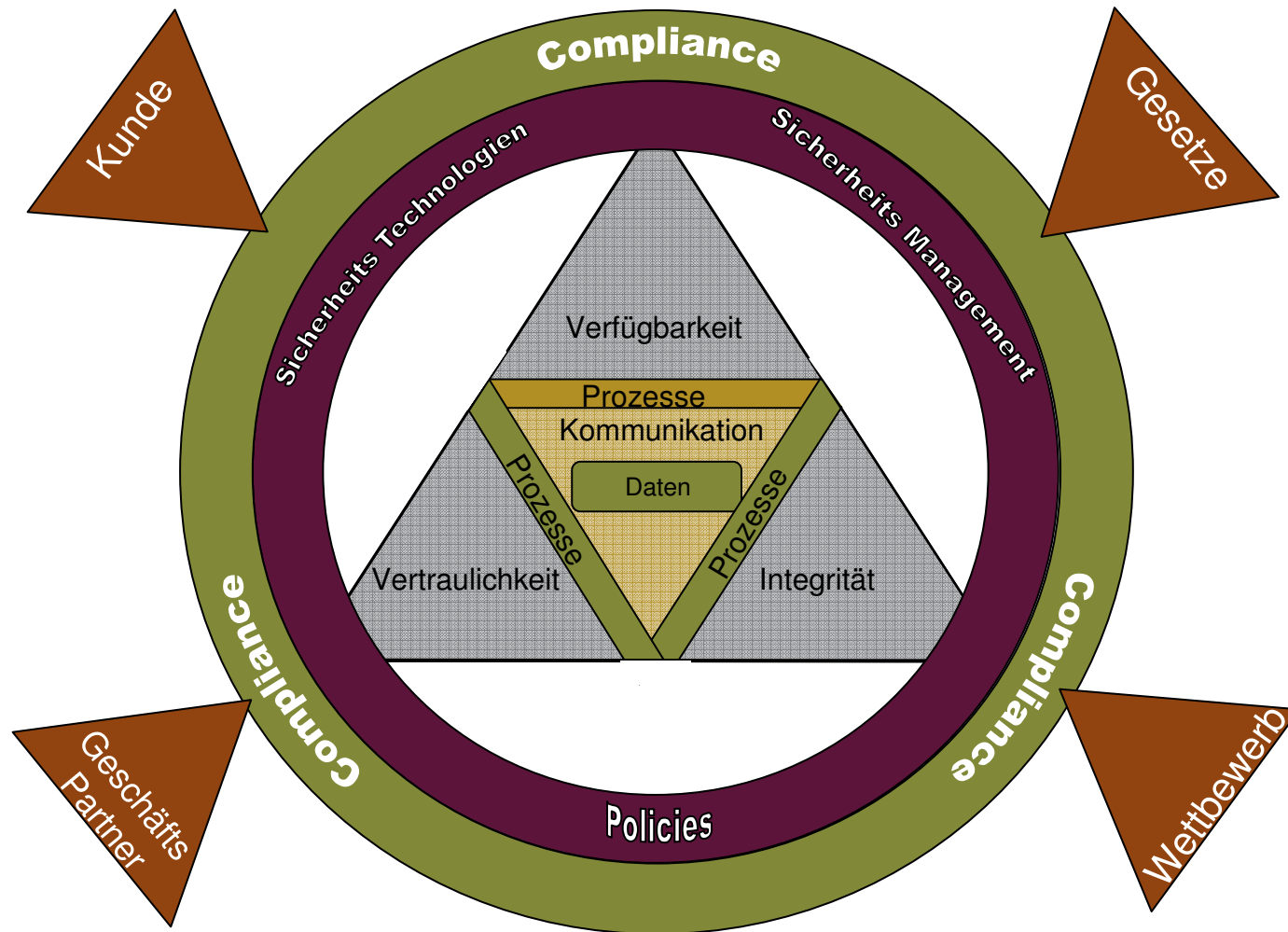
(Gartner: Understanding the Costs of Compliance, 7 Juli, 2006)



# Es gibt viele Regularien und Sicherheitsstandards oder Standards mit deutlichem Sicherheitsbezug!



# Compliance – Bindeglied zwischen Anforderungen und Sicherheit



# Motivation

## ↑ Gesetze

- schreiben Sicherheitsmassnahmen vor

## ↑ Kunde und/oder Geschäftspartner

- verlangt nach bestimmten Standards um an seiner Wertschöpfungskette teilzunehmen (Zugriff auf Datenbanken, Prototypenschutz etc.)

## ↑ Konkurrenz

- erfüllt bestimmte Sicherheitsstandards und hat somit Marktvorteile
- zwingt zu Sicherheitsmassnahmen (Schutz von Geschäftsgeheimnissen etc.)

# Wahl des Standards

- ↯ Die Wahl zu einem oder mehreren Sicherheitsstandards ist eine strategische Entscheidung
- ↯ Sinn und Zweck darf dabei niemals nur „Compliance“ sein – Sie wollen IHRE Sicherheit erhöhen und RISIKEN minimieren!
- ↯ Es muss geklärt werden:
  - Warum muss ich Compliant sein
    - welche Gesetze?
    - welche Kundenvorgaben?
    - welche Marktzwänge?
    - welche Risiken?
      - Externe Risiken (Haftungsrisiken etc.)
      - Interne Risiken (Standard=best practice verlangt AV etc.)

# Neue Tendenzen

- ↑ Multinationale Konzerne müssen gegenüber vielen Standards und Regeln compliant sein und zwingt sie zum nachhaltigen Wirtschaften
- ↑ Aber nicht nur im Zuge des nachhaltigen Wirtschaftens verlangen sie immer häufiger, das ihre Zulieferer gegenüber
  - Bekannten Standards (BS7799, ISO27001 etc.)
  - Oder eigenen Standardscompliant sind.
- ↑ Im Zuge der Extended Company Entwicklung verschwinden die Grenzen zwischen den Unternehmen bei der Informationsverarbeitung – d.h. Die **Sicherheitsstandards der Konzerne werden auf die Zulieferer weitergeleitet.**
- ↑ Nachdem Unternehmen intern ihre Sicherheit und Compliance auf den Weg gebracht haben, bewegt sich der Focus nun auf die Geschäftspartner.

# Business Partners-Commercial Compliance

“ Compliance gegenüber Gesetzen ist nicht die einzige Compliance Form.

Commercial compliance – also Regeln die ein Unternehmen folgen muss um mit anderen Unternehmen Geschäfte zu betreiben... werden auch immer wichtiger werden.”

- *Gartner Report: “Understanding the Components of Compliance”, John Bace, Carol Rozwell, 7 Juli 2006*



# Beispiele

## ↑ Fragebogen zum nachhaltigen Wirtschaften (Informationsschutz)

- **Wurden nachweislich aussagefähige Schutzbedarfs- und Risikoanalysen durchgeführt?** (Themen: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität)
- **Verfügen Sie über ein anerkanntes aktuelles Informationsschutz Testat (Audit)?** (Themen: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität; siehe auch Informationsschutz-Rahmenanforderungen auf der Homepage für Zulieferer)

## ↑ Geheimhaltungsvereinbarung

- ...hat das Recht, sich jederzeit vom Umfang und Zustand der vom [Geheimnissträger] getroffenen Maßnahmen auch in seinem Betriebstätten und Geschäftsräumen zu überzeugen.
- Unabhängig von den vorstehenden Regeln wird festgelegt, dass der ...für jeden gesonderten Einzelfall der Zuwiderhandlung gegen diese Geheimhaltungsverpflichtung 50.000,00 € Vertragsstrafe zahlt.

## ↑ Nutzungsvertrag Austausch CAD Daten

- ... wird ein schriftlich fixiertes Sicherheitskonzept vorlegen, in dem die vorgegebenen Sicherheitsstandards der Anlage ... beachtet sind und einen Nachweis einschließlich einer schriftlichen Bestätigung über deren Einhaltung führen.

# Risk-Based Compliance: ermöglicht

- ↑ Bessere und besser informierte Risiko Entscheidungen
- ↑ Besseres Verhältnis zu Behörden, Auditoren, Geschäftspartnern
- ↑ Verwendet Compliance Ressourcen dort, wo sie am meisten gebraucht werden.

Es ist keine technische Fragestellung

Es ist.....

eine Notwendigkeit die eng mit allen Bereichen einer Organisation verwoben ist.

# Introduction to Cybertrust

## The Global Information Security Specialist

- 100% focused on security since 1989
- Full range of security & compliance offerings
- Product-independent intelligence
- Flexible Delivery
- Combination of in-depth technical & business expertise
- Specialise in the complex needs of large enterprises
- Professional services, managed services and technologies



*Aligning Security to your Business*



# Market leadership

## Analysts

- Largest privately held security company (Gartner)
- Largest Managed Security Services (Frost & Sullivan)
- Leader in Security Risk Management (The Yankee Group)
- Largest provider of Forensic Services and PCI Certifications

## Customers

- 4,000+ clients
- Over 50% of leading companies
- Governments around the globe

## Company

- Founded 1989
- 950+ people
- Global offices
- Over €200 Million in revenue

## Proven Abilities

- Predicted every major Internet attack in the last four years
- Increased operational efficiency by 75%
- Secure €4 trillion in bank transfers per annum





Vielen Dank !

Für Fragen oder Feedback stehe ich gerne zur  
Verfügung

**Sascha-A. Beyer**

**[Sascha.Beyer@Cybertrust.com](mailto:Sascha.Beyer@Cybertrust.com)**

**Office : +49 2102 420 774**

**Mobile: +49 172 9320396**