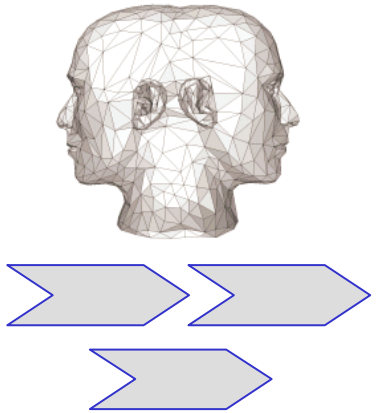
GenericIAM

generische Prozesse für das
Identity- und Access Management



Task Force Compliance - Update

Version 1.0

Ein kurzer Rückblick

- Entstanden aus Diskussion um „NIFIS-GenericIAM-Compliance-Checkliste“ (Dez. 2006)
- Formulierte Ziele (März 2007)
  - Sammlung weiterer Informationen zum Thema Compliance
  - Zusammenfassen der gewonnenen Arbeitsergebnisse in einer Präsentation (mittelfristiges Ziel)
  - Erarbeiten einer Identity und Access Management Readyness Checkliste (langfristiges Ziel)
- Erste Präsentation auf 5. GenericIAM Meeting in Düsseldorf
- Erstes Feedback
  - Der Aspekt wie die Compliance Anforderungen die generischen Prozesse beeinflussen muss klarer herausgearbeitet werden
  - Problem: sehr viele, sehr unterschiedliche Regelungen, die teilweise auch Branchen-/Zielgruppenspezifisch sind -> Einfluss der Compliance Anforderungen auf generische IAM-Prozesse nicht abbildbar!

Häufig sind mehrere Regelwerke zu beachten

- FISMA (US)
- NIST 800-53
- HIPAA
- Canadian and Asian Privacy Laws

Gesundheit

Öffentliche Verwaltung

Übergreifende Regelwerke

- SOX
- PIPEDA
- Canada Multilatéral Instrument 52-111
- CA SB-1386
- EU Data Protection Directive

Finanzwesen

Energie

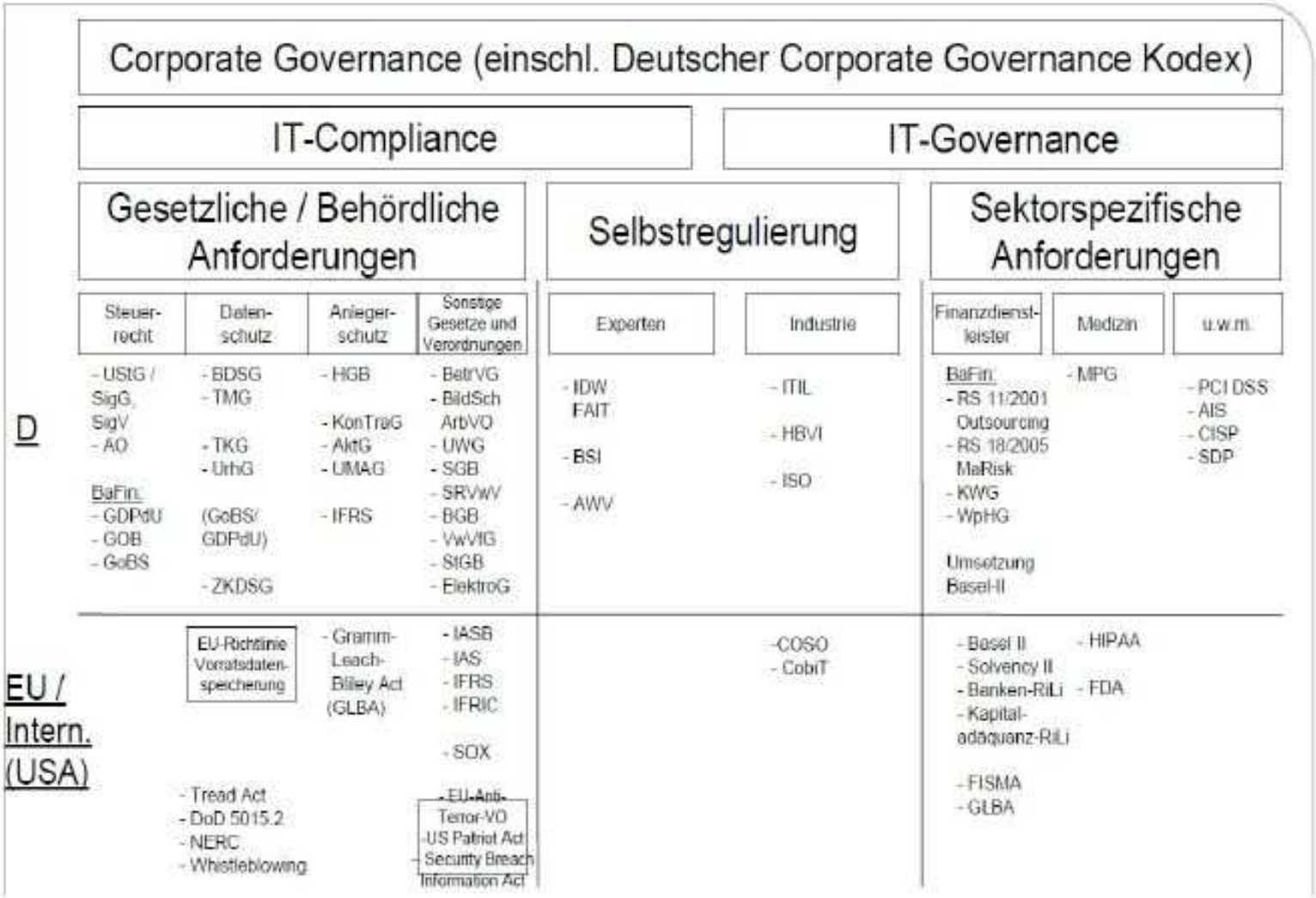
Umwelt und Chemie

- GLBA* and USA Patriot Act
- Basel II
- PCI/DSS*
- NASD 3010/3110
- MiFiD
- Solvency II

- NERC CIP 1300
- Energy Bill of 2005

- FDA 21 CFR 11

Beispiele für externe Anforderungen



Diskussion

- Gibt es einen Einfluss auf die generischen IAM-Prozesse?
  - Woraus lässt sich dieser ableiten?
  - Gibt es eigenständige generische Prozesse, die sich aus Compliance Anforderungen ableiten lassen?
- Gibt es Möglichkeiten der Fokussierung?
- Wie soll weiter verfahren werden?