Informations- / IT-Sicherheit Standards

Überblick über Ziele, Anforderungen, Nutzen

Gesellschaft für Informatik e.V., Sicherheit 2008, Saarbrücken

Ingrid Dubois

dubois it-consulting gmbh

Informationssicherheit

Angemessenen Schutz für Informationen

Vertraulichkeit, Verfügbarkeit, Integrität

Compliance

Erfüllen der Anforderungen

Effizienz

Verbessern der Prozesse

Zufriedenheit

von Kunden und Mitarbeitern

Vorteile auf dem Markt

bei Kunden und Lieferanten

...

Standards zum Informations-Sicherheitsmanagement

- **BSI-Standard 100-1**
  Managementsysteme für Informationssicherheit (ISMS)

- **ISO/IEC 27001:2005**
  Information security management systems – Requirements
- **ISO/IEC 27002:2007**
  Code of practice for information security management

- **ISO/IEC 13335-x:yyyy**
  Management of information and communications technology security.
  Concepts and models for information and technology security management

- **BS 25999-1:2006**
  Business continuity management – Code of practice
- **BS 25999-2:2007**
  Business continuity management – Specification

BSI: Bundesamt für **S**icherheit in der **I**nformationstechnik
ISO: **I**nternational **S**tandardization **O**rganization
IEC: **I**nternational **E**lectrotechnical **C**ommission
BS: **B**ritish **S**tandard

Standards mit Bezug zur Informationssicherheit

- **DIN EN ISO 9001**
  Anforderungen an Qualitätsmanagementsysteme

- **IT Infrastructure Library ITIL**
  Sammlung von “best practices“ für IT-Services (ITSM (IT Service Management))
  Sicherheitsmanagement-Prozess orientiert sich an BS 7799

- **ISO/IEC 20000** (IT Service Management (ITSM)
  Part 1: Information technology - Service Management - Specification
  Part 2: Information technology - Service Management - Code of Practice

- **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology (**CObIT**)
  ‘IT governance‘ Richtlinien, um IT und Unternehmensziele zu überwachen

Weitere Standards mit Bezug zu Informations-/IT-Sicherheit

- **OECD-Richtlinie zur Sicherheit von IT-Systemen und Netzwerken**
- **PS 330** (**P**rüfungs**s**tandard des Instituts für Wirtschaftsprüfer)
- **SAS70** (**S**tatement on **A**uditing **S**tandards Number 70)
- **GPG (G**ood **P**ractice **G**uidelines**)**
- **PCI DSS** (**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard)
- **CoSO** (**Co**mmittee of **S**ponsoring **O**rganizations, Treadway Commission)
- **ISO/IEC 15408-x:2005, C**ommon **C**riteria **(CC)**
- **TIA-942** (**T**elecommunications **I**ndustry **A**ssociation Data Center Standards)
- …

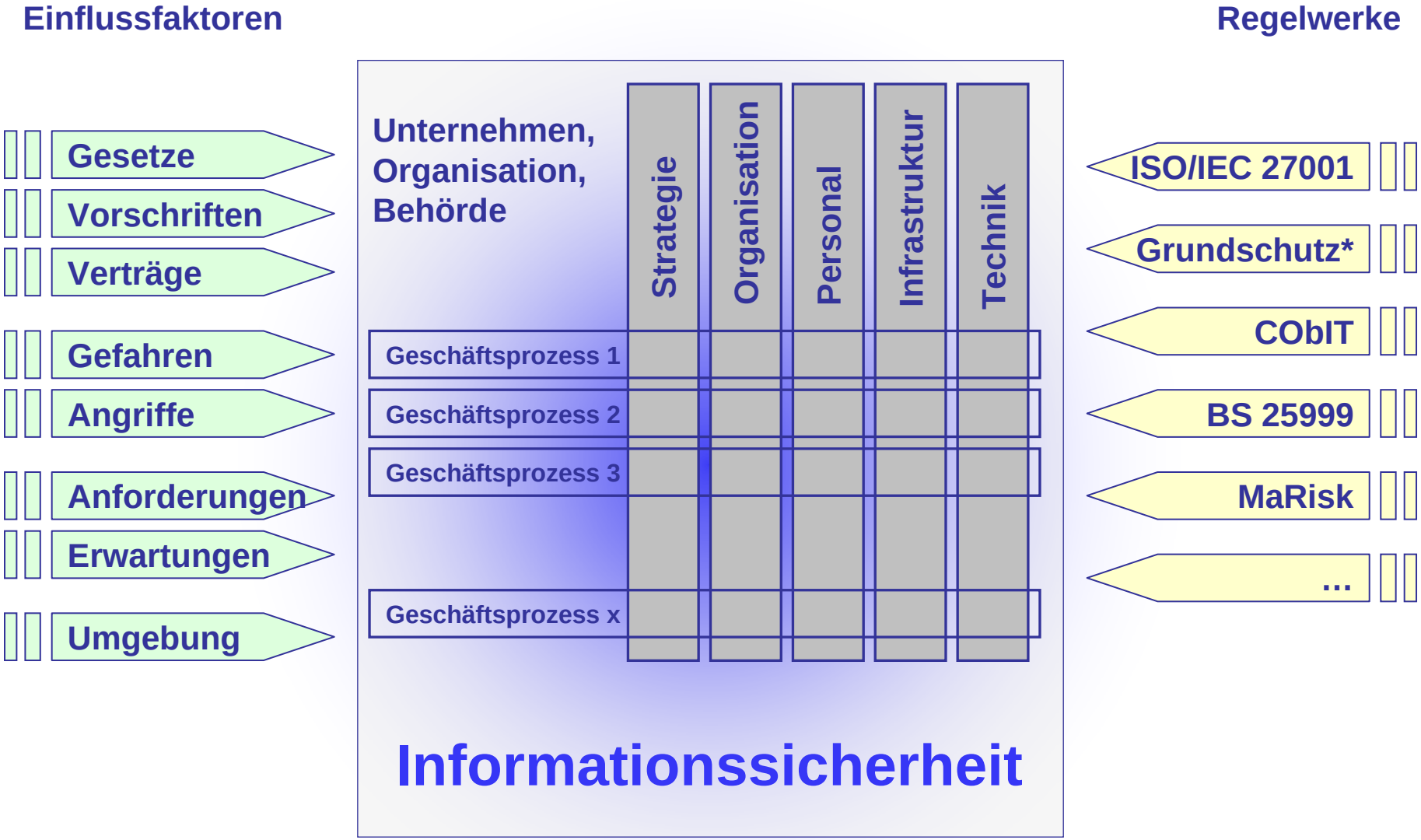
IT- und Computerrecht

- **Gesetze, die nahezu jedes Unternehmen / jede Organisation betreffen**
  - **H**andels**g**esetz**b**uch **(HGB)**
  - **T**elekommuni**k**ations**g**esetz (TKG), **T**ele**m**edien**g**esetz **(TMG)**
  - **Urh**eberrechts**g**esetz (UrhG) **…**

- **Gesetze, die je nach Geschäftsfeld oder Auftrag zu beachten sind**
  - **G**esetz zur **Kon**trolle und **Tra**nsparenz **(KonTraG)**
  - Datenschutzgesetze (Bundes- oder Landesdatenschutzgesetze, ggf. weitere)
  - **S**arbanes **O**xley **A**ct **(SOA)**
  - **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (**HIPAA)**
  - **F**ood and **D**rug **A**dministration **(FDA)**
  - **M**arkets **i**n **F**inancial **I**nstruments **D**irective (**MiFID)**
  - 8. EU-Richtlinie (Euro-SOX) ab Juli 2008
  - **…**

- **Vorschriften**
  - **A**bgaben**o**rdnung (AO), GoB, GoBS, GDPdU, ..
  - Bildschirmarbeitsplatzverordnung
  - **MaRisk** (Mindestanforderungen an das Risikomanagement)
  - …

Informationssicherheit & zuverlässige Geschäftsprozesse



* ISO/IEC 27001 auf der Basis von IT-Grundschutz

Dankeschön

eingetragenes Markenzeichen der dubois it-consulting gmbh