Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2a)

Vorlesung im Sommersemester 2013

an der Universität Ulm

von Bernhard C. Witt

2. Grundlagen der IT-Sicherheit

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes	➔	Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
✓	Technischer Datenschutz		Risiko-Management
✓	Kundendatenschutz		Konzeption von IT-Sicherheit

Anforderungen zur IT-Sicherheit:

- Compliance
- Stand der Technik / internationale Standards
- Einflussfaktor Recht
- Einflussfaktor Technik
- Einflussfaktor Unternehmens-spezifika

Compliance (1)

Definition 8: Compliance
Übereinstimmung mit festgelegten Regeln

Zu den festgelegten Regeln zählen:

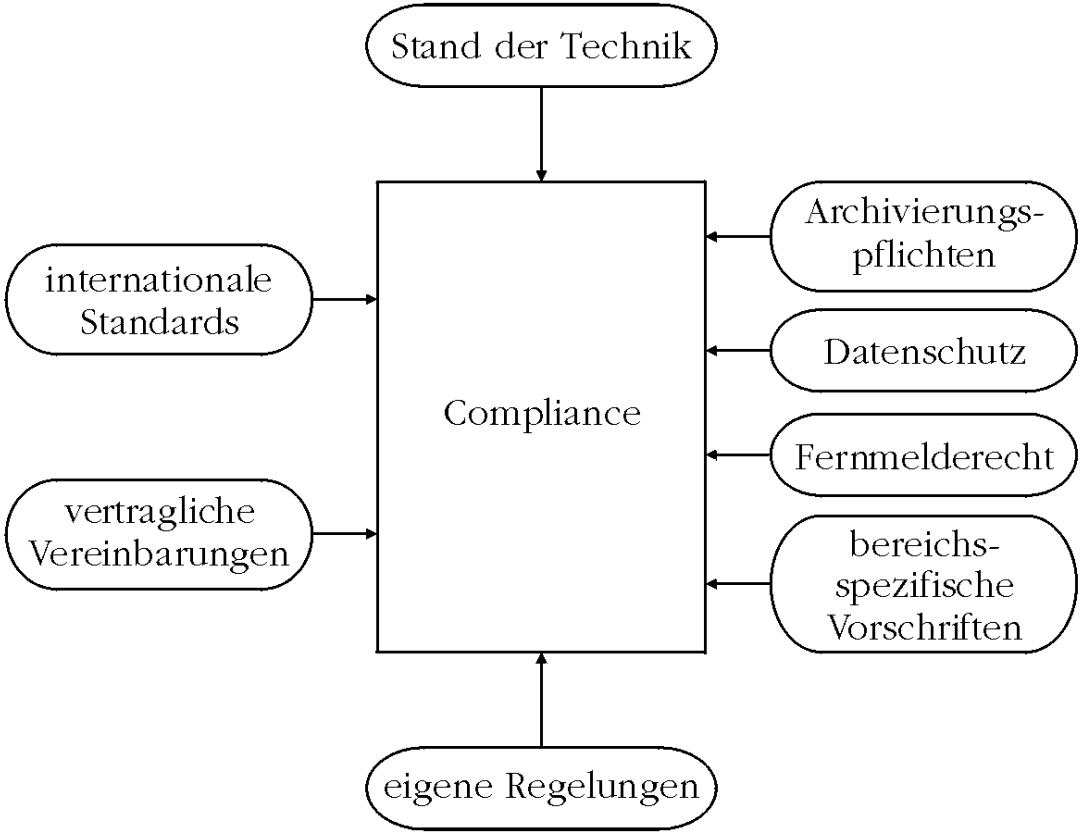
→ Rechtliche Regeln

→ Best practice Regeln (internationaler) Standards

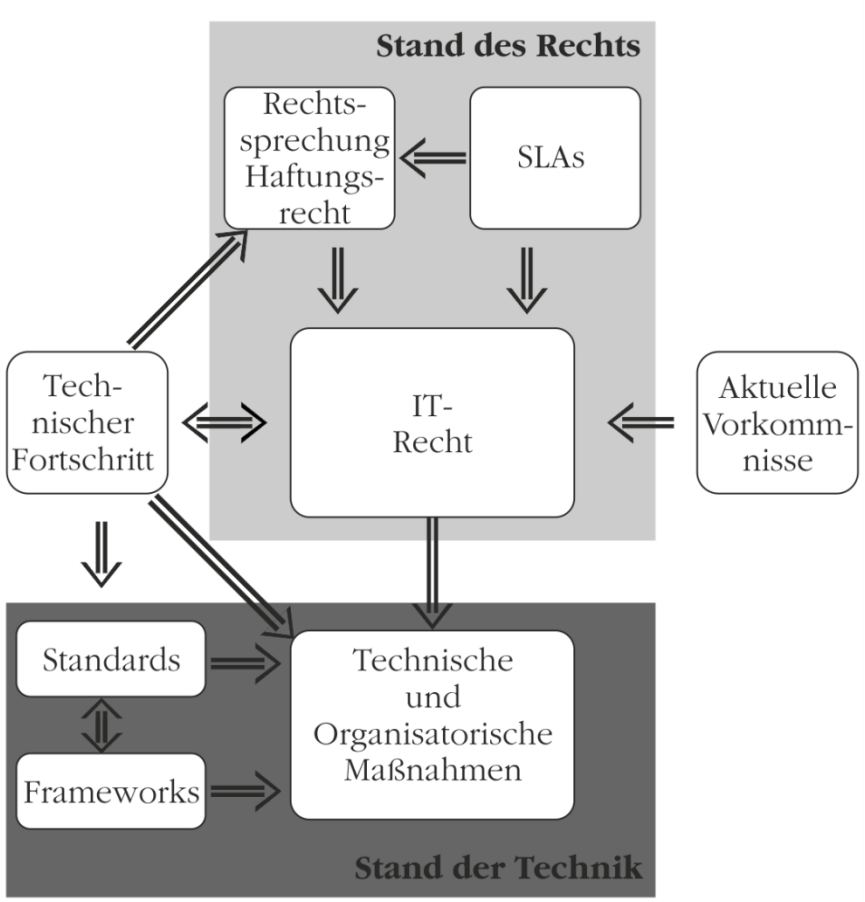
→ Regeln aufgrund von Verträgen mit Kunden (insb. zu SLAs)

→ Interne Regeln (Richtlinien, Policies, Dienstanweisungen)

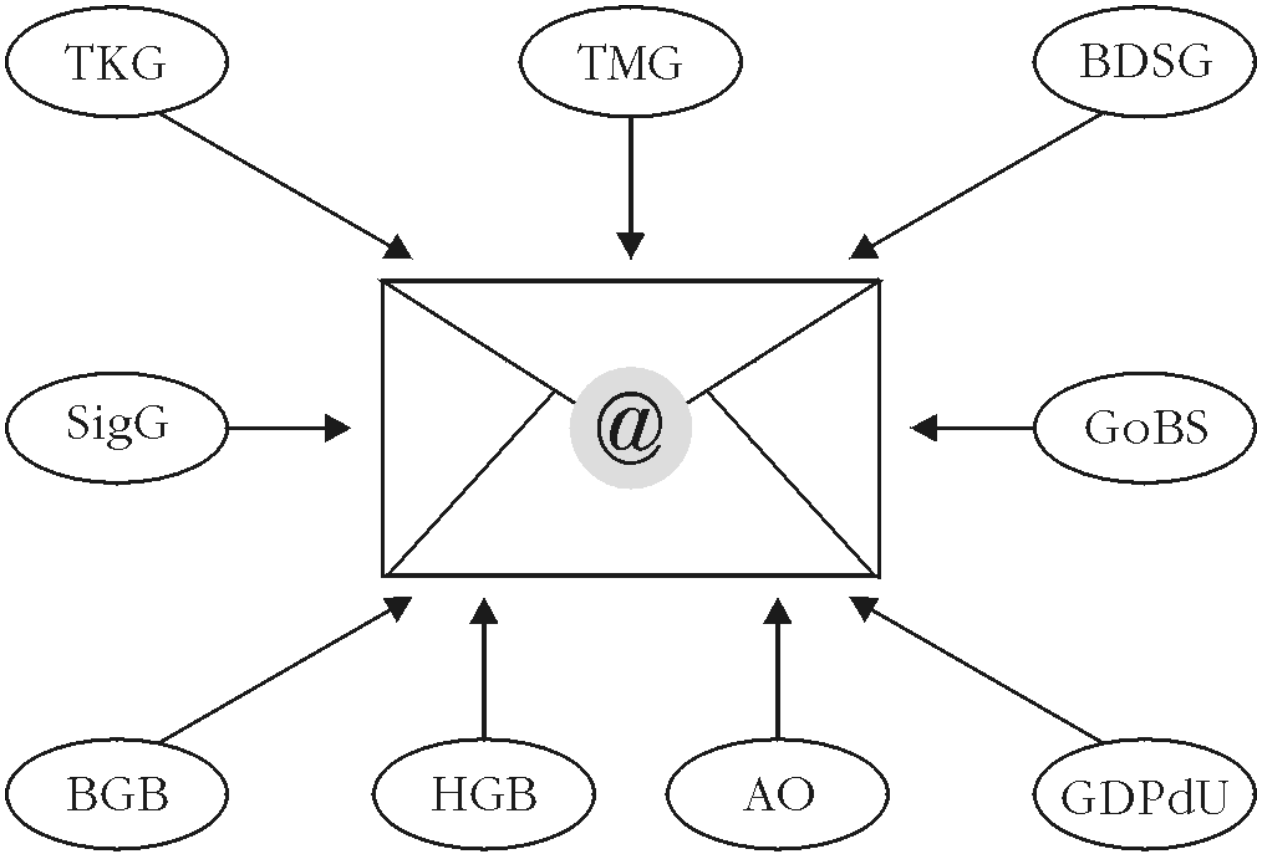
Compliance (2)



Compliance (3)



Beispiel: E-Mail-Compliance (1)



Beispiel E-Mail-Compliance (2)

Dient eine E-Mail
- der Anbahnung,
- dem Abschluss
- oder der Verwerfung

eines Handelsgeschäftes
oder der Mitteilung zur bestehenden Geschäftsbeziehung,

so ergibt sich eine **Archivierungspflicht**!
(u.a. § 37a HGB i.V.m. § 257 HGB bzw. §§ 145-147 AO)

→ 10 Jahre bei Abschlussrelevanz, sonst 6 Jahre

Beispiel E-Mail-Compliance (3)

- stellen E-Mails Geschäftsbriefe dar?

→ **Aufbewahrung & Absicherung** der E-Mails!
Bereits Zugang hat ggf. Rechtsfolgen!
Aussonderung von SPAM & Malware!

- Privatnutzung E-Mail gestattet/geduldet?

→ E-Mails unterliegen **Fernmeldegeheimnis**!

- Verbindungsdaten sind personenbezogen:

→ E-Mails unterliegen **Datenschutz**!

Stand der Technik

Definition 9: Stand der Technik

Entwicklungsstand technischer Systeme, der zur vorsorgenden Abwehr spezifischer Gefahren geeignet und der verantwortlichen Stelle zumutbar ist

→ Maßgeblich für Stand der Technik: Gefahrenprävention!
→ Maßnahmen zum Stand der Technik müssen aber zumutbar sein
→ Verhältnismäßigkeitsprüfung inhärent
→ Internationale Standards gute Referenz für Stand der Technik
→ Aber: Kein Automatismus für gerichtsfeste Compliance!
→ Best Practice Standards genießen jedoch einen höheren Schutz hinsichtlich nötiger Sorgfaltspflicht als andere Standards

Compliance zu internationalen Standards

- **Umgang mit Informationen**
  → Informationssicherheitsmanagement (ISO/IEC 2700x)
  → Incident Management (ISO/IEC 27035)
  → IT Forensik (ISO/IEC 27037)
- **Disaster Recovery & Business Continuity Management**
  → Disaster Recovery Management (ISO/IEC 24762)
  → Business Continuity Management (BS 25999)
  → Preparedness & Continuity Management (ISO/DIS 22301)
  → Incident Preparedness & Operational Continuity (ISO/PAS 22399)
  → ICT Readiness for Business Continuity (ISO/IEC 27031)
- **Steuerung der IT**
  → Corporate Governance of IT (ISO/IEC 38500)
  → Governance of Information Security (ISO/IEC 27014)
- **Betrieb von IT-Services**
  → IT-Service-Management (ITIL bzw. ISO/IEC 20000-x)
  → Integriertes Management zu Informationssicherheit & IT-Services (ISO/IEC 27013)
  → Outsourcing finanzwirksamer IT-Services (SAS 70 → ISA 402)
  → Information Security for Supplier Relationships (ISO/IEC 27036-x)
- **Betrieb von Netzwerken**
  → Netzwerksicherheit (ISO 7492-2, ISO/IEC 27033-x)
- **plus zahlreiche Standards zur Systemsicherheit**

Zur ISMS-Standardisierung

„Grundschutz“ (1995):

- bis 2005 „IT-Grundschutzhandbuch“, seither „IT-Grundschutz-Kataloge“; plus 4 Standards zur Compliance mit ISO/IEC 27001
- Framework für Maßnahmen, die einen niedrigen bis mittleren Schaden abwenden (Grundschutz)
  Anm.: Framework = Angaben, wie etwas zu machen ist
- IT-Verbund → Bausteine → Maßnahmen mittlerer Schutzbedarf

„BS 7799“ (1995): Information Security Management System

- British Standard 7799
- seit 2000 (für BS 7799-1): ISO/IEC 17799 → ISO/IEC 27002
- seit 2005 (für BS 7799-2): ISO/IEC 27001 (zertifizierbarer Teil)
- BS 7799-3 keine ISO/IEC-Norm (stattdessen ISO/IEC 27005)
- Sektorspezifische Ergänzungen: 27011 (TK), 27799 (GW), …

Informationssicherheit

Definition 10: Informationssicherheit

Schutz der Verfügbarkeit, Integrität und Vertraulichkeit (und ggf. weiterer Eigenschaften) von Informationen *(nach ISO/IEC 27002)*

→ Gewährleistung von **Schutzzielen**

→ betrifft alle Informationen eines Unternehmens
Geschäftsgeheimnisse + Datengeheimnis

→ Information ist ein hoher Vermögenswert

→ Verknüpfung mit IT-Risiko-Management zwingend

→ Informationssicherheit ist Aufgabe des Managements

Informationssicherheit regelt

- Informations-Sicherheits-Politik (information security policy)
- Organisation der Informationssicherheit
- Verantwortlichkeit für die und Klassifizierung der Vermögenswerte
- Sicherheit im Rahmen des Personalwesens
- Physische und umgebungsbezogene Sicherheit → Schutzzonen
- Netzwerksicherheit & Datensicherung
- Steuerung von Zutritt, Zugang & Zugriff
- Sicherung der Betriebsbereitschaft & Umgang mit Verwundbar-keiten
- Management von Störfällen & Angriffen
- Gewährleistung eines kontinuierlichen Geschäftsbetriebs
- Erfüllung der Verpflichtungen (aus rechtlichen und organisa-torischen Anforderungen, z.B. Datenschutz/Fernmelderecht)

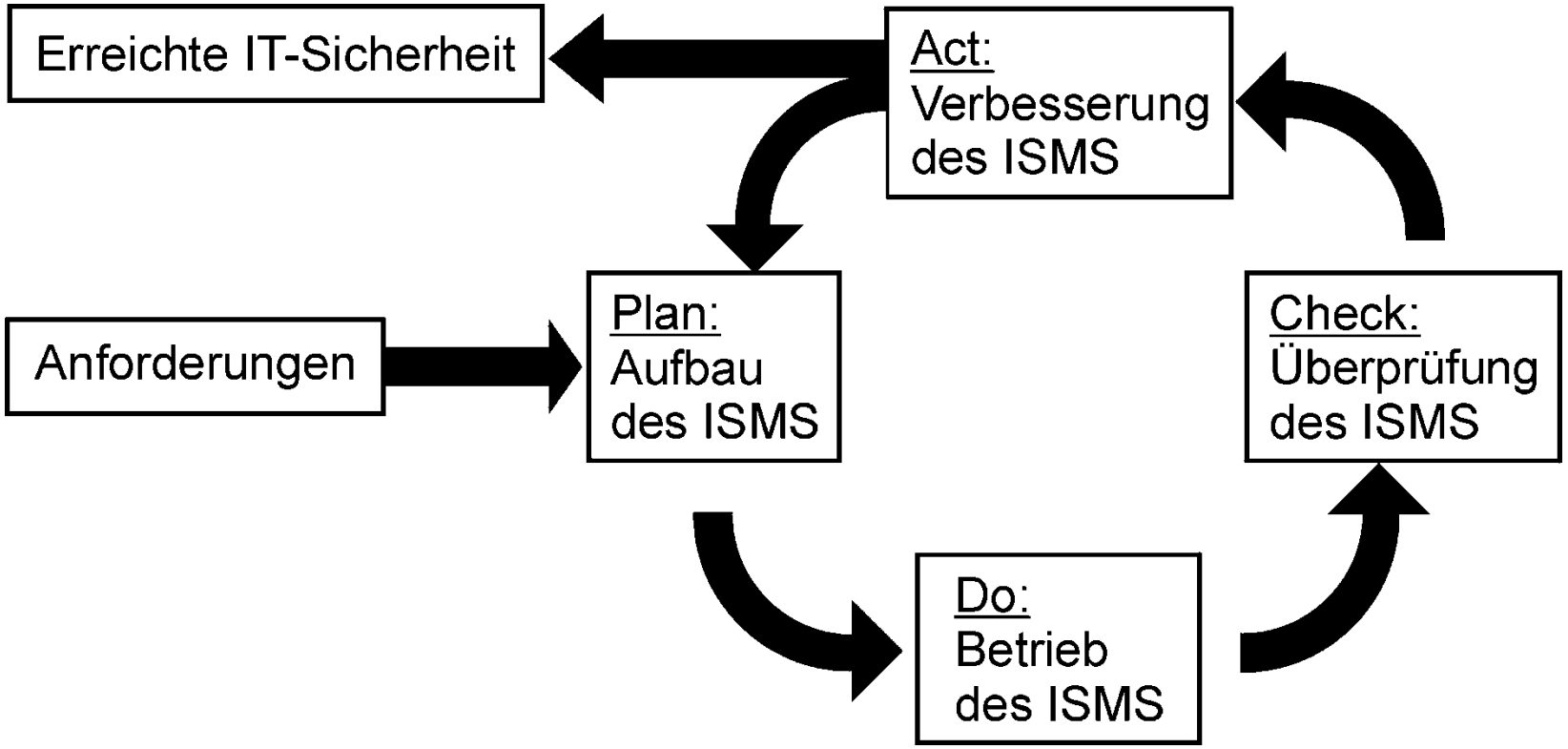
= Kontrollbereiche zur Informationssicherheit gemäß ISO/IEC 27002

ISMS-Leitlinie

Zu treffende Regelungen zum ISMS in der Leitlinie (nach ISO/IEC 27002):

- Festlegung der **Ziele** der umzusetzenden Informationssicherheit & deren **Bedeutung** für die Einrichtung (inkl. Aussage des Managements bzw. der Behördenleitung zur Priorisierung)
- **Geltungsbereich** der Leitlinie
- Beschreibung der **Anforderungen**
  - ° gesetzliche Vorgaben
  - ° anzuwendende Standards
  - ° zu beachtende Prinzipien
  - ° relevante Vorgaben durch vertragliche Vereinbarungen / SLAs
- Festlegung zentraler **Methoden**
  - ° IT Risk Assessment (zentral für die konkrete Planung der Maßnahmen!)
  - ° Business Impact Analysis (zentral zur Schutzbedarfsfeststellung!)
- Festlegung der **Verantwortlichkeiten**
- **Kommunikation**skonzept (inkl. zur Awareness)
- **Konsequenzen** für Nichtbeachtung der Vorgaben zur Informationssicherheit
- Auflistung des kompletten **Regelwerk**s zur Durchsetzung der Leitlinie (inkl. Konzepte, Verfahrensbeschreibungen, Dienstanweisungen, etc.), in denen die jeweiligen Einzelmaßnahmen zur Informationssicherheit festgelegt werden

Vorgehensmodell nach ISO/IEC 27001



ISMS = Informationssicherheitsmanagementsystem

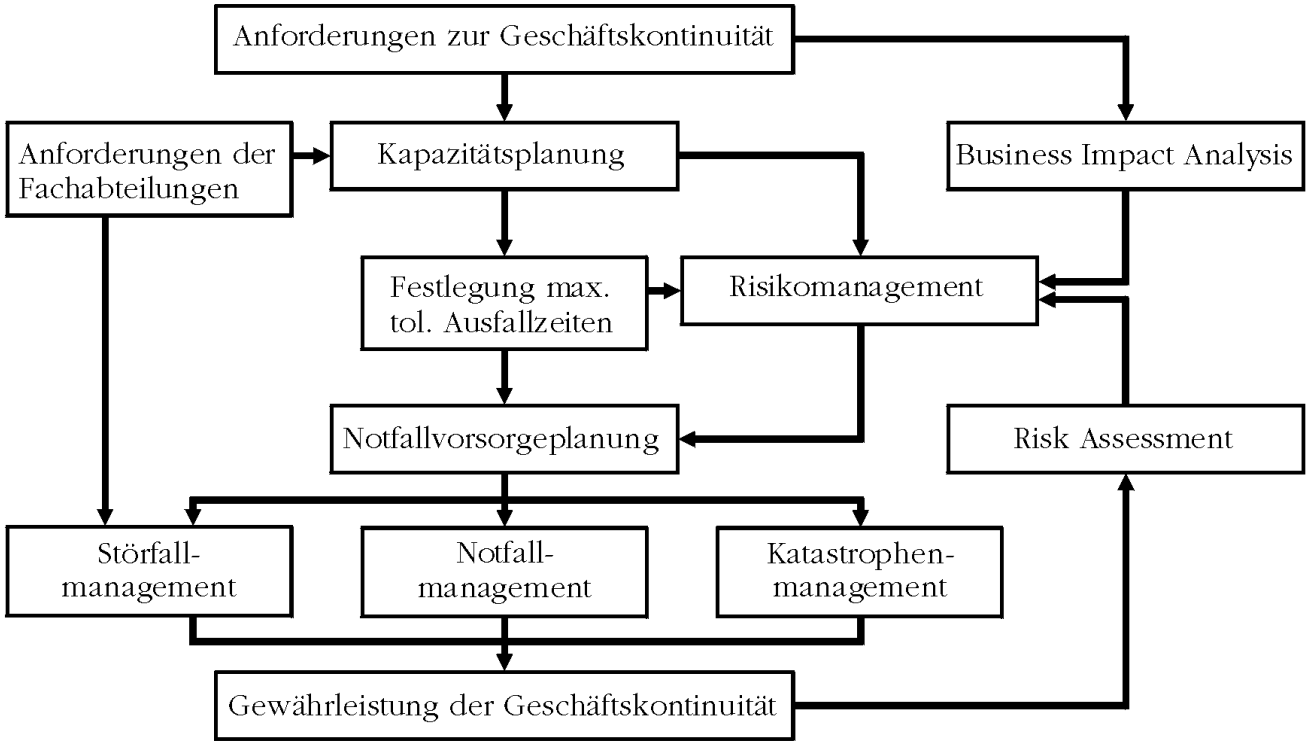
Hinweise zum PDCA-Modell

- Basiert auf sog. **Deming Cycle** (Qualitätsverbesserungszyklus nach W. Edwards Deming)
- In der **PLAN**-Phase werden die Vorgaben und Anforderungen bestimmt (inkl. Zielsetzung!) und die Übereinstimmung der vorgefundenen Einstellungen hinsichtlich dieser Rahmen überprüft (1. Risk Assessment)
- In der **DO**-Phase werden entsprechende technische und organisatorische Maßnahmen ergriffen, um die Vorgaben und Anforderungen zielgerichtet umzusetzen, und dabei insbesondere entsprechende Konfigurationen vorgenommen
- In der **CHECK**-Phase wird überprüft, inwiefern die getroffenen Maßnahmen dazu geeignet sind, die vorgegebenen Ziele zu erreichen (2. Risk Assessment – über Wirksamkeit der Controls)
- In der **ACT**-Phase werden im Sinne einer kontinuierlichen Verbesserung Konsequenzen aus der Überprüfung gezogen, der bestehende Status Quo neu bewertet und die Grundlage für den nächsten Durchlauf gelegt

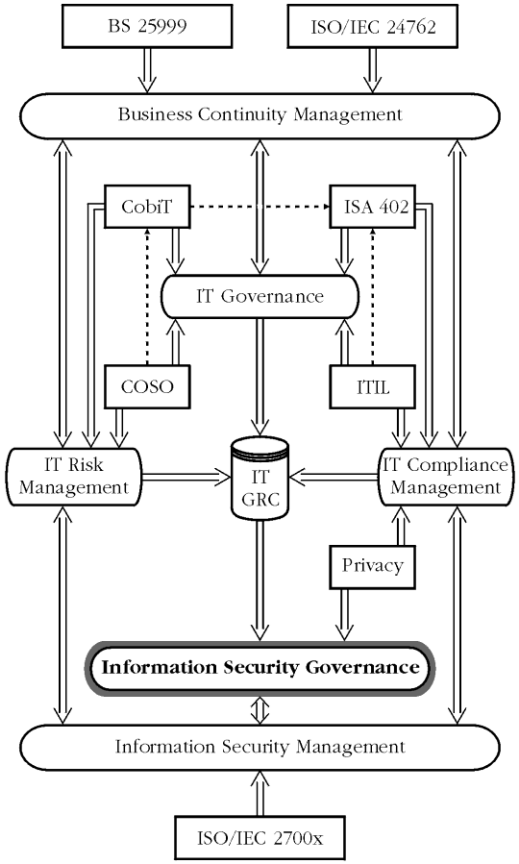
Business Continuity Management

- Grundlage: **BS 25999** (Teil 1: 2006; Teil 2: 2007)
- **Gewährleistung der Geschäftskontinuität** mithilfe
  - **Business Impact Analysis** (BIA) → Identifikation kritischer und für den Fortbestand bedrohlicher Prozesse der gesamten Wertschöpfungskette (inkl. Stakeholder!) → Priorisierung für Wiederanlauf
    Maximum Tolerable Period of Disruption (MTPD) = maximal tolerierbare Ausfallzeit (für jeden Prozess und jede Ressource!)
    Recovery Time Objective (RTO) = Dauer f. Wiederanlauf kritischer IT
    Recovery Point Objective (RPO) = maximal zulässiger Datenverlust
  - **Business Continuity Plan** → Dokumentation der Vorgehensweisen beim Eintreten eines bedrohlichen Notfalls (= Notfallkonzept)
    *Hinweis: **Notfall** = außergewöhnliche Abweichung vom Normalbetrieb (→ zu unterscheiden von Störfällen, die im Rahmen des laufenden Betriebs beherrschbar sind, und Katastrophen, die sich großflächig auswirken und i.d.R. staatlich reglementiert werden)*
  - Durchführung von **Notfallübungen** anhand stimmiger Szenarien

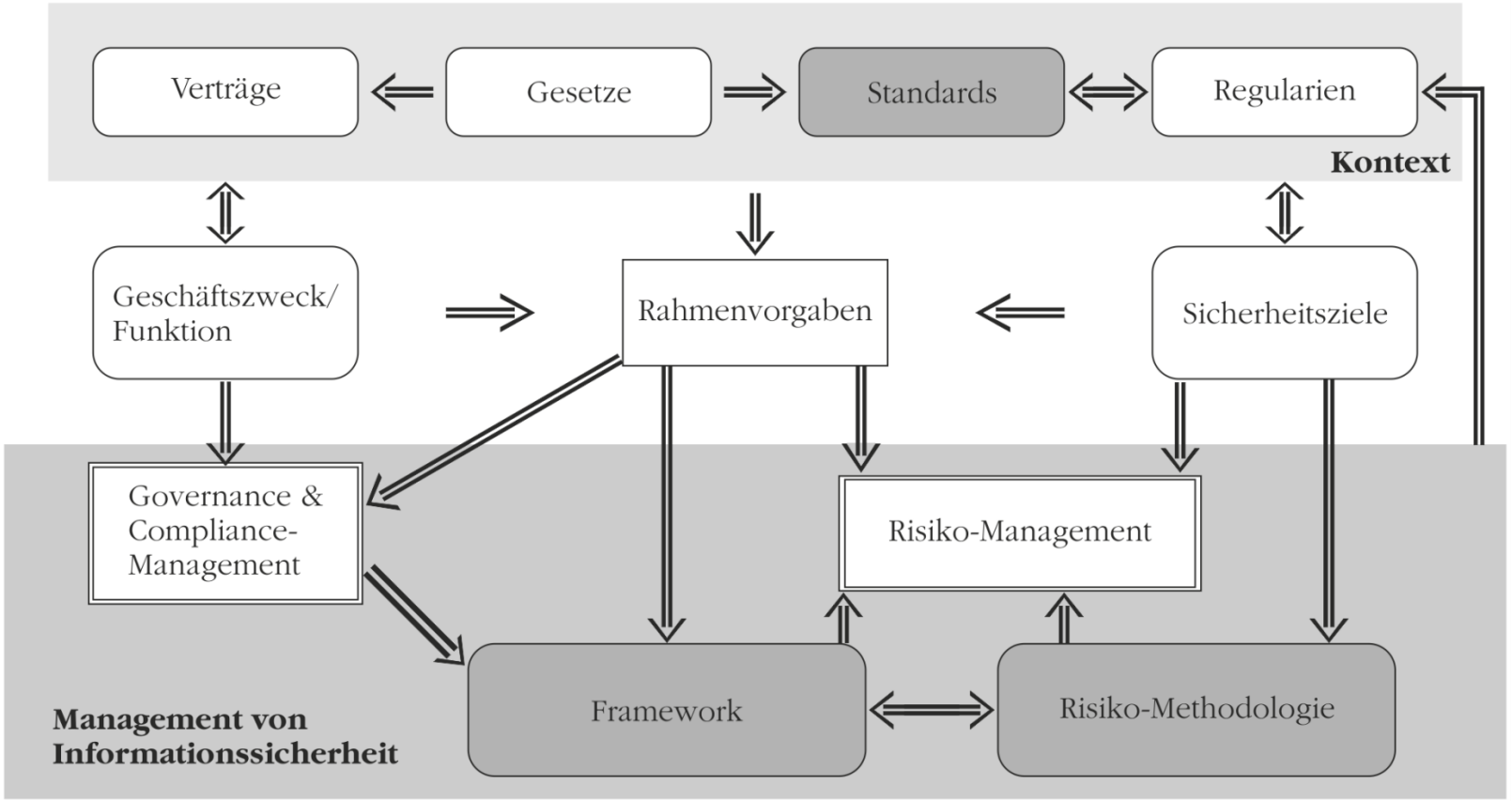
Absicherung der Geschäftskontinuität



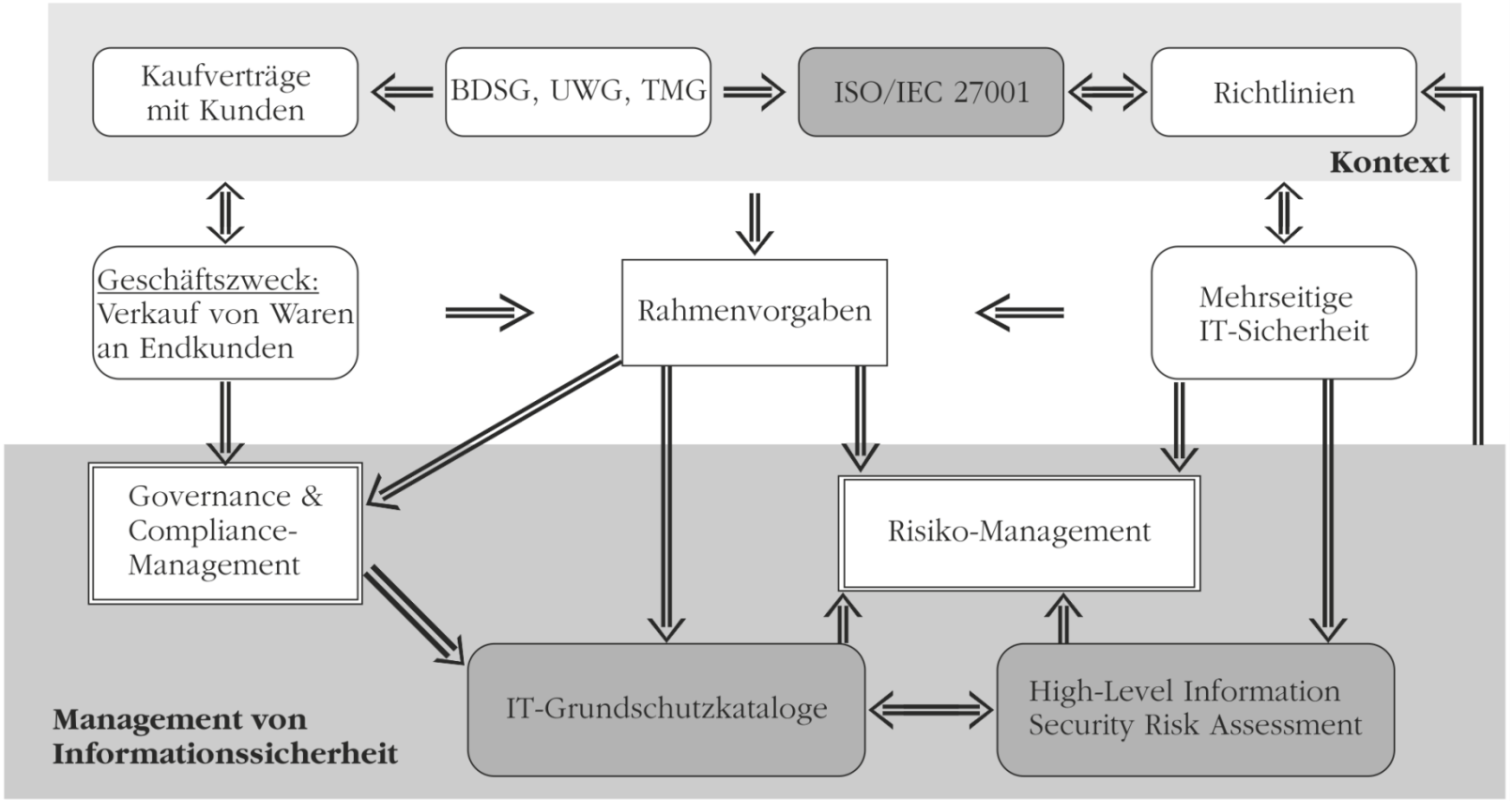
Zusammenspiel der Standards: Information Security Governance



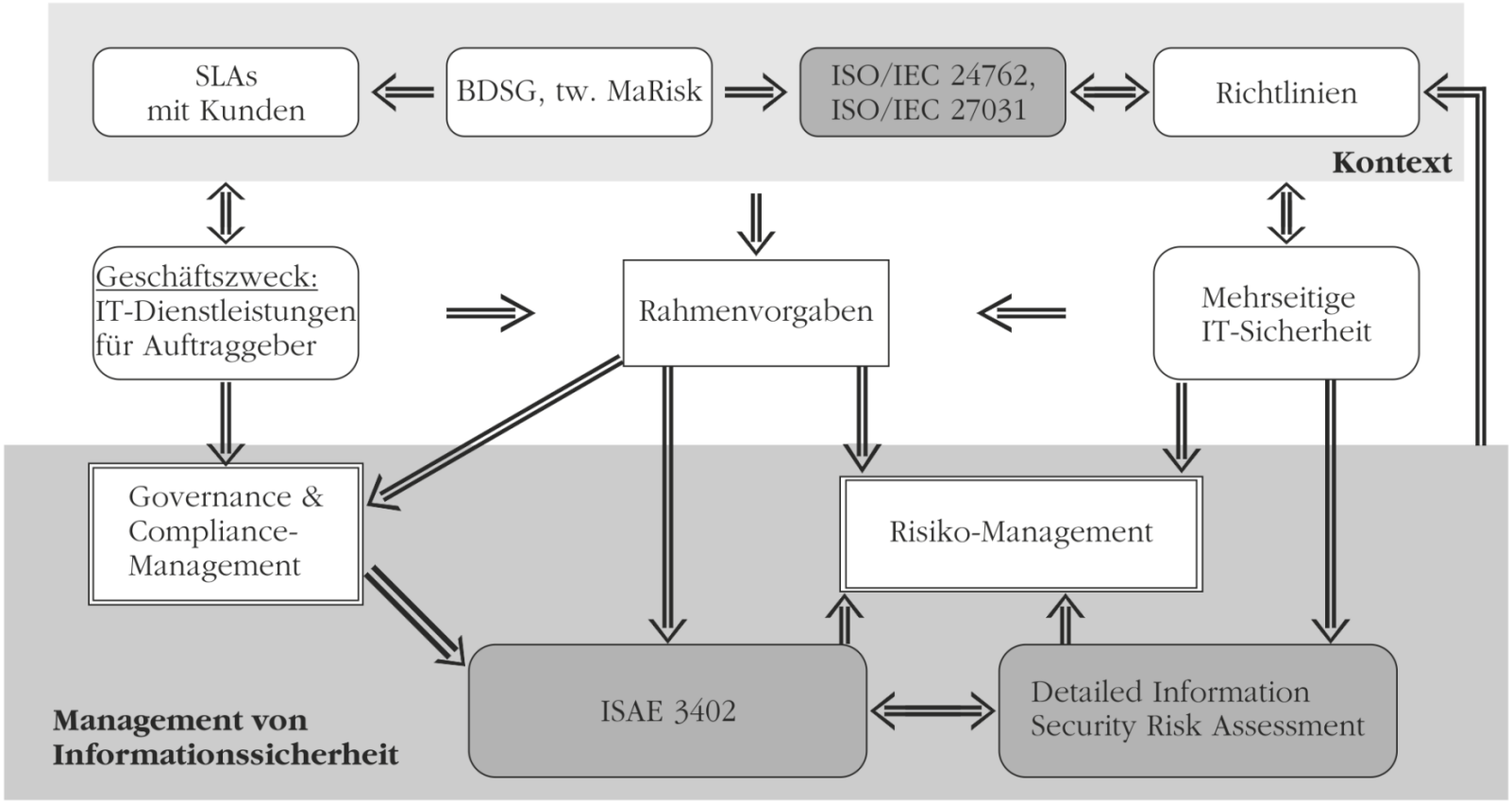
Zusammenhang für ISMS



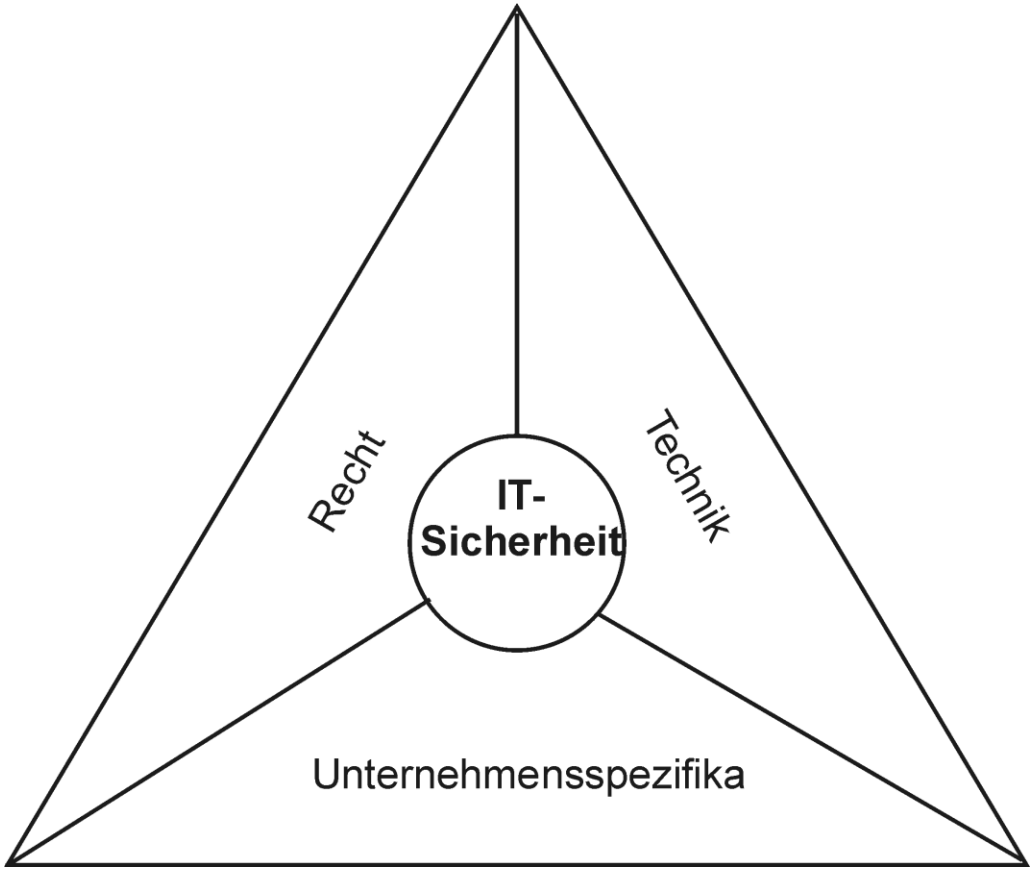
Beispiel-ISMS: Kundendatenschutz



Beispiel-ISMS: IT-Outsourcing



Einflussfaktoren der IT-Sicherheit



Einflussfaktor Recht (1)

Sorgfaltspflicht:

- KonTraG (§ 91 II AktG, § 43 I GmbHG) → Überwachungssystem zur Erkennung fortbestands-gefährdender Entwicklungen
- Haftungsrecht (§ 276 BGB, § 100 UrhG)
- Betriebs- und Geschäftsgeheimnisse (§ 17 UWG)
- Buchführungspflichten (§§ 238 I & 257 HGB, §§ 145-147 AO)
- Schutz vor Angriffen (§§ 202a, 202c, 268, 269, 303b & 305a StGB)

Straftaten mit Computerbezug

§ 201 StGB: Verletzung der Vertraulichkeit des Wortes
§ 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
§ 202a StGB: Ausspähen von Daten
§ 202b StGB: Abfangen von Daten
§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten
§ 203 StGB: Verletzung von Privatgeheimnissen
§ 206 StGB: Verletzung des Post- oder Fernmeldegeheimnisses
§ 263a StGB: Computerbetrug
§ 268 StGB: Fälschung technischer Aufzeichnungen
§ 269 StGB: Fälschung beweiserheblicher Aufzeichnungen
§ 270 StGB: Täuschung im Rechtsverkehr bei Datenverarbeitung
§ 271 StGB: Mittelbare Falschbeurkundung
§ 274 StGB: Urkundenunterdrückung
§ 303a StGB: Datenveränderung
§ 303b StGB: Computersabotage
§ 305a StGB: Zerstörung wichtiger Arbeitsmittel
§ 317 StGB: Störung von Telekommunikationsanlagen

Umgang mit § 202c StGB

§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Folgen für die Administration der IT-Sicherheit:

- Die Einstufung als Straftat setzt Vorsatz voraus. Insofern steht die Tätigkeit der IT-Administration mit dem Ziel der Gewährleistung der IT-Sicherheit keineswegs unter Strafe. Allerdings ist es hierzu zweckmäßig, die Methoden der Angreifer und damit insbesondere die Wirkungsweise der sog. „Hackertools“ zu kennen.
- Der IT-Administration kann daher angeraten werden, sich sowohl die „Beschaffung“ als auch den Einsatz von „Hackertools“ durch die Geschäftsleitung genehmigen zu lassen, so dass deren Einsatz nicht unbefugt erfolgt.
- Entsprechende „Hackertools“ sind gegen unbefugten Zugriff zu schützen.
- Über den durchgeführten Einsatz ist ein Protokoll zu erstellen, das ebenfalls gegen unbefugten Zugriff abzusichern ist.

Einflussfaktor Recht (2)

Datenschutz:

- grundlegend: §§ 3a, 4, 9 (samt Anlage), 28, 31 und 42a BDSG
- Haftungsrecht (§§ 7, 43 & 44 BDSG)

Fernmeldegeheimnis:

- §§ 88, 93, 100, 107, 109 & 109a TKG
- §§ 13 & 15a TMG
- §§ 206 & 303a StGB

Einflussfaktor Recht (3)

sowie spezialrechtliche Vorgaben:

- insbesondere für Banken, Gesundheitswesen, Sozialwesen, Arbeitsrecht und international tätige Unternehmen (z.B. Sarbanes-Oxley-Act)

und vertragsrechtliche Verpflichtungen:

- New Basel Capital Accord (Basel II → Basel III)
  → Verbilligung der Fremdkapitalfinanzierung für Unternehmen mit gutem Rating
  → Berücksichtigung operationaler Risiken & Nachweis der Verlässlichkeit + Stabilität des DV-Systems
  → in EU-Recht (EU-RL 2006/48+49/EG) integriert

Haftung IT-Verantwortlicher (1)

- **Schlechterfüllung** arbeitsvertraglicher Pflichten berechtigt zum Schadensersatz (§ 280 I BGB i.V.m. § 611 I BGB)
- Nachweis für Schlechterfüllung obliegt Arbeitgeber (§ 619a BGB)
- Haftung nach **Verschuldensgrad** gestaffelt (§ 276 BGB i.V.m. § 254 BGB):
  ° Vorsatz → voll
  ° grobe Fahrlässigkeit → voll, sofern verhältnismäßig
  ° „mittlere“ Fahrlässigkeit → anteilig
  ° (leichte) Fahrlässigkeit → nicht
  (Grundlage: diverse BAG-Urteile)
- Schadensersatz bei betrieblich veranlassten Tätigkeiten auch abhängig vom Betriebsrisiko („**gefahrgeneigte Arbeit**“)

Haftung IT-Verantwortlicher (2)

- Verletzung des Fernmeldegeheimnisses strafbewährt (§ 206 StGB)
- Urkundenunterdrückung durch Vernichtung, Beschädigung oder Zurückhaltung von (elektronischen) Buchführungsunterlagen strafbar (§ 274 StGB)
- Dritter hat Recht auf Schadensersatz (§ 823 BGB) und Unterlassung (§ 1004 BGB)
- Betroffener kann bei Datenschutzverstoß wider der Sorgfaltspflicht Recht auf Schadensersatz geltend machen (§ 7 BDSG)
  → Beweislast trägt die verantwortliche Stelle!
- Verletzung des Datengeheimnisses bzw. Fernmeldegeheimnisses berechtigt (je nach Schwere des Vergehens) zur fristlosen Kündigung (ArbG-Urteile)
- Unbefugte Offenbarung personenbezogener Daten kann bis zu 300.000 € kosten (§ 43 II & III BDSG)
- Strafrechtliche Folgen nur bei Vorteilsnahme oder bewusster Schädigung (§ 44 BDSG)

Einflussfaktor Technik (1)

Informationen als besonderer „Rohstoff“:

- Information ist immateriell
- Wert von Informationen mal exponentiell, mal subtrahierend
- Informationen sind manipulierbar
- Informationen auch unbewusst oder ungewünscht übertragbar
- Zugang zu und Bewertung von Informationen entscheidend

→ neue Maßstäbe! (auch für rechtliche Regelungen!)

Einflussfaktor Technik (2)

Fortentwicklung der Informationstechnik:

- schnelle Fortentwicklung von IT-Systemen (Verdoppelung der Datenspeicherkapazitäten & Arbeitsgeschwindigkeit alle 2 Jahre)
- hohe Komplexität vernetzter IT-Systeme
- stark anwachsender Sektor Informationswirtschaft
- hohe Abhängigkeit von IT-Systemen & Informationen
- Allgegenwart der Datenverarbeitung (Notebooks, Smartphones, IT in vielen technischen Systemen, …)
- Ambivalenz technischer Entwicklungen („dual use“)

→ technisches Grundverständnis nötig

Einflussfaktor Unternehmensspezifika (1)

Branchenzugehörigkeit & Marktstellung

- branchenspezifische Anforderungen (insb. für Banken, Versicherungen, Pharmaunternehmen, Automobilindustrie → Stichwort: „Nachweis guter Praxis“)
- marktbeherrschende Stellung
- internationale Ausrichtung (vor allem hinsichtlich SOX)
- Vorteile durch bzw. Forderung nach Zertifizierungen
- Abwehr von Wirtschaftsspionage
  lt. KPMG-Studie: Verletzung Betriebs- und Geschäftsgeheimnis von 22 % (2003) auf 31 % (2006) gestiegen, inzwischen wieder auf 24 % (2010) zurückgegangen; Bereich IT wird in 36 % (2010) angegriffen (plus 9-%-Punkte gegenüber 2006)

Einflussfaktor Unternehmensspezifika (2)

Innerbetriebliche Organisation

- Stellenwert der IT-Administration
- Bestellung eines Datenschutzbeauftragten
- Einsetzung eines IT-Sicherheitsbeauftragten (CIO, CISO etc.)
- Aktivität der internen Revision (in Kenntnis von IT-Spezifika)
- Bewusstsein (Awareness) hinsichtlich IT-Sicherheit
- Erfahrung aus zurückliegenden Sicherheitsvorfällen / Datenpannen
- Zufriedenheit der Mitarbeiter