

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

Vorlesung im Sommersemester 2009
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
✓	Schwerpunktthema zur Vertiefung		Konzeption von IT-Sicherheit

Anforderungen zur IT-Sicherheit:

- Compliance
- Einflussfaktor Recht
- Einflussfaktor Technik
- Internationale Standards
- Einflussfaktor Unternehmensspezifika

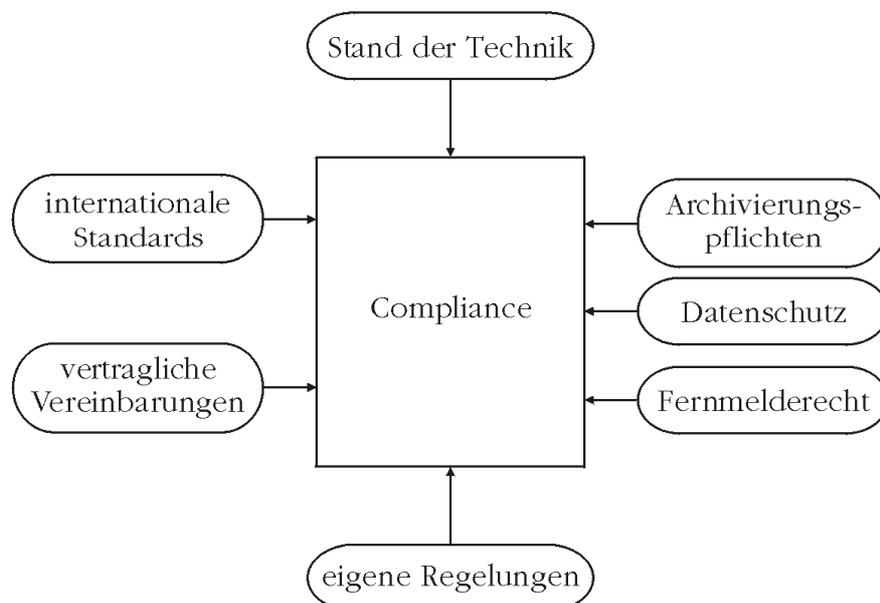
Compliance (1)

Definition 8: Compliance

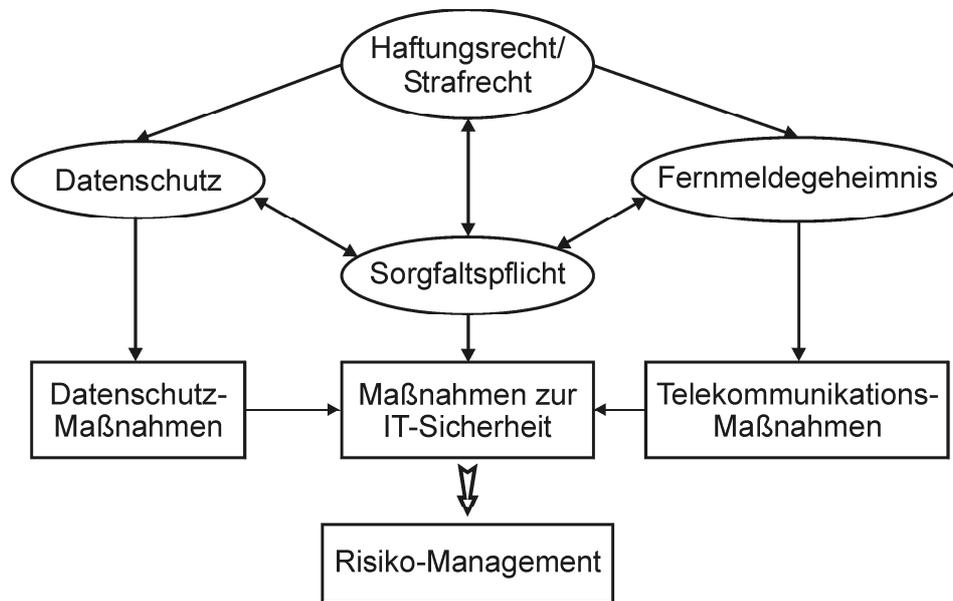
Übereinstimmung mit festgelegten Regeln

- Rechtliche Regeln
- Best practice Regeln (internationaler) Standards
- Regeln aufgrund von Verträgen mit Kunden
- Interne Regeln (Richtlinien, Policies, Dienstanweisungen)

Compliance (2)



Compliance zu Sicherheitsrecht

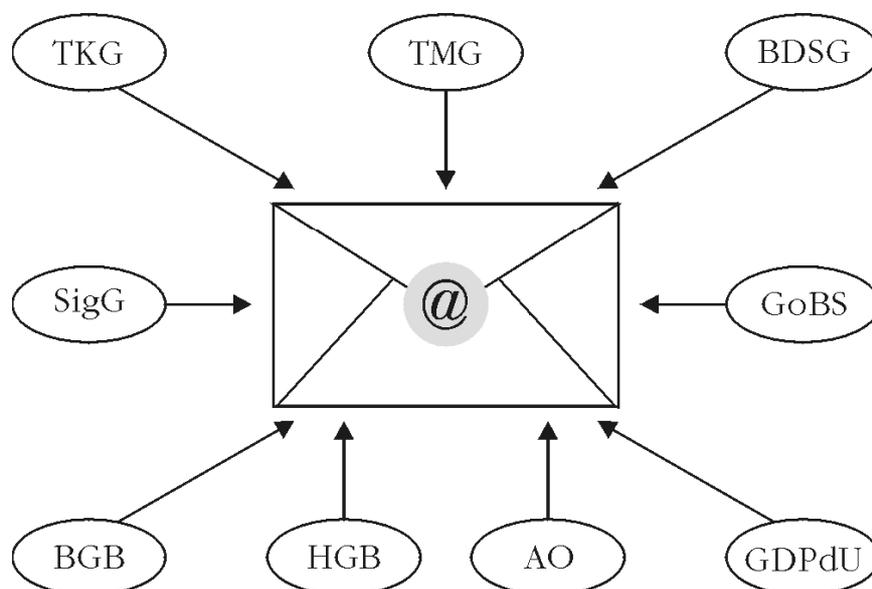


Bernhard C. Witt

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

5

Beispiel: E-Mail-Compliance (1)



Bernhard C. Witt

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

6

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

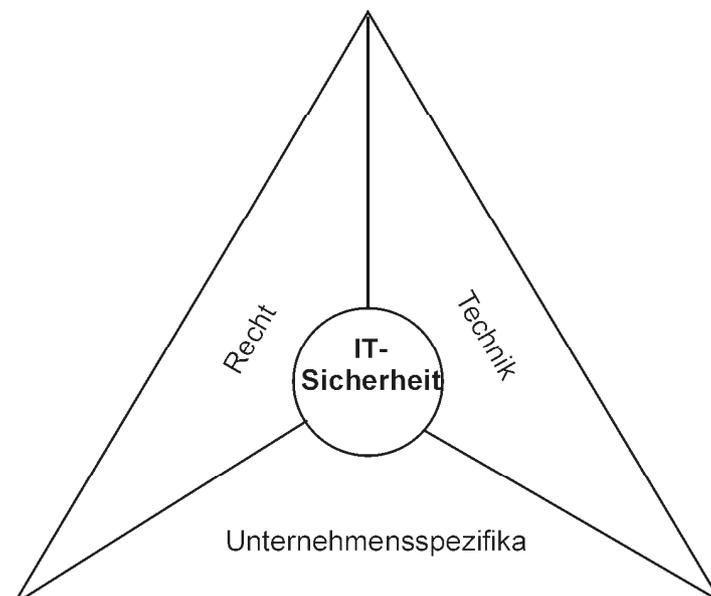
Beispiel E-Mail-Compliance (3)

- 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!**

Compliance zu internationalen Standards

- **Umgang mit Informationen**
 - Informationssicherheitsmanagement (ISO/IEC 2700x)
 - Incident Management (ISO/IEC TR 18044)
 - **Betrieb von IT-Services**
 - IT-Service-Management (ITIL bzw. ISO/IEC 20000)
 - Outsourcing finanzwirksamer IT-Services (SAS 70)
 - **Betrieb von Netzwerken**
 - Netzwerksicherheit (ISO 7492-2, ISO/IEC 18028)
 - **Disaster Recovery & Business Continuity Management**
 - Disaster Recovery Management (ISO/IEC 24762)
 - Business Continuity Management (BS 25999)
 - Incident Preparedness & Operational Continuity (ISO/PAS 22399)
 - **Steuerung der IT**
 - Corporate Governance of IT (ISO/IEC 38500)
- Maßgeblich für „Stand der Technik“!

Einflussfaktoren der IT-Sicherheit



Einflussfaktor Recht (1)

Sorgfaltspflicht:

- KonTraG (§ 91 II AktG, § 43 I GmbHG) → Überwachungssystem zur Erkennung fortbestandsgefährdender Entwicklungen
- Haftungsrecht (§ 276 BGB, § 100 UrhG)
- Betriebs- und Geschäftsgeheimnisse (§ 17 UWG)
- Buchführungspflichten (§§ 238 I & 257 HGB, §§ 145-147 AO)
- Schutz vor Angriffen (§§ 202a, 268, 269, 270, 303b & 305a StGB)

Einflussfaktor Recht (2)

Datenschutz:

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

Fernmeldegeheimnis:

- §§ 88, 100, 107 & 109 TKG
- § 13 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)
 - Verbilligung der Fremdkapitalfinanzierung für Unternehmen mit gutem Rating
 - Berücksichtigung operationaler Risiken & Nachweis der Verlässlichkeit und Stabilität des DV-Systems

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 („**gefahreneneigte 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 250.000 € 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 der IT-Systeme
 - stark anwachsender Sektor Informationswirtschaft
 - hohe Abhängigkeit von IT-Systemen & Informationen
 - Allgegenwart der Datenverarbeitung
 - Ambivalenz technischer Entwicklungen
- technisches Grundverständnis nötig

Einflussfaktor Technik (3)

Kenndaten aus den <kes>-Sicherheitsstudien:

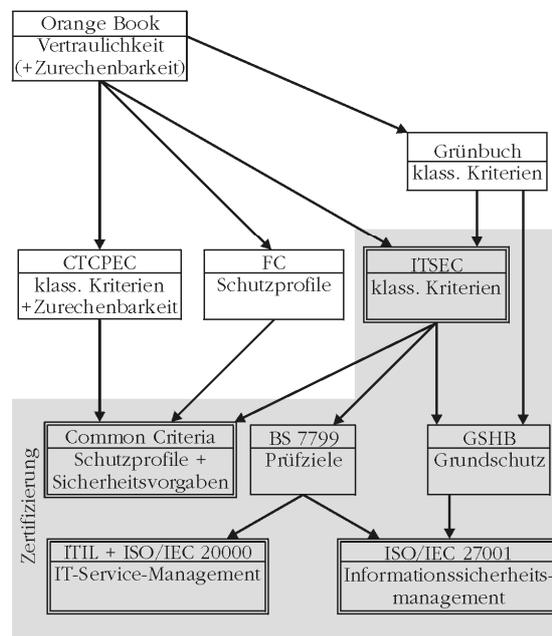
- Verhältnis von eingesetzter IT pro Mitarbeiter anwachsend:
1990: 0,06 → 1996: 0,23 → 2002: 0,63 → 2008: 0,98
- Telearbeit (Home Office) stark anwachsend:
2004: 0,01 → 2006: 0,07 → 2008: 0,25

Definition 9: Stand der Technik

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

→ Internationale Standards gute Referenz für Stand der Technik

Entwicklung relevanter Standards



Bernhard C. Witt

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

19

Hinweise zu den Standards (1)

„Orange Book“ (1983):

- Trusted Computer System Evaluation Criteria

„Grünbuch“ (1989):

- Kriterien für die Bewertung der Sicherheit von Systemen der IT

„ITSEC“ (1990):

- Information Technology Security Evaluation Criteria

„Grundschatz“ (1995):

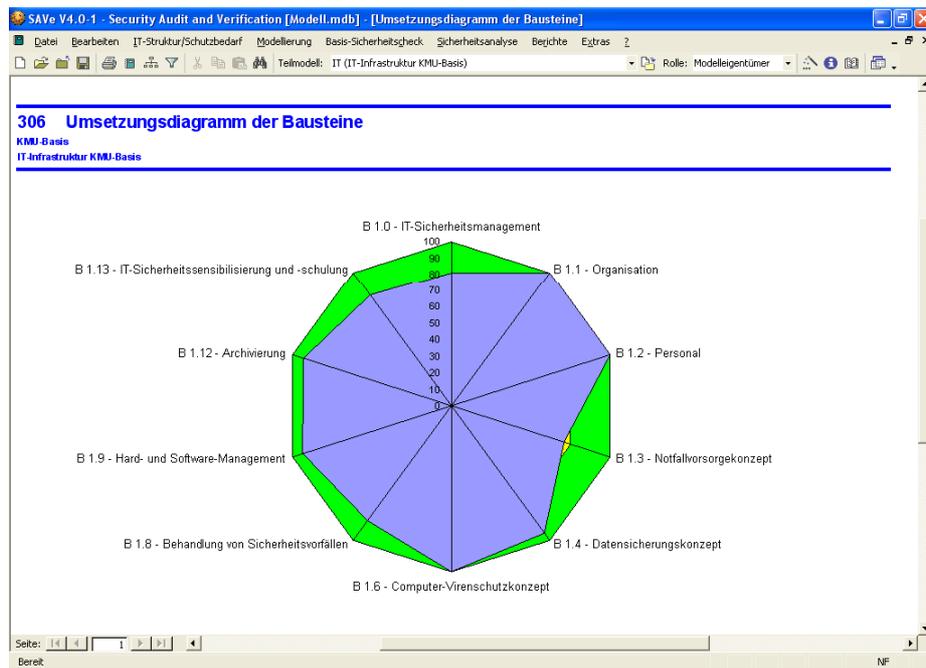
- bis 2005 „IT-Grundschatzhandbuch“, seither „IT-Grundschatz-Kataloge“
- prüft nur Maßnahmen, die einen niedrigen bis mittleren Schaden abwenden (Grundschatz)
- Für Mindestschutz lassen sich sog. „Pflichtbausteine“ ermitteln

Bernhard C. Witt

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

20

Umsetzung der Pflichtbausteine



Bernhard C. Witt

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

21

Hinweise zu den Standards (2)

„Common Criteria“ (1996):

- Common Criteria for Information Technology Security Evaluation
- = ISO/IEC 15408
- verwendete Schutzprofile werden nach ISO/IEC 15446 erstellt

„BS 7799“ (1995):

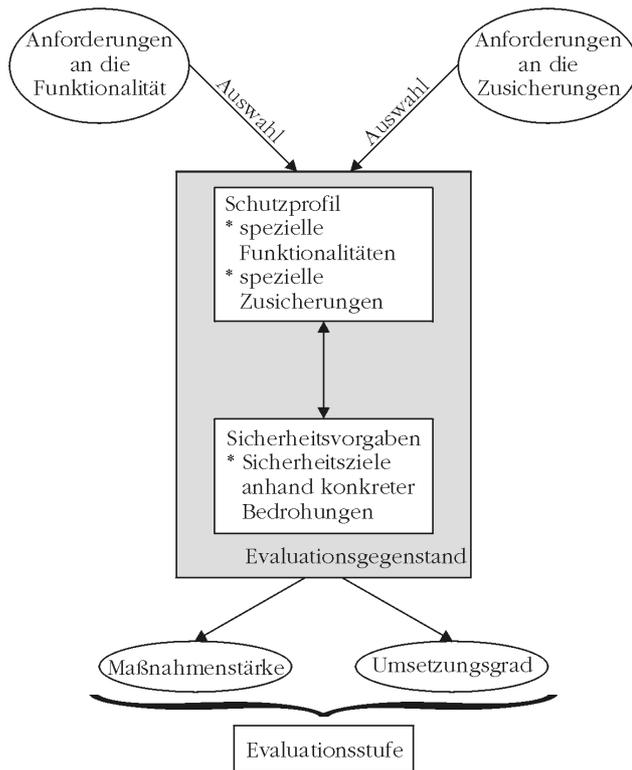
- Information Security Management System
- British Standard 7799
- seit 2000 (für BS 7799-1): ISO/IEC 17799 → ISO/IEC 27002
- seit 2005 (für BS 7799-2): ISO/IEC 27001 (zertifizierbarer Teil)
- BS 7799-3 nicht als ISO/IEC-Norm umgesetzt

Bernhard C. Witt

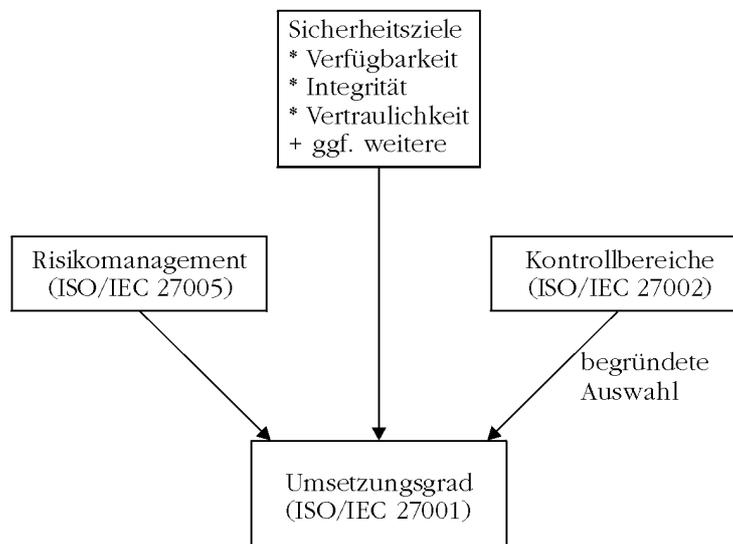
Grundlagen des Datenschutzes
und der IT-Sicherheit (Teil 2a)

22

Struktur der Common Criteria



Struktur zum Information Security Management



Informationssicherheit

Definition 10: Informationssicherheit

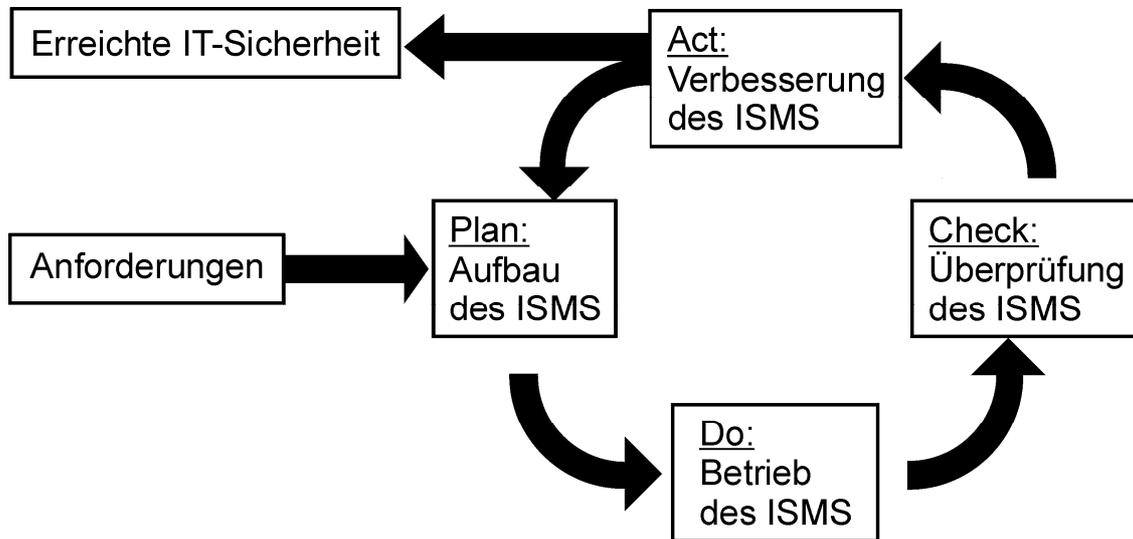
Schutz der Verfügbarkeit, Integrität und Vertraulichkeit
(und ggf. weiterer Eigenschaften) von Informationen
(nach ISO/IEC 27002)

- Gewährleistung von Schutzzielen
- betrifft alle Informationen eines Unternehmens
- Information ist ein hoher Vermögenswert
- Verknüpfung mit IT-Risiko-Management
- Informationssicherheit ist Aufgabe des Managements

Informationssicherheit regelt

- Informations-Sicherheits-Politik (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 Verwundbarkeiten
- Management von Störfällen & Angriffen
- Gewährleistung eines kontinuierlichen Geschäftsbetriebs
- Erfüllung der Verpflichtungen (aus rechtlichen und organisatorischen Anforderungen, z.B. Datenschutz/Fernmelderecht)

Vorgehensmodell nach ISO/IEC 27001



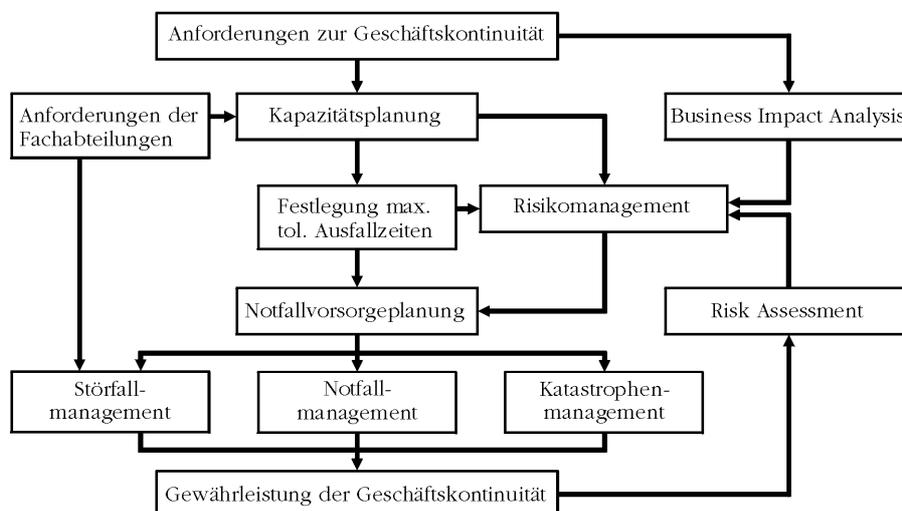
Hinweise zum PDCA-Modell

- 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



Alternative Vorsorgestrategien

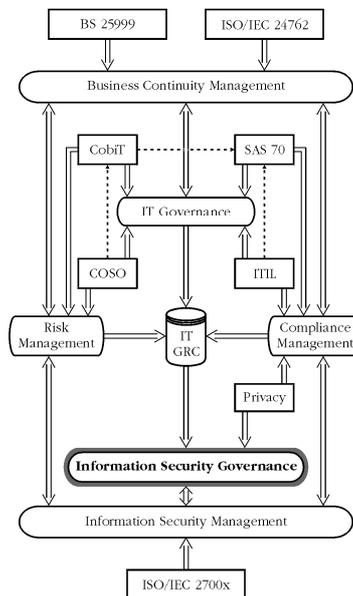
Wiederanlauf-Maßnahmen	1998	2000	2002	2004	2006	2008
Cluster (mit Überkapazitäten)	9%	14%	46%	38%	36%	49%
laufende Systeme („hot“)	16%	17%	40%	34%	31%	34%
Räume m. wicht. HW („warm“)	20%	19%	43%	28%	37%	30%
leere Räume („cold“)	12%	15%	36%	29%	25%	17%
Räume f. Pers. mit Infrastrukt.	-----	9%	25%	17%	18%	16%
Räume f. Pers. oh. Infrastrukt.	-----	7%	13%	9%	9%	11%
konfigurationsidentische Netze	13%	11%	25%	19%	22%	15%
Nutzungsvertrag v. Ressourcen	17%	15%	30%	25%	20%	16%
Nutzungsvertrag v. Containern	5%	6%	7%	8%	12%	11%
Vertrag schnelle HW-Ersatzlief.	25%	31%	44%	41%	37%	38%
Abschluss von Versicherungen	31%	41%	61%	44%	41%	46%

Quelle: <kes>-Sicherheitsstudien

Weitere internationale Standards

- **FIPS 140-1/2** (1994)
= ISO/IEC 19790
- **ITIL** (1995)
Information Technology Infrastructure Library
→ prozess-, service- & kunden-orientierte IT-Organisation
→ zertifizierbar via ISO/IEC 20000
- **CobIT** (1996)
Control Objectives for Information and related Technology
→ IT-Governance (auf Geschäftszweck hin ausgerichtete Steuerung der eingesetzten Informationstechnik)
- **ISO TR 13335** (1996)
→ Technische Reports zum IT-Sicherheitsmanagement
→ seit 2004 (für ISO TR 13335-1 & 13335-2): ISO/IEC 13335-1
→ seit 2008 (für ISO TR 13335-3 & 13335-4): ISO/IEC 27005

Zusammenspiel der Standards: Information Security Governance



Bernhard C. Witt

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

33

Einflussfaktor Unternehmensspezifika (1)

Branchenzugehörigkeit & Marktstellung

- branchenspezifische Anforderungen (insb. für Banken, Versicherungen, Pharmaunternehmen, Automobilindustrie → Nachweis guter Praxis)
- marktbeherrschende Stellung
- internationale Ausrichtung (vor allem hinsichtlich SOX)
- Vorteile durch bzw. Forderung nach Zertifizierungen
- Abwehr von Wirtschaftsspionage (KPMG-Studie: Verletzung Betriebs- und Geschäftsgeheimnis von 20 % (2003) auf 31 % (2006) gestiegen!)

Bernhard C. Witt

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

34

Einflussfaktor Unternehmensspezifika (2)

Innerbetriebliche Organisation

- Stellenwert der IT-Administration
- Bestellung eines Datenschutzbeauftragten
- Einsetzung eines IT-Sicherheitsbeauftragten (CIO, CISO etc.)
- Aktivität der internen Revision
- Bewusstsein hinsichtlich der IT-Sicherheit
- Erfahrung aus Sicherheitsvorfällen
- Zufriedenheit der Mitarbeiter

Einflussfaktor Unternehmensspezifika (3)

Besetze Funktion	1996	2000	2004	2006	2008
Datenschutzbeauftragter	75%	82%	70%	75%	78%
zentr. IT-Sicherheitsbeauftragter	32%	30%	58%	46%	49%
Revision f. Informationsverarb.	39%	41%	35%	33%	33%
Ausschuss f. Informationssicherh.	16%	16%	13%	13%	23%
dezentr.IT-Sicherheitsbeauftragter	18%	17%	12%	-----	-----
IT-Sicherheitsteam (CERT/CSIRT)	-----	-----	19%	21%	-----

Quelle: <kes>-Sicherheitsstudien