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

Vorlesung im Sommersemester 2019

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 7: Compliance**
Übereinstimmung mit festgelegten Regeln

Zu den festgelegten Regeln zählen:

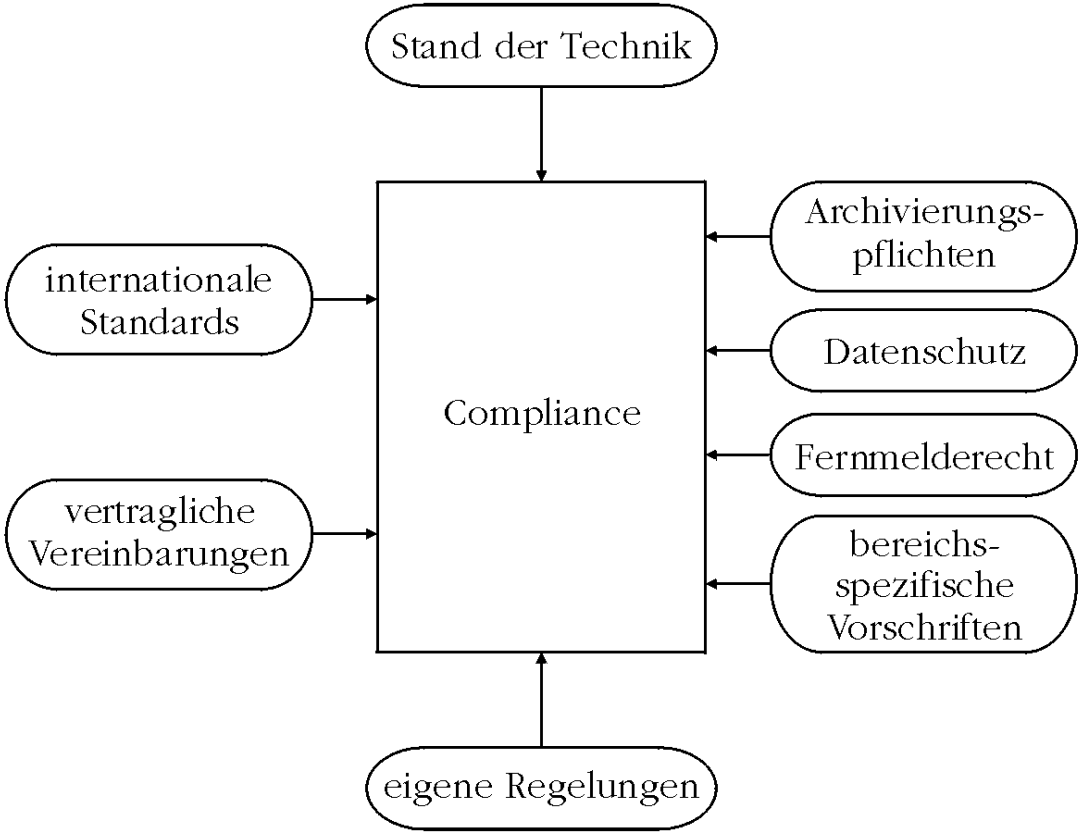
→ Rechtliche Regeln

→ Best practice Regeln (internationaler) Standards

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

→ Interne Regeln (Richtlinien, Policies, Dienstanweisungen)

# Compliance (2)



# Stand der Technik

**Definition 8: Stand der Technik**

Entwicklungsstand technischer Systeme, der zur vorsorgenden Abwehr spezifischer Gefahren geeignet & 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

Im Rahmen des **IT-Sicherheitsgesetzes** wird nach dessen Begründung unter „Stand der Technik“ verstanden der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.

# Compliance zu internationalen Standards

- **Umgang mit Informationen**
  → Informationssicherheitsmanagement (ISO/IEC 2700x)
  → Information Security Incident Management (ISO/IEC 27035-x)
  → IT Forensik (ISO/IEC 27037)
- **Business Continuity Management**
  → Business Continuity Management (ISO 22301)
  → Business Continuity Management Guidance (ISO 22313)
  → 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 (ISA 402, ISAE 3402 & SSAE 16)
  → 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**

# Informationssicherheit

**Definition 9: Informationssicherheit**

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Information (und ggf. weiterer Eigenschaften – nach ISO/IEC 27000)

→ Aufrechterhaltung von **Schutzzielen**

→ betrifft alle Informationen eines Unternehmens
**Geschäftsgeheimnisse + Datengeheimnis**

→ Information ist ein hoher Vermögenswert

→ Verknüpfung mit IT-Risiko-Management zwingend

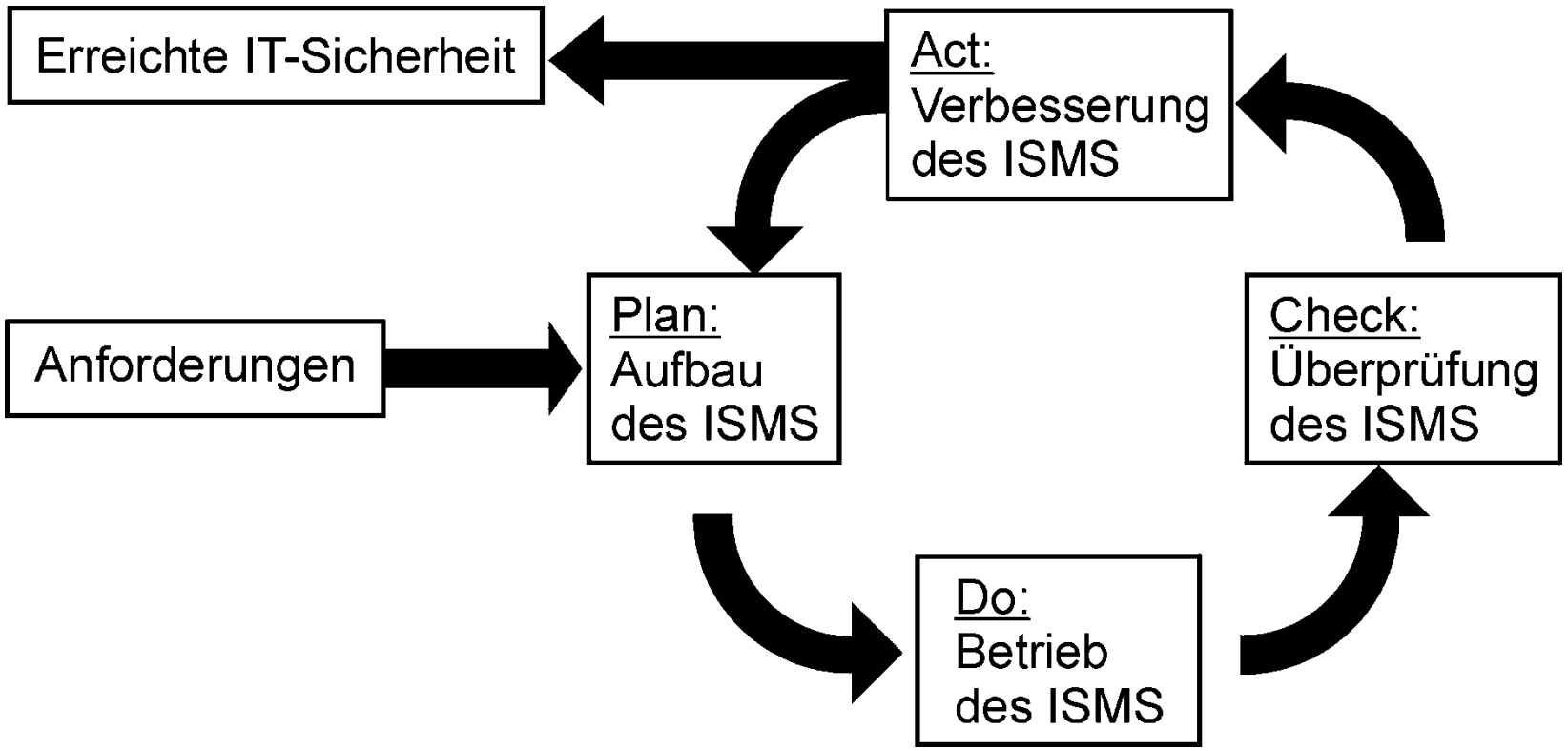
→ Informationssicherheit ist Aufgabe des Managements

# Informationssicherheit regelt

- Informations-Sicherheits-Politik (information security policy) und Vorgaben des Managements zur Informationssicherheit
- Organisation der Informationssicherheit
- Sicherheit im Rahmen des Personalwesens
- Verantwortlichkeit für die und Klassifizierung der Vermögenswerte
- Steuerung von Zutritt, Zugang & Zugriff
- Einhaltung kryptographischer Vorgaben
- Physische und umgebungsbezogene Sicherheit → Schutzzonen
- Sicherung der Betriebsbereitschaft & Umgang mit Verwundbarkeiten
- Kommunikationssicherheit → Netzwerksicherheit & sicherer Datentransfer
- Erwerb, Entwicklung und Wartung von IT-Systemen
- Informationssicherheit innerhalb der Lieferkette
- Management von Störfällen & Angriffen
- Gewährleistung eines kontinuierlichen Geschäftsbetriebs
- Erfüllung der Verpflichtungen (aus rechtlichen und organisatorischen Anforderungen, z.B. Datenschutz/Fernmelderecht/Copyright)

= Kontrollbereiche zur Informationssicherheit gemäß ISO/IEC 27002

# PDCA-Vorgehensmodell




ISMS = Informationssicherheitsmanagementsystem

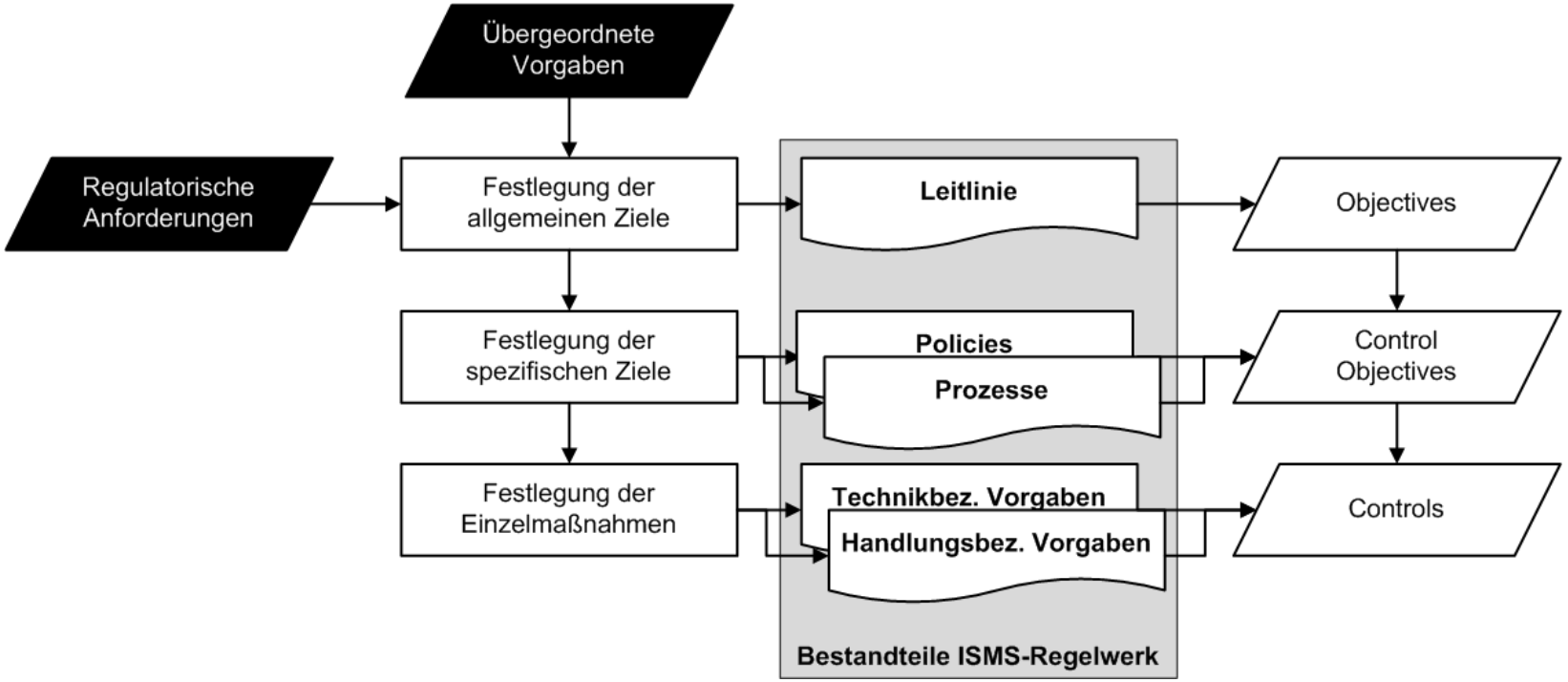
# Hinweise zum PDCA-Modell

- 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 – zur Festlegung geplanter Maßnahmen)
- 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

# Zum Managementsystem

- **Managementsystem** = Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Policies, Ziele (= zu erreichende Ergebnisse) und Prozesse zum Erreichen dieser Ziele festzulegen (nach ISO/IEC 27000) → mit Managementsystem wird Zielerreichung gesteuert
- Ziele und Umsetzungen können sich im Laufe der Zeit ändern
  → **Fortlaufende Verbesserung** nötig
- Ein **Informationssicherheitsmanagementsystem** (ISMS) umfasst:
  - Leitlinie zur Informationssicherheit (zur Festlegung übergeordneter Ziele des ISMS)
  - Verfahren (= Prozesse zur risikobasierten Steuerung und Aufrechterhaltung von Informationssicherheit)
  - Richtlinien (= verbindliche Vorgaben zur Erreichung von Informationssicherheitszielen im Detail)
  - und damit verbundene Ressourcen und Tätigkeiten,
  - die jeweils von der Organisation gesteuert werden, um ihre Informationswerte (Primary Assets) zu schützen

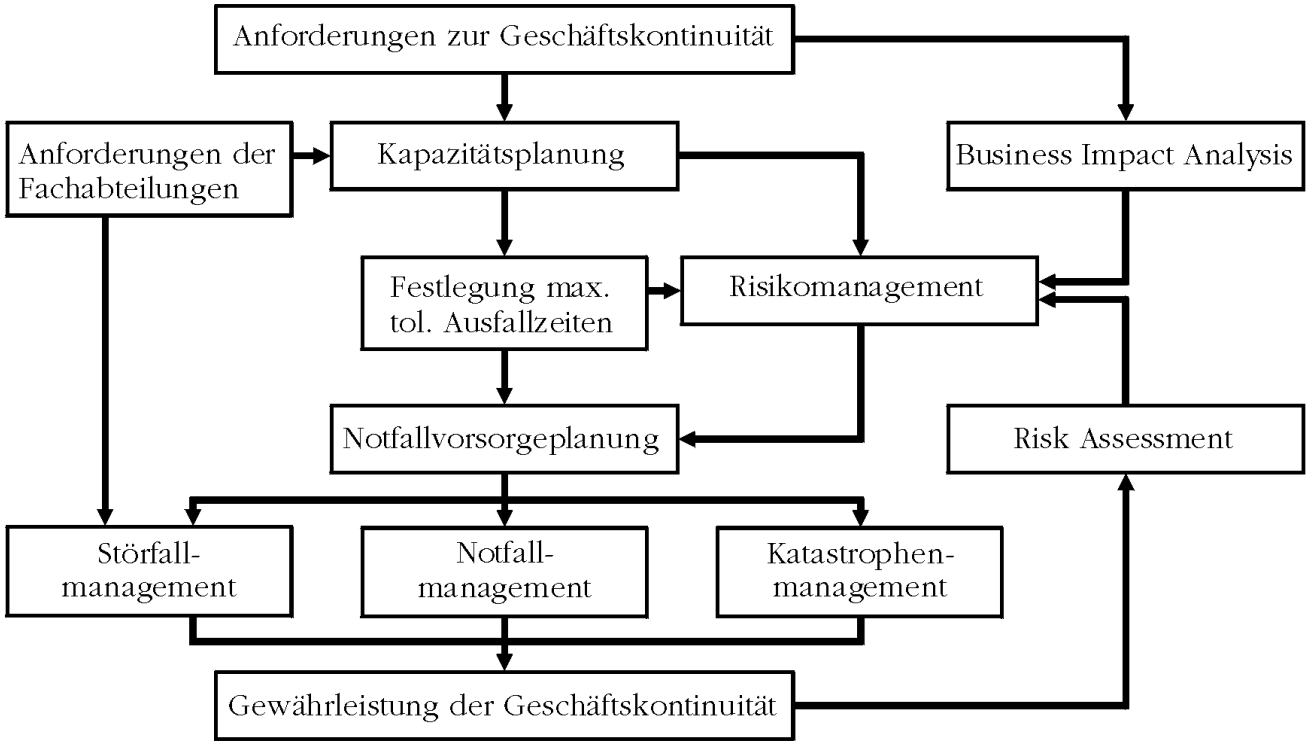
# Zusammenhang Ziele & Maßnahmen im ISMS



# Business Continuity Management

- Grundlage: **ISO 22301** (Requirements) **& ISO 22313** (Guidance)
- **Gewährleistung der Geschäftskontinuität** mithilfe
  - **Business Impact Analysis** (BIA) → Identifikation kritischer und für den Fortbestand bedrohlicher Prozesse der gesamten Wertschöpfungskette (inkl. etwaiger Abhängigkeiten auch gegenüber Lieferanten) & Ermittlung der Folgen (Personenschaden, Complianceverstoß, Reputationsschaden, Finanzschaden, Qualitätseinbußen, Umweltschaden) → Priorisierung für Wiederanlauf
    *Minimum Business Continuity Objective* (MBCO) = Minimum funktionstüchtiger Ressourcen, um Geschäftsziele während einer Unterbrechung zu erfüllen
    *Recovery Time Objective* (RTO) = maximale Dauer bis zum Wiederanlauf
    *Recovery Point Objective* (RPO) = maximal akzeptabler Datenverlust
    (→ Backup-Zyklen & Redundanzen!)
  - **Business Continuity Plan** → Dokumentation der (strategischen, taktischen & operativen) Vorgehensweisen beim Eintreten eines Notfalls (= Notfallkonzept)
    ***Notfall*** *= außergewöhnliche Abweichung vom Normalbetrieb (→ unterscheidet sich von Störfällen, die im Rahmen des laufenden Betriebs beherrschbar sind, und von Katastrophen, die sich großflächig auswirken & i.d.R. staatlich reglementiert sind)*
  - Durchführung von **Notfallübungen** anhand stimmiger Szenarien

# Absicherung der Geschäftskontinuität

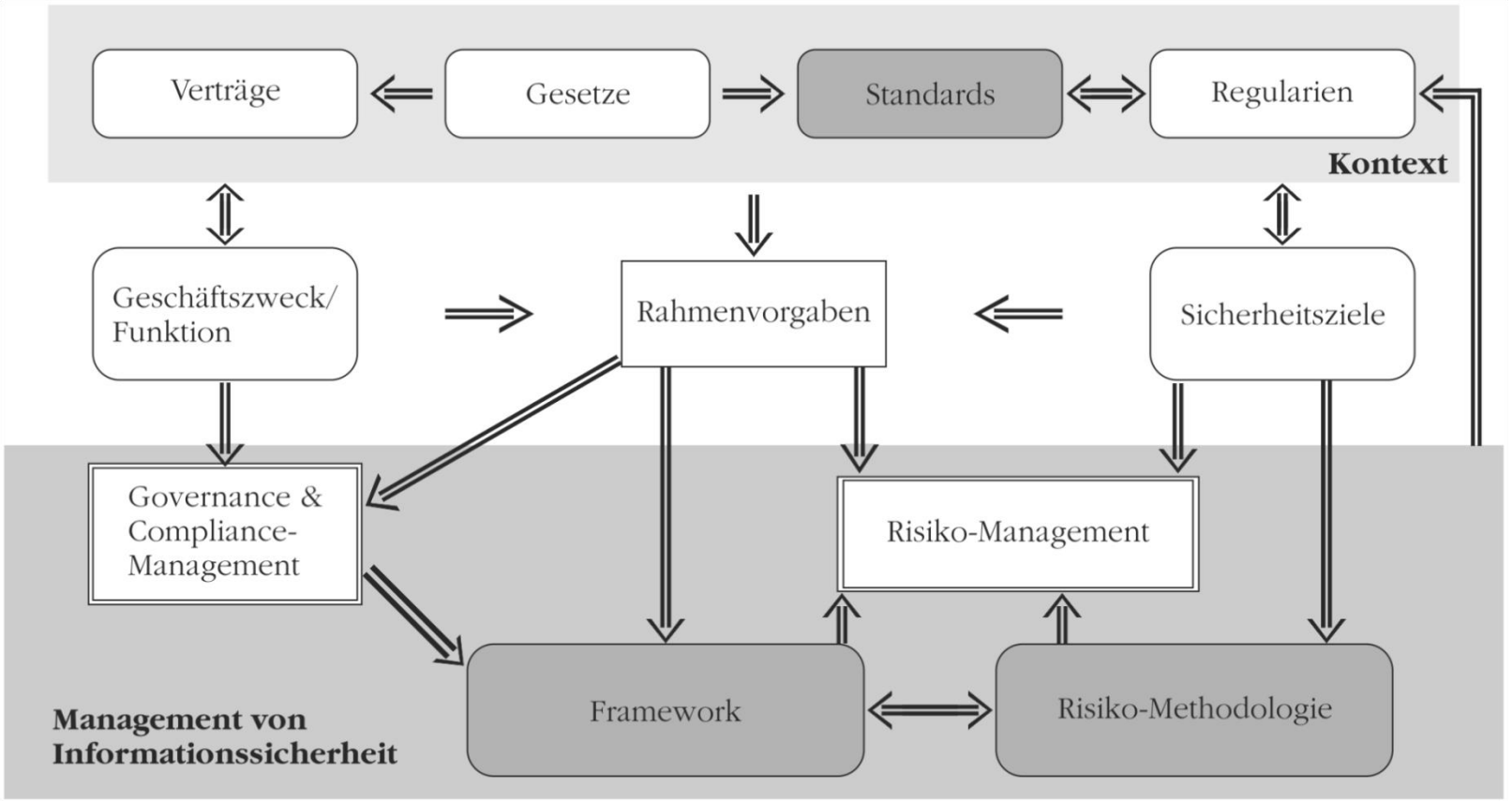


# Datensicherung

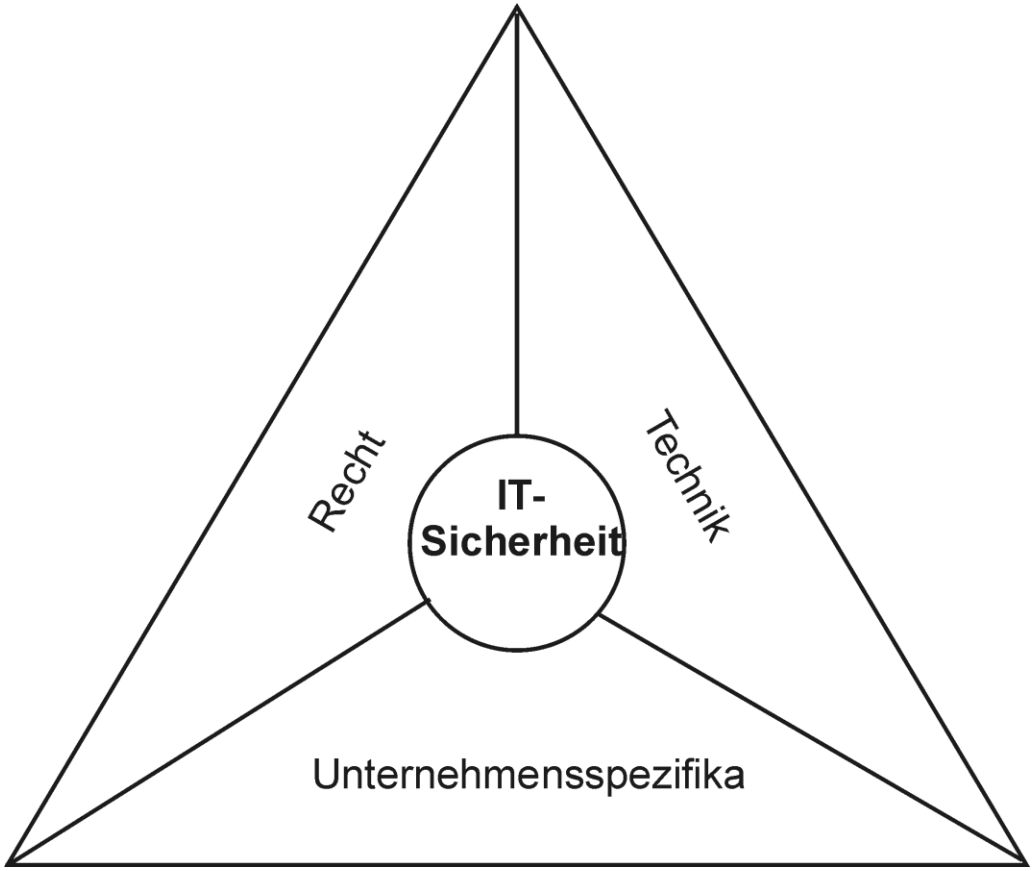
Im Rahmen der Rechtsprechung lassen sich folgende **Regelungen zur Datensicherung** ableiten:

- täglich hat wenigstens eine Differenzsicherung zu erfolgen und wöchentlich eine Vollsicherung (nach dem Urteil des OLG Hamm vom 01.12.2003; Az.: 13 U 133/03)
- der Erfolg einer Datensicherung ist zu überprüfen (nach dem Urteil des OLG Karlsruhe vom 07.11.1995; Az.: 3 U 15/95)
- bei einer Datensicherung muss die Wiederherstellbarkeit der gesicherten Daten auch bei einem Hardwaretausch überprüft werden (nach dem Urteil des LG Stuttgart vom 30.01.2002; Az.: 38 O 149/00 KfH)
- selbst bei manuellen Datensicherungen sind Vorkehrungen zur Vermeidung von Bedienfehlern zu treffen (nach dem Urteil des OLG Oldenburg vom 03.06.2003; Az.: 9 U 10/03)
- wurde für einen Nutzer dauerhaft für Nebenpflichten ein Mail-Account angelegt, müssen die auf diesem Account abgelegten Daten so lange vorgehalten werden, bis der Nutzer keine Verwendung für diese Daten mehr hat (nach dem Beschluss des OLG Dresden vom 05.09.2012; Az.: 4 W 961/12)

# Zusammenhang für ISMS



# 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** (nach EU-DSGVO):

- Art. 5 (Grundsätze), 24 (Verantwortung), 25 (Privacy by Design / Default), 28 (Auftragsverarbeitung), 32 (Schutzmaßnahmen), 33+34 (Datenpannen) & 35 (Datenschutz-Folgenabschätzung)
- Haftungsrecht: Art. 82 (Schadensersatz) & 83 (Bußgeld)

**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

# IT-Sicherheitsgesetz (1)

- Im Zuge des IT-Sicherheitsgesetzes (wirksam seit 25.07.2015) wurden besondere Vorschriften für **kritische Infrastrukturen** erlassen. Dazu zählen Einrichtungen, Anlagen oder Teile davon aus den Sektoren
  - Energie,
  - Informationstechnik und Telekommunikation,
  - Transport und Verkehr,
  - Gesundheit,
  - Wasser,
  - Ernährung sowie
  - Finanz- und Versicherungswesen,

  die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

# IT-Sicherheitsgesetz (2)

- Für diese Sektoren wurden im Rahmen der **BSI-KritisV** bestimmt, dass folgende Anlagen zur Erbringung einer kritischen Dienstleistung unter das IT-Sicherheitsgesetz fallen:
  → betriebsnotwendige Anlagen
  → für den Betrieb bedeutsame Nebeneinrichtungen
- Für die einzelnen Sektoren wurden in der BSI-KritisV einerseits qualitative Kriterien (Auflistung kritischer Dienstleistungen) als auch branchenspezifische Schwellenwerte (quantitative Kriterien; Versorgung von 500.000 Personen) benannt
- Betreiber kritischer Infrastrukturen haben nach § 8a Abs. 1 BSIG angemessene organisatorische und technische Vorkehrungen **zur Vermeidung von Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse unter Einhaltung des Stands der Technik zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind

# IT-Sicherheitsgesetz (3)

- Organisatorische und technische Vorkehrungen gelten im Kontext von kritischen Infrastrukturen nur dann als angemessen, wenn der dafür **erforderliche Aufwand nicht außer Verhältnis zu den Folgen** eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht
  - → Begründungspflicht für das Nichtergreifen von Schutzvorkehrungen, die nach Stand der Technik üblich sind
  - → Folgen für Ausfall / Beeinträchtigung gesamtwirtschaftlich / gesellschaftlich
  - → Begründung i.d.R. nur über kompensatorische Maßnahmen möglich
- Betreiber kritischer Infrastrukturen haben mind. alle 2 Jahre die Erfüllung der Anforderungen aus § 8a Abs. 1 BSIG nachzuweisen (unter Benennung von aufgedeckten Sicherheitsmängeln!)
- Erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die zu einem Ausfall oder eine Beeinträchtigung der Funktionsfähigkeit betriebener kritischer Infrastrukturen führen können oder geführt haben, sind dem BSI unverzüglich zu melden

# IT-Sicherheitsgesetz (4)

- Von den Betreibern einer kritischen Infrastruktur wird nach der Begründung des IT-Sicherheitsgesetzes insbesondere erwartet:
  - Betrieb eines Information Security Managements, welches u.a. die Sicherheitsorganisation festlegt und durch ein IT-Risikomanagement flankiert wird
  - Identifikation und Management kritischer Cyber-Assets
  - Betrieb von Maßnahmen zur Angriffsprävention und –erkennung
  - Implementierung eines Business Continuity Managements
  - Umsetzung branchenspezifischer Sicherheitsstandards
- Eine Störung liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken
- Erheblich und damit meldepflichtig sind IT-Störungen, die nicht bereits automatisiert oder mit wenig Aufwand mithilfe der nach Stand der Technik ergriffenen Maßnahmen abgewehrt werden können
  → neuartige, außergewöhnliche oder aufwandsintensive Störungen

# 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 (Art. 82 EU-DSGVO)
  → Beweislast trägt der Verantwortliche!
- Verletzung des Datengeheimnisses bzw. Fernmeldegeheimnisses berechtigt (je nach Schwere des Vergehens) zur „fristlosen“ Kündigung (ArbG-Urteile)
- Unbefugte Offenbarung personenbezogener Daten kann (wegen Verstoß gegen Art. 5 Abs. 1 lit. f EU-DSGVO) bis zu 20 Mio. € kosten (Art. 83 Abs. 5 EU-DSGVO)

# 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 2016:)
  - Datendiebstahl / Datenmissbrauch 24 %
  - Verletzung von Schutz- und Urheberrechten 18 %
  - Verrat von Betriebs- und Geschäftsgeheimnis 12 %

# 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