Doku*time* 2013

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Compliance und Datenschutz –
Wie sicher sind unsere digitalen Daten?

Prof. Dr. Michael Klotz

5. Dezember 2013, Greifswald

gfo | gesellschaft für organisation e.v.

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

Compliance und Datenschutz – Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Gliederung

1. Verortung Datenschutz – Datensicherheit – Compliance
2. So sicher, wie sie sein müssen
   (Perspektive der Legal Compliance)
3. ... wie sie sein sollen
   (Perspektive der Compliance mit Normen und Standards)
4. ... wie sie sind
   (Perspektive der Überwachung)
5. Fazit

Die gfo im Überblick

fachhochschule stralsund
university of applied sciences

- 1922, gegründet, gemeinnütziger Verein
- Regionale Meetings mit Vorträgen und Erfahrungsaustausch
- Jährlicher gfo-Jahreskongress für Organisation und Management, jährlicher Process Solutions Day (PSD)
  sowie weitere regionale Tagungen mit deutlichen Mitgliederrabatten
- Nutzung eines Netzwerkes von Organisationsexperten unterschiedlichster Branchen und Unternehmensgrößen
- Zugang zum
  - BPM CBOK (Business Process Management Common Body of Knowledge)
  - BABOK (Business Analysis Body of Knowledge)
- Kostenloser Bezug der Zeitschrift Führung + Organisation (zfo) (6 Hefte pro Jahr)
- Vergünstigungen bei gfo-Kongressen, Veranstaltungen, Zertifizierungen und Partnern (Weiterbildung, Verlage)
- Mitgliedsbeiträge: Einzelpersonen 100,- €, Unternehmen 322,- €, Stud. 33 €/Jahr

Compliance und Datenschutz – Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

SIMAT

Gliederung

1. Verortung Datenschutz – Datensicherheit – Compliance
2. So sicher, wie sie sein müssen
   (Perspektive der Legal Compliance)
3. ... wie sie sein sollen
   (Perspektive der Compliance mit Normen und Standards)
4. ... wie sie sind
   (Perspektive der Überwachung)
5. Fazit

1. Verortung Datenschutz – Datensicherheit – Compliance

fachhochschule stralsund
university of applied sciences

SIMAT

Datenschutz ist die Umsetzung des Rechts auf informationelle Selbstbestimmung gemäß dem sog. Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983:

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

(BVerfG – Bundesverfassungsgericht, Az.1 BvR 209, 269, 362, 420, 440, 484/83)

Link: http://openjur.de/u/268440.html

1. Verortung Datenschutz – Datensicherheit – Compliance

fachhochschule stralsund
university of applied sciences

Abgrenzung nach BSI (Bundesamt für Sicherheit in der Informationstechnik):

Datenschutz =

Schutz personenbezogener Daten vor dem Missbrauch durch Dritte

Datensicherheit (Informationssicherheit) =

Schutz von Daten hinsichtlich gegebener Anforderungen an deren **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** bezeichnet.

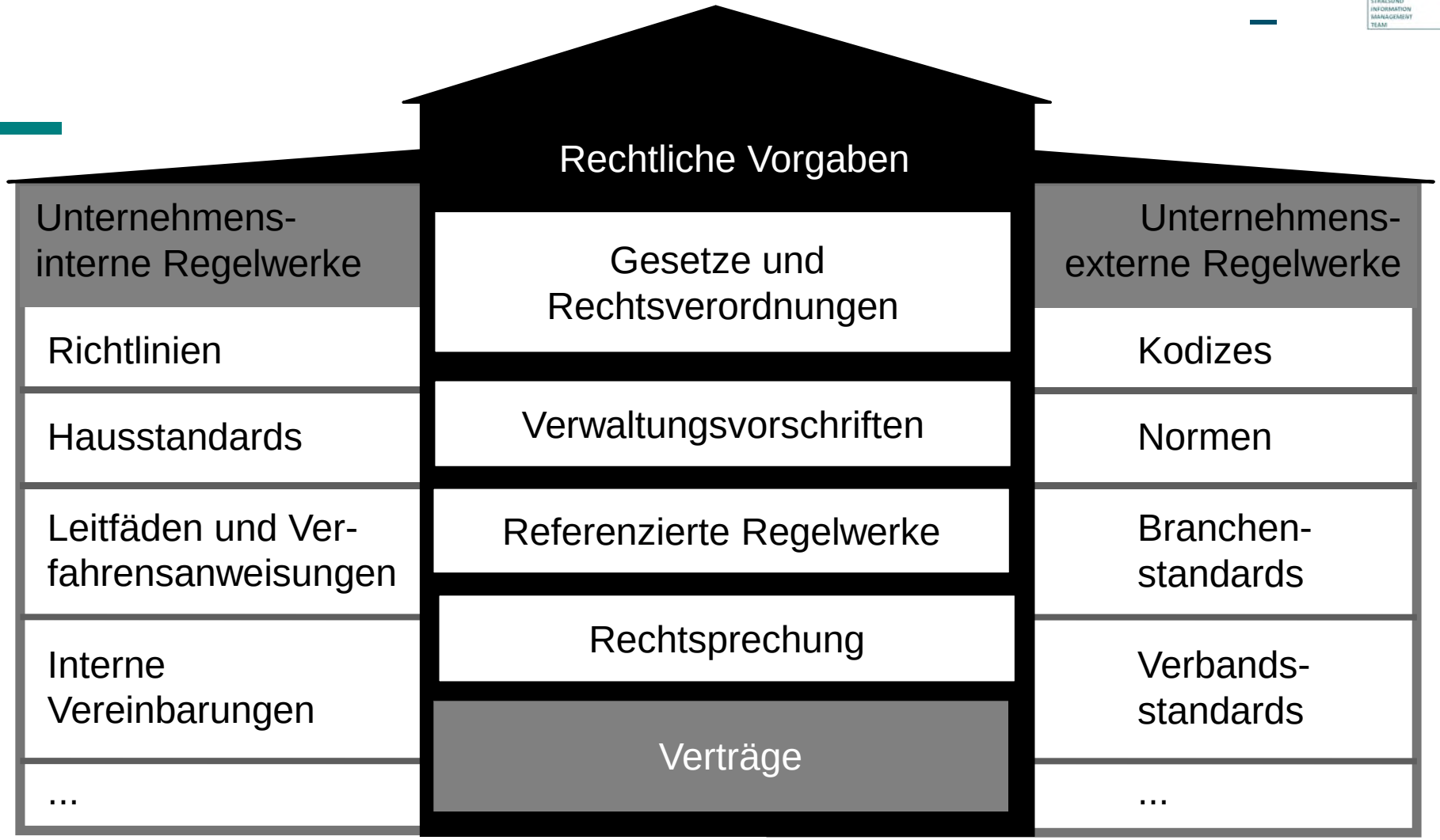
- **Vertraulichkeit:** Schutz vor unbefugter Preisgabe
- **Verfügbarkeit:** Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen stehen zum geforderten Zeitpunkt zur Verfügung
- **Integrität:** Die Daten sind vollständig und unverändert.

Quelle: BSI Leitfaden für Informationssicherheit, IT-Grundschutz kompakt, Stand Feb. 2012, S. 14
Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

1. Verortung Datenschutz – Datensicherheit – Compliance

fachhochschule stralsund
university of applied sciences
SIMAT

1. Verortung Datenschutz – Datensicherheit – Compliance



Quelle: Klotz, M.: IT-Compliance. In: Tiemeyer (Hg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 5. Auflage, München: Hanser 2013, S. 733

Compliance und Datenschutz – Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

SIMAT

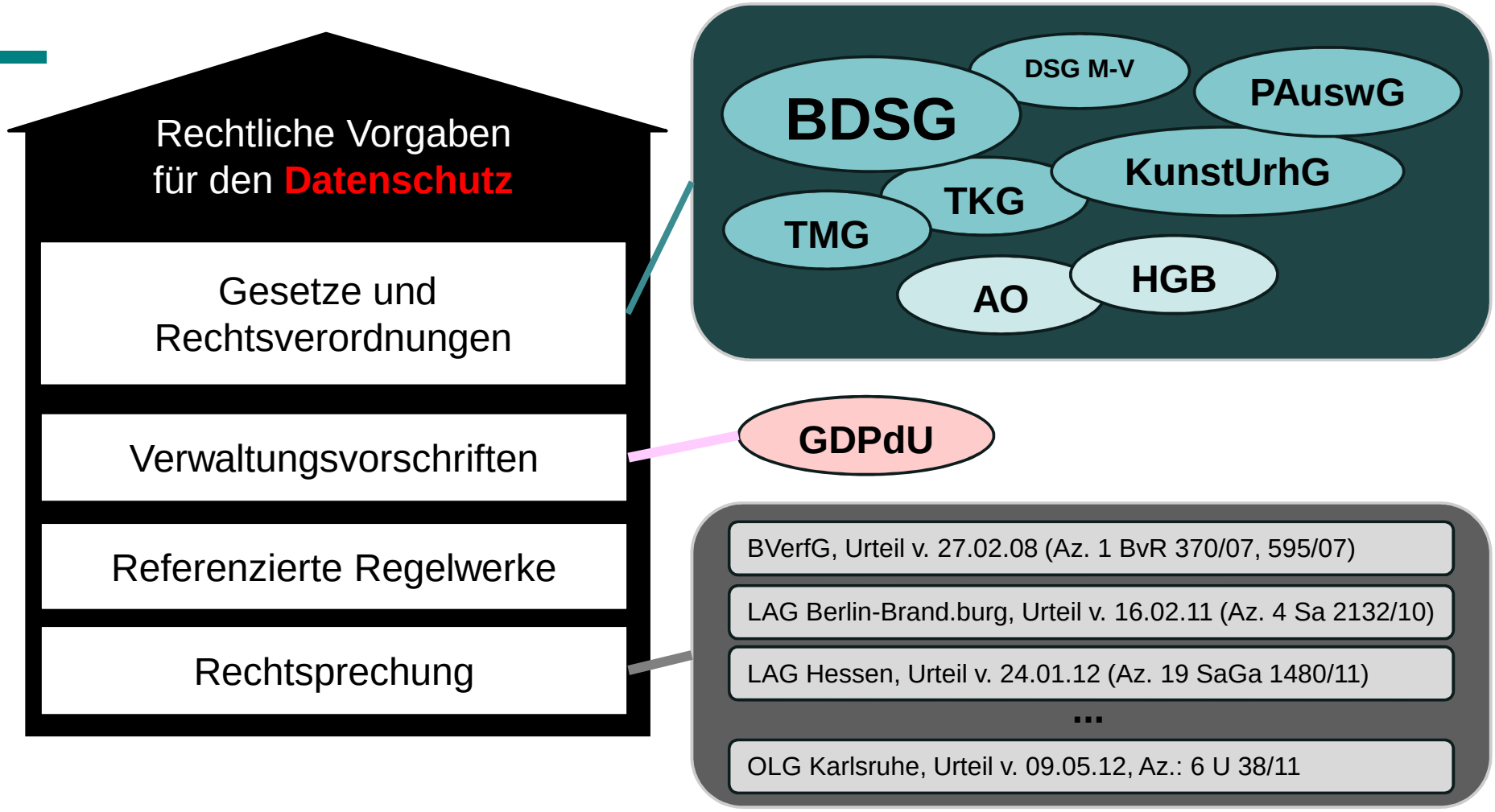
Gliederung

1. Verortung Datenschutz – Datensicherheit – Compliance
2. So sicher, wie sie sein müssen
   (Perspektive der Legal Compliance)
3. ... wie sie sein sollen
   (Perspektive der Compliance mit Normen und Standards)
4. ... wie sie sind
   (Perspektive der Überwachung)
5. Fazit

2. So sicher, wie sie sein müssen

fachhochschule stralsund
university of applied sciences

SIMAT



2. So sicher, wie sie sein müssen

fachhochschule stralsund
university of applied sciences
SIMAT

Technische und organisatorische (Mindest-)Maßnahmen nach Anlage (zu § 9 Satz 1)

1. **Zutrittskontrolle**: kein Zutritt zur Räumen mit IT-Systemen, mit denen personenbezogene Daten (pD) verarbeitet oder genutzt werden
2. **Zugangskontrolle**: keine Nutzung von IT-Systemen durch Unbefugte
3. **Zugriffskontrolle**: keine Datenzugriff durch Personen ohne Zugriffsberechtigung und Sicherstellung, dass pD „bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“
4. **Weitergabekontrolle**: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von pD bei elektronischen Übertragung und Transport und Möglichkeit der Prüfung und Feststellung, an welche Stellen eine Übermittlung vorgesehen ist

Eine Maßnahme nach Nummer 2-4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

2. So sicher, wie sie sein müssen

fachhochschule stralsund
university of applied sciences

Technische und organisatorische (Mindest-)Maßnahmen nach Anlage (zu § 9 Satz 1)

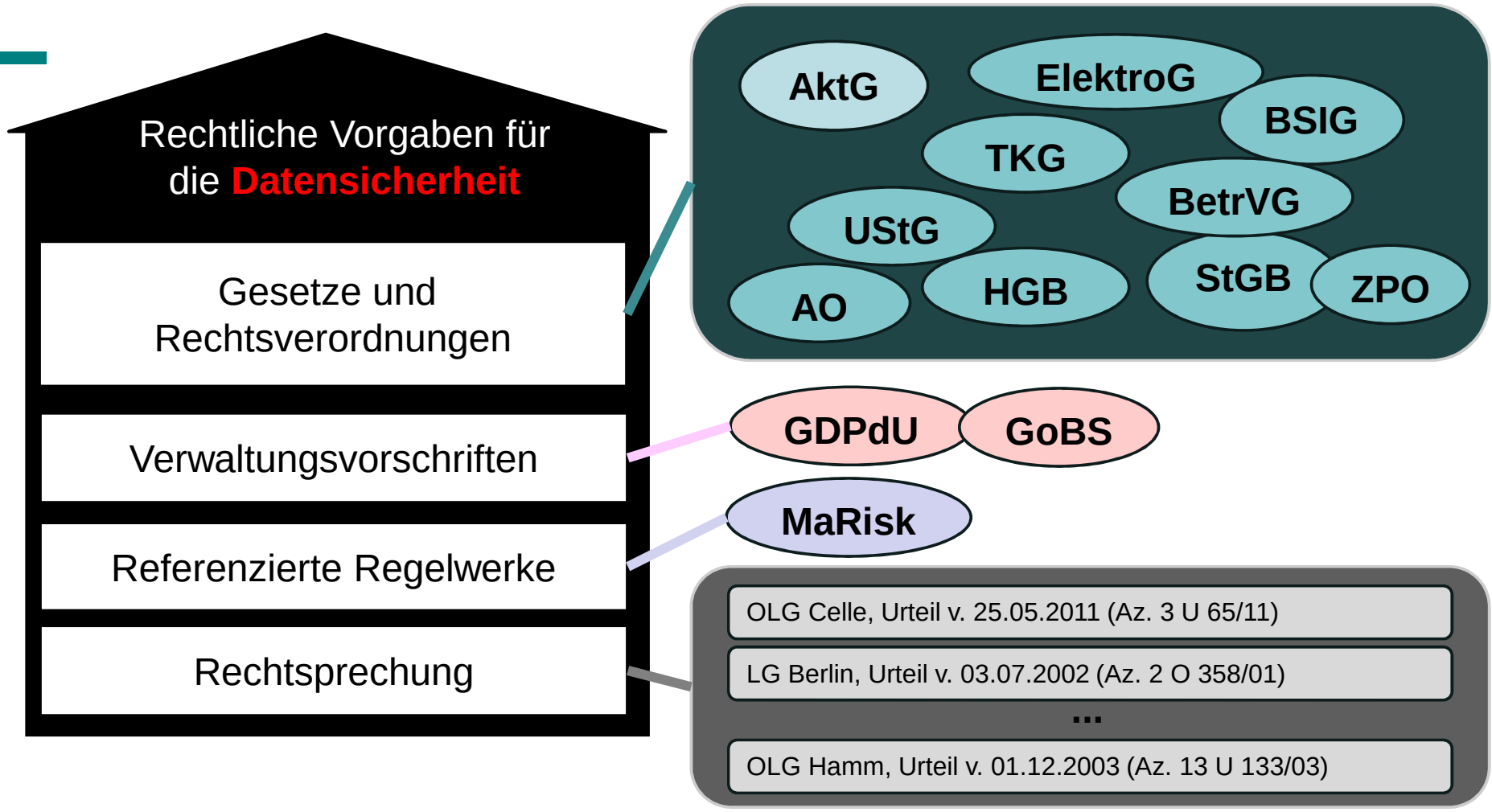
5. **Eingabekontrolle**: Möglichkeit der nachträglichen Überprüfung und Feststellung, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind
6. **Auftragskontrolle**: Sicherstellung, dass im Auftrag verarbeitete pD, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
7. **Verfügbarkeitskontrolle**: Schutz der personenbezogenen Daten gegen zufällige Zerstörung oder Verlust
8. **(Trennungskontrolle**:) Sicherstellung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

⟶ **Das sind natürlich auch alles Maßnahmen der Datensicherheit!**

2. So sicher, wie sie sein müssen

fachhochschule stralsund
university of applied sciences

SIMAT



2. So sicher, wie sie sein müssen

fachhochschule stralsund
university of applied sciences

SIMAT

GOBS
Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

- Publiziert als BMF-Schreiben vom 7. November 1995
- Ziel der Datensicherungsmaßnahmen ist es, die Risiken für die gesicherten Programme/Datenbestände hinsichtlich Unauffindbarkeit, Vernichtung und Diebstahl zu vermeiden
- ausgeprägtes Datensicherheitskonzept ist unabdingbar; dieses umfasst auch die Sicherung der EDV-technischen Installationen (Hardware, Leitungen etc.)
- rechnungslegungsrelevante Informationen sind gegen Verlust zu sichern und gegen unberechtigte Veränderung zu schützen
- darüberhinaus sind sensible Informationen des Unternehmens gegen unberechtigte Kenntnisnahme zu schützen
- Zugriffs- bzw. Zugangskontrollen gegen unberechtigte Veränderungen
- Datensicherheitskonzept ist der technischen Entwicklung anzupassen
- Datensicherungskonzept ist zu dokumentieren

Quelle:
http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Betriebspruefung/015.pdf?__blob=publicationFile&v=3

2. So sicher, wie sie sein müssen

fachhochschule stralsund
university of applied sciences
SIMAT

LG Berlin, Urteil v. 03.07.2002 (Az. 2 O 358/01)

- Kündigung eines Vorstandsmitglieds (vom Berufungsgericht wg. Fristüberschreitung für unwirksam erklärt)
- vom Vorstand getroffene Maßnahmen erfüllten nicht Anforderungen an ein Risikofrüherkennungssystem nach § 91 Abs. 2 AktG und § 25a KWG
- entsprechende Feststellung im Jahresabschlussbericht der beauftragten Wirtschaftsprüfungsgesellschaft
- expliziter Bezug auf Schwächen in der IT, insb. mangelhafte Datenqualität, die sich in einem veralteten und unvollständigen Datenbestand zeigte.
- Mangel lt. Gericht „besonders gravierend, weil die Qualität und ständige Verfügbarkeit von EDV-Daten grundlegend ist für die Überwachung von Risiken und die Reaktion auf Risiken“
- gekündigtes Vorstandsmitglied konnte sich nicht darauf berufen, für die Datenverarbeitung nicht verantwortlich gewesen zu sein, da sie zum fraglichen Zeitpunkt „in den Verantwortungsbereich des Gesamtvorstands und damit auch in seine Verantwortung fiel“

Compliance und Datenschutz – Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

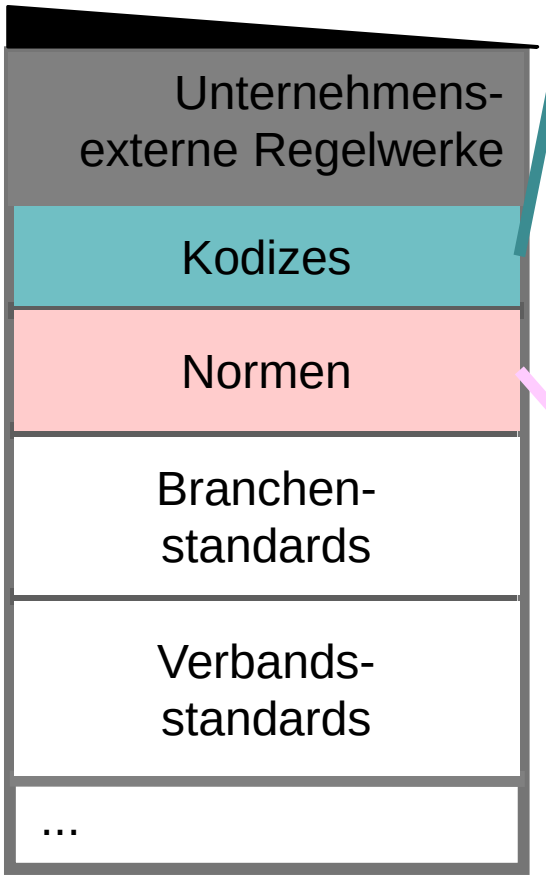
SIMAT

Gliederung

1. Verortung Datenschutz – Datensicherheit – Compliance
2. So sicher, wie sie sein müssen
   (Perspektive der Legal Compliance)
3. ... wie sie sein sollen
   (Perspektive der Compliance mit Normen und Standards)
4. ... wie sie sind
   (Perspektive der Überwachung)
5. Fazit

4. ... wie sie sein sollen

fachhochschule stralsund
university of applied sciences



OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security (2002)

- DIN 66399 Büro- und Datentechnik – **Vernichten** von **Datenträgern**
- DIN ISO/IEC **27000** Informationstechnik – IT-Sicherheitsverfahren – **Informationssicherheits-Managementsysteme** – **Überblick** und Terminologie
- DIN ISO/IEC **27001** Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – **Anforderungen** (z)
- DIN ISO/IEC **27002** Informationstechnik - IT-Sicherheitsverfahren – **Leitfaden** für das Informationssicherheits-Management
- ISO/IEC 18043 Information technology – Security techniques – Selection, deployment and operations of **intrusion detection system**
- ISO/IEC 20000-1 Information technology – Service management – Part 1: **Service management** system requirements (z)
- ISO/IEC 20000-2 Information technology – Service management – Part 2: **Guidance** on the application of service management systems

4. ... wie sie sein sollen

fachhochschule stralsund
university of applied sciences

- ISO/IEC 24762 Information technology – Security techniques – Guidelines for information and communications technology **disaster recovery** services
- ISO/IEC **27003** Information technology – Security techniques – Information security management system **implementation guidance**
- ISO/IEC **27004** Information technology – Security techniques – Information security management – **Measurement**
- ISO/IEC **27005** Information technology – Security techniques – Information security **risk management**
- ISO/IEC **27014** Information technology – Security techniques – **Governance** of information security
- ISO/IEC **27031** Information technology – Security techniques – Guidelines for information and communication technology readiness for **business continuity**
- ISO/IEC **27032** Information technology – Security techniques – Guidelines for **cybersecurity**
- ISO/IEC **27035** Information technology – Security techniques – Information **security incident management**

4. ... wie sie sein sollen

fachhochschule stralsund
university of applied sciences

- BSI-Standard 100-1: **Managementsysteme** für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-**Vorgehensweise** (z)
- BSI-Standard 100-3: **Risikoanalyse** auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: **Notfallmanagement**
- BSI: **IT-Grundschutzkataloge**
- ITIL® (Information Technology Infrastructure Library) des Cabinet Office/APM
- **Payment Card** Industry Data Security Standard (PCI DSS) (z)

"ITIL® " ist eingetragenes Warenzeichen des Cabinet Office.

4. ... wie sie sein sollen

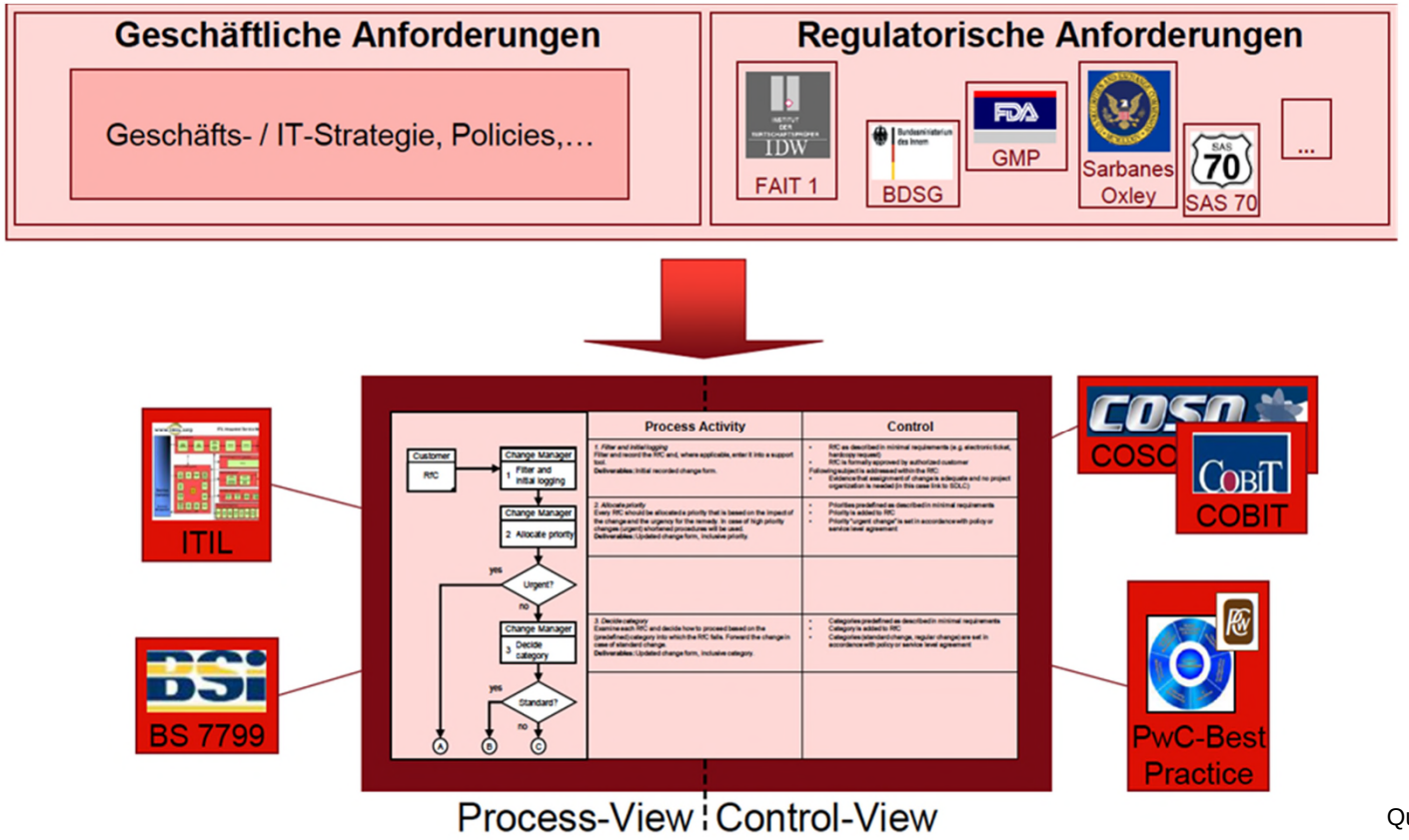
fachhochschule stralsund
university of applied sciences

- COBIT 5 (Control Objectives for Information and Related Technology) der ISACA (Information Systems Audit and Control Association)
- IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie (z)
- IDW PS 880: Die Prüfung von **Softwareprodukten**
- IDW RS FAIT 1: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von **Informationstechnologie**
- IDW RS FAIT 2: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von **Electronic Commerce**
- IDW RS FAIT 3: Grundsätze ordnungsmäßiger Buchführung beim Einsatz **elektronischer Archivierungsverfahren**
- IDW RS FAIT 4: Anforderungen an die Ordnungsmäßigkeit und Sicherheit IT-gestützter **Konsolidierung**sprozesse
- International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a **Service Organization** (z)

4. ... wie sie sein sollen

fachhochschule stralsund
university of applied sciences

Die Herausforderung besteht in der integrativen Handhabung der unterschiedlichsten Anforderungen.



Quelle: PwC, Dr. Martin Fröhlich

Compliance und Datenschutz – Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

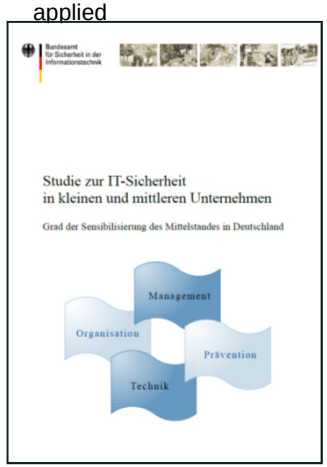
SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Gliederung

1. Verortung Datenschutz – Datensicherheit – Compliance
2. So sicher, wie sie sein müssen
   (Perspektive der Legal Compliance)
3. ... wie sie sein sollen
   (Perspektive der Compliance mit Normen und Standards)
4. ... wie sie sind
   (Perspektive der Überwachung)
5. Fazit

4. ... wie sie sind

fachhochschule stralsund
university of applied



Ergebnisse einer qualitativen Studie des BSI von 2011:

- Bewusstsein für IT-Sicherheit ist in KMU generell vorhanden
- KMU im Bereich IT-Sicherheit grds. gut aufgestellt
- 2/3 der Sicherheitsmaßnahmen nach IT-Grundschutz umgesetzt
- Nachholbedarf im Bereich kritischer IT-Sicherheitsprozesse (Sicherheitsvorfälle, Notfallmanagement, Bewertung der Gefahrenbereiche)
- Umfangreiche Maßnahmen sind realisiert in den Bereichen Datensicherung, Risikobewertung der Geschäftsprozesse, Informationen zur Bedrohungslage, Sicherheitsupdates, Absicherung der Netzwerke
- Unternehmensleitung nimmt Verantwortung für IT-Sicherheit deutlich sichtbar wahr
- IT-Sicherheitsverantwortlicher nur in 50% der Unternehmen benannt
- Primärer Handlungsbedarf besteht im Bereich der Präventivmaßnahmen und der IT-Sicherheitsmanagementprozesse

Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf;jsessionid=6192459BA481748896A8B2D1AAC0C751.2_cid286?__blob=publicationFile

4. ... wie sie sind

fachhochschule stralsund
university of applied sciences

Prüfung der Datensicherheit erfolgt im Rahmen des internen Kontrollsystems (IKS):

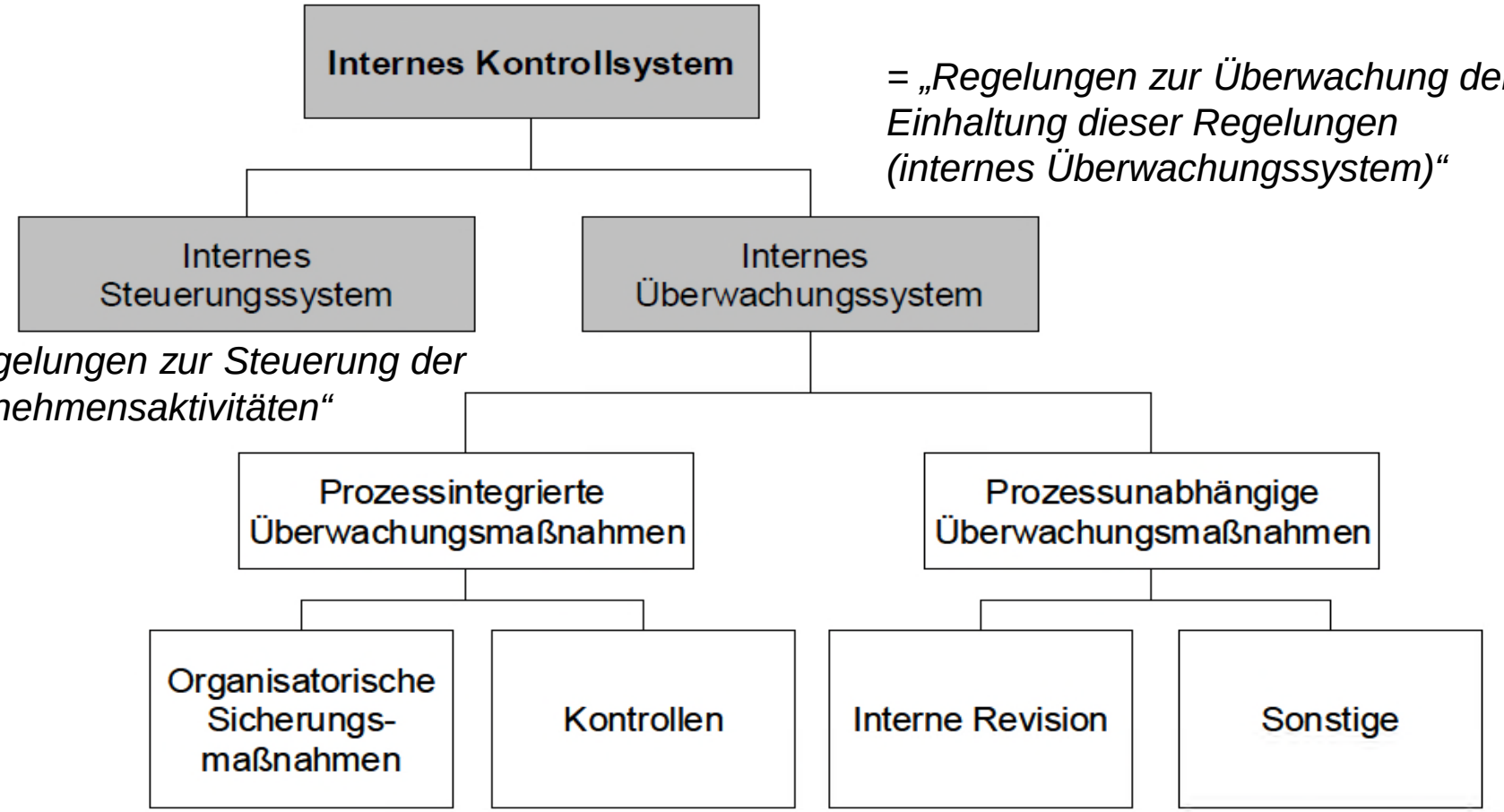
„Unter einem **internen Kontrollsystem** werden die von dem Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen des Managements

- zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit (hierzu gehört auch der **Schutz des Vermögens**, einschließlich der Verhinderung und Aufdeckung von Vermögensschädigungen),
- zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen **Rechnungslegung** sowie
- zur Einhaltung der für das Unternehmen maßgeblichen **rechtlichen Vorschriften**."

Nach **GoBS** gilt: „Die Beschreibung des IKS ist Bestandteil der Verfahrens-dokumentation ... . Eine Wahlmöglichkeit für den Buchführungspflichtigen, welche Beschreibung er für erforderlich hält, besteht nicht."

Quelle: IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261 n.F., Stand: 01.03.2012)

4. ... wie sie sind



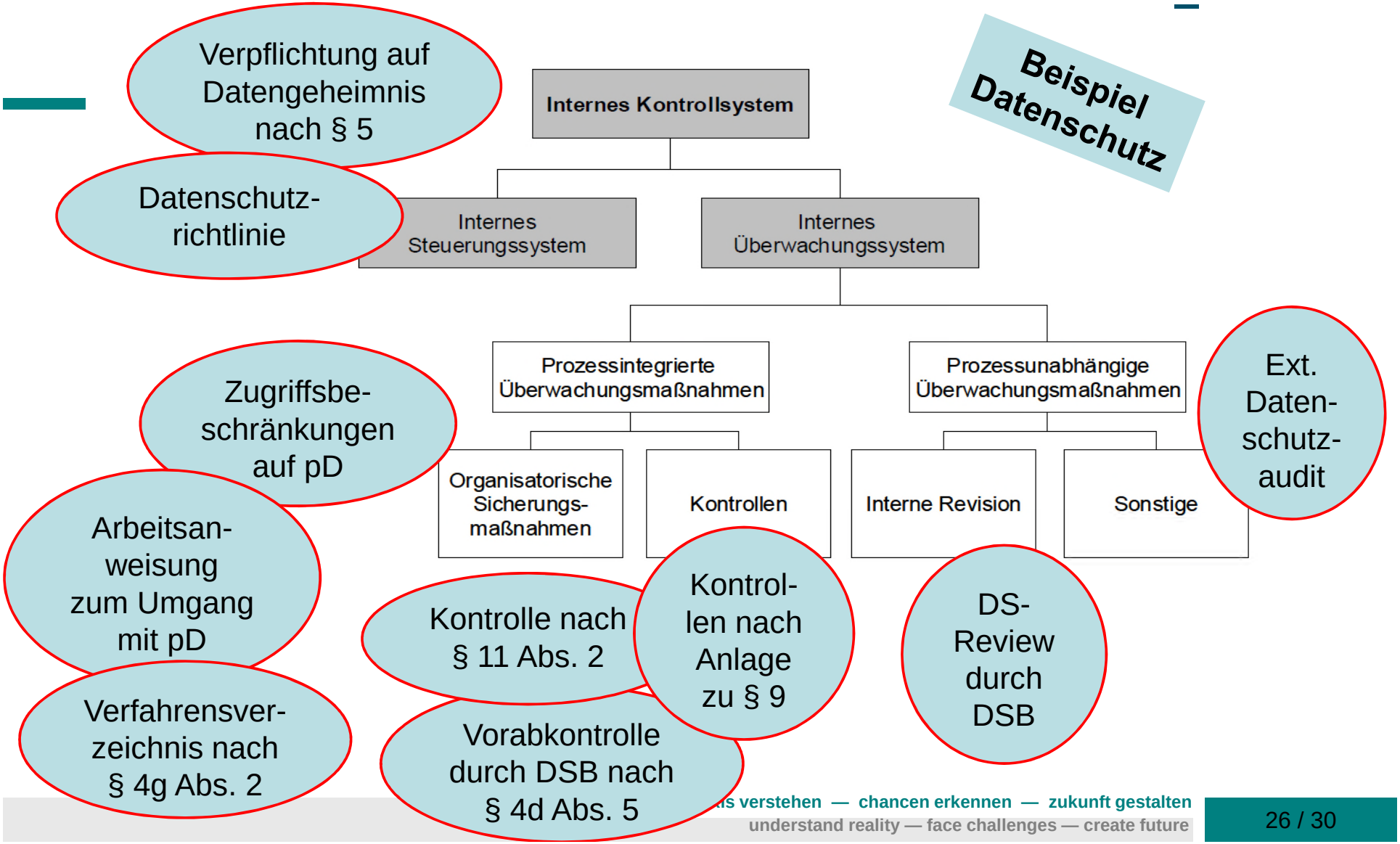
= „Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem)“

= „Regelungen zur Steuerung der Unternehmensaktivitäten“

Quelle IDW, entnommen aus Bungartz, Oliver: Handbuch Interne Kontrollsysteme, 3. Aufl. Erich Schmidt, Berlin 2012, S. 24

4. ... wie sie sind

fachhochschule stralsund
university of applied sciences



Compliance und Datenschutz – Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

SIMAT

Gliederung

1. Verortung Datenschutz – Datensicherheit – Compliance
2. So sicher, wie sie sein müssen
   (Perspektive der Legal Compliance)
3. ... wie sie sein sollen
   (Perspektive der Compliance mit Normen und Standards)
4. ... wie sie sind
   (Perspektive der Überwachung)
5. Fazit

5. Fazit: Wie sicher sind unsere digitalen Daten?

fachhochschule stralsund
university of applied sciences

Unsere Daten sind in dem Umfang sicher

- wie wir uns an gesetzliche Vorgaben halten,
- uns an selbst gewählten Normen und Standards orientieren,
- hieraus Grundsätze, Verfahren sowie technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit entwickeln,
- diese im Rahmen des dokumentierten internen Kontrollsystems (IKS) umsetzen
- und durch die Prüfung des IKS sicherstellen, dass die Überwachungsmaßnahmen wirksam sind bzw. identifizierte Schwachstellen durch kontinuierliche Verbesserung des IKS entfernt werden.

Kontakt und Information

Prof. Dr. Michael Klotz

FH Stralsund, FB Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
Fon +49 (0)3831 45-6946
Fax +49 (0)3831 45-6604
eMail michael.klotz@fh-stralsund.de

Fragen?


Ihr wollt an meine Daten?
Die hab ich AES-256-verschlüsselt!
© quickmeme