DialogCamp

FOM Hochschule

Integration von Informationssicherheits- und Datenschutzmanagement

Warum wir Synergieeffekte zwischen Informationssicherheits- und Datenschutzmanagement nutzen sollten um EU-DSGVO-Compliance zu erlangen

Dominik Schrahe

Agenda

1. **Informationssicherheit vs. Datenschutz**

2. **Schnittmengen Informationssicherheits- & Datenschutzmanagement**

3. **Herausforderungen der Integration**

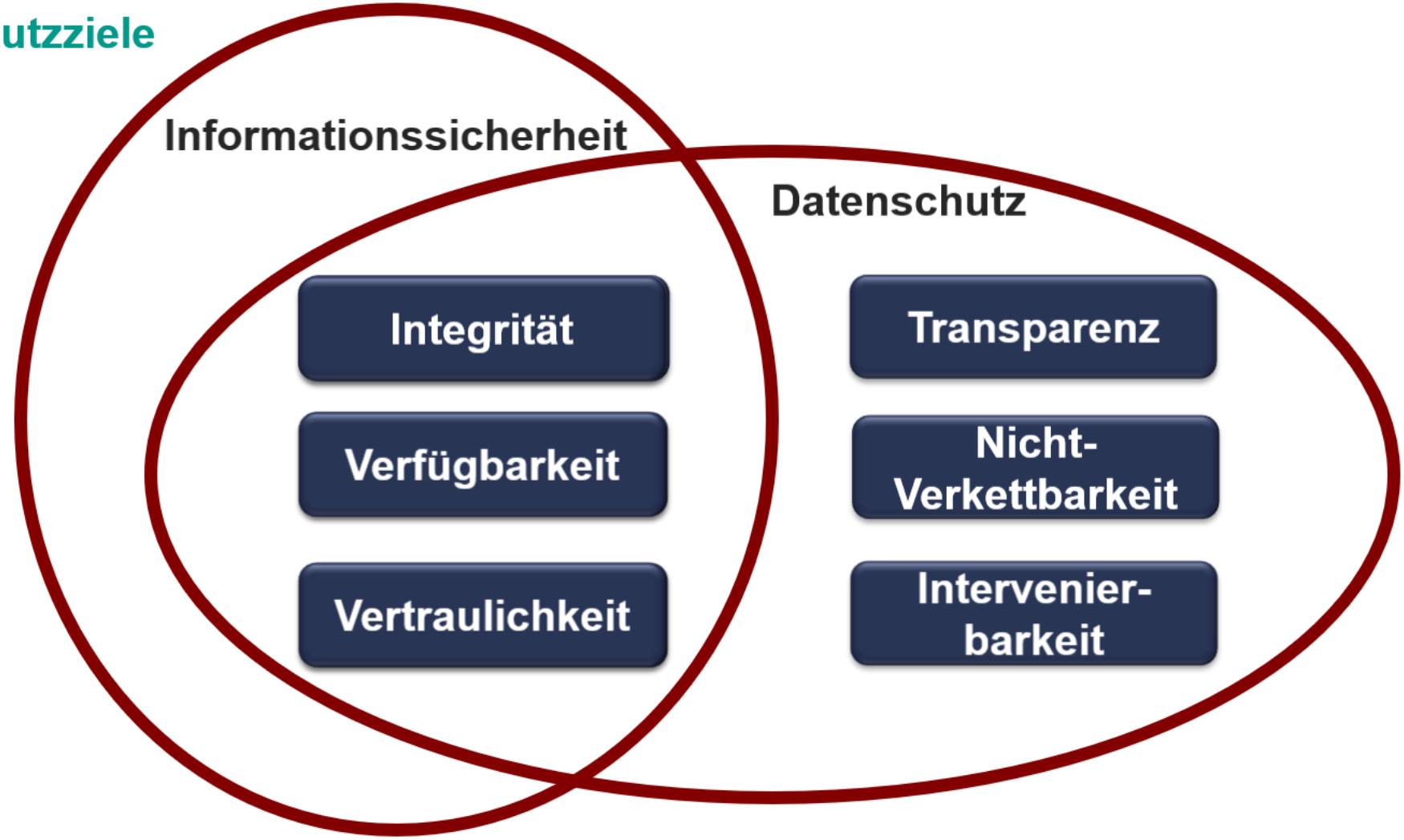
4. **Aufbau- und Ablauforganisation des integrierten Managementsystems**

5. **Fazit und Diskussion**

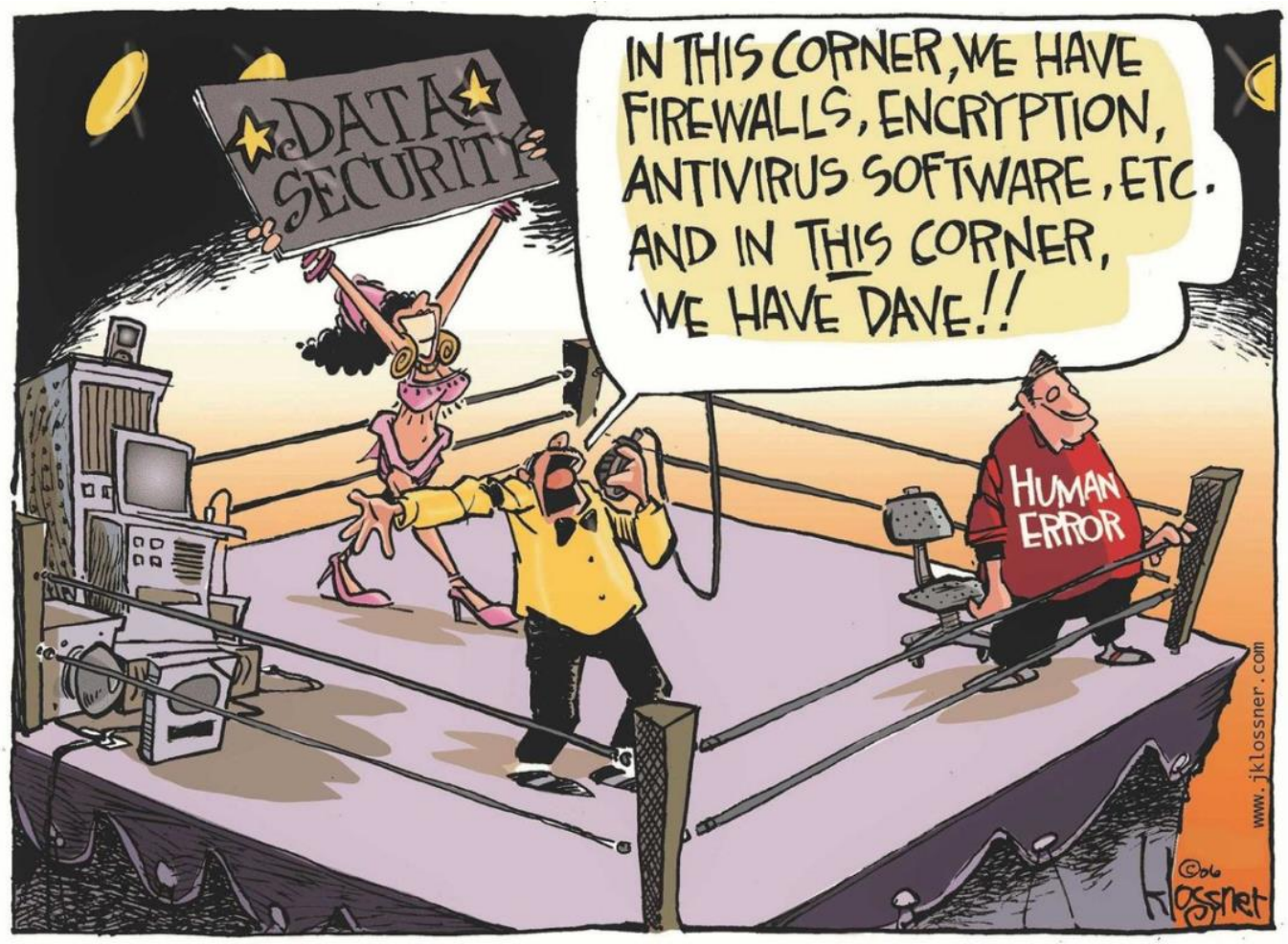
Gemeinsamkeiten und Unterschiede

- **Welche Gemeinsamkeiten und Differenzen bestehen zwischen beiden Disziplinen?**
- **Ist eine integrierten Betrachtungsweise möglich/ sinnvoll?**
- **Informationssicherheit = technischer Datenschutz?**

Schutzziele



1. Informationssicherheit vs. Datenschutz



➔ **Erforderlich sind Managementsysteme, die über eine technische Betrachtung hinausgehen**

Managementsysteme [Vgl. Loomans, D. u.a. (2014)]

- **Verbund aller organisatorischen und technischen Einrichtungen um ein Ziel (z.B. Datenschutz-Compliance) zu erreichen**
- **Risikoanalyse**
- **Definition von Rollen und Zuständigkeiten**
- **Definition von Prozessen**
- **Prüfung der Zielerreichung**

DSGVO und Datenschutzmanagementsysteme [Art. 32 EU-DSGVO]

- **Präventive und reaktive technische und organisatorische Maßnahmen**
- **Risikoangemessenheit**
- **Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit**
- **Regelmäßige Überprüfung und Evaluierung**

➔ **Erforderlichkeit eines Datenschutzmanagementsystems (DSMS)**

DSMS und Informationssicherheitsmanagementsysteme (ISMS)

- **Eigenständiges DSMS müsste nahezu alle ISMS-Bestandteile abbilden** [Vgl. Quiring-Kock, 2012]
- **Angemessenes Informationssicherheitsniveau als Voraussetzung für DSMS** [Vgl. Quiring-Kock, G. (2012)]
- **Aber: Trennung zwischen ISMS und DSMS um Kontrollfunktionen des DSMS ggü. Dem ISMS gerecht werden zu können** [Vgl. Rost, 2013]

2. Schnittmengen Informationssicherheits- & Datenschutzmanagement

Informationssicherheitsmgmt.

[Vgl. Kersten, H., Klett, G. (2015)]

Schutz von Wertgegenständen (sog. Assets) bspw.

- **Immobilien**
- **Maschinen/Geräte**
- **Datenbestände**
- **Soft Assets (z.B. Image)**

Präventiv sowie reaktiv

Datenschutzmgmt.

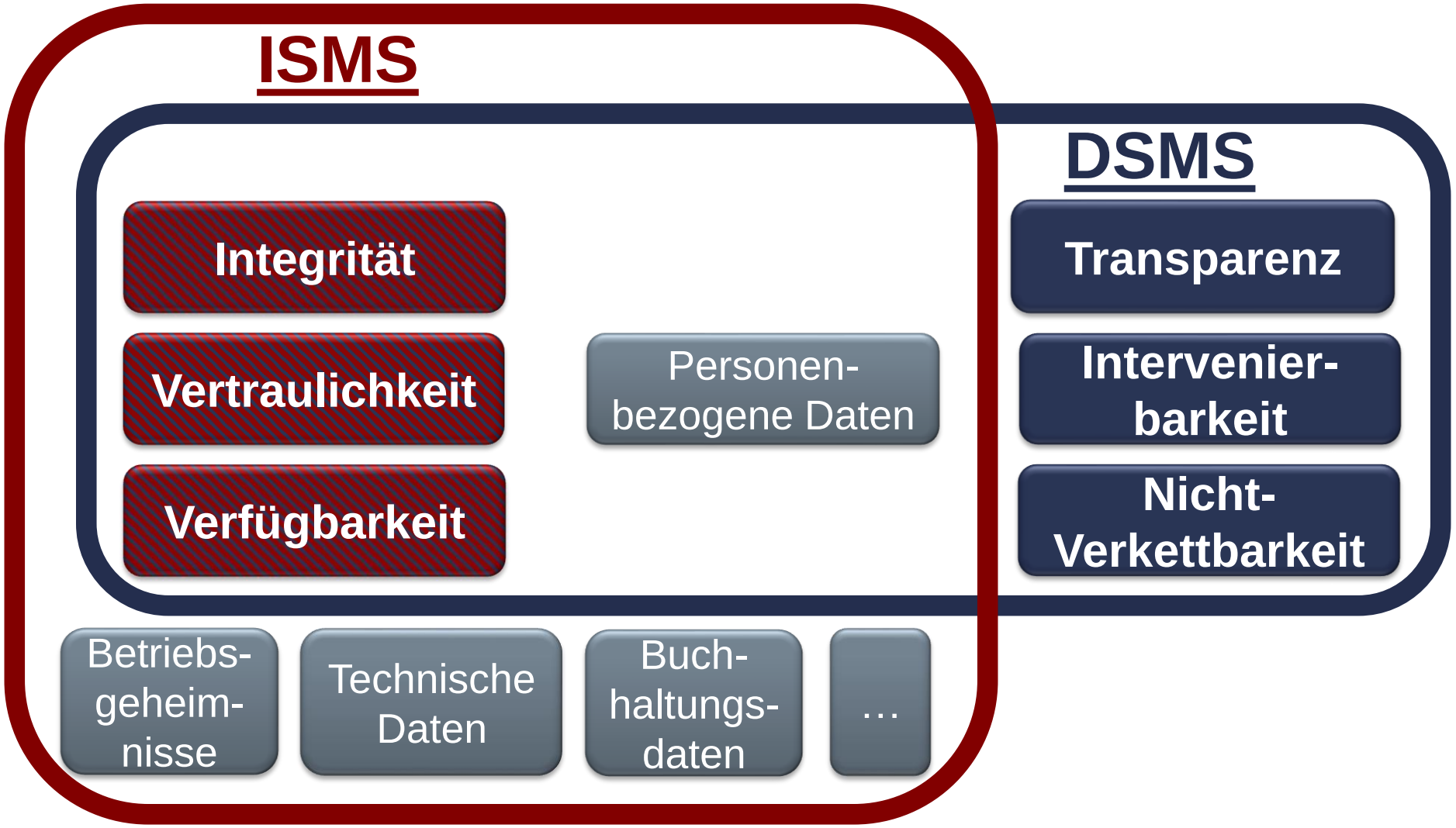
[Vgl. Rost, M. (2013); Bock, K. u.a. (2016)]

Schutz personenbezogener Daten bspw.

- **Mitarbeiterdaten**
- **Kundenstammdaten**
- **Gesundheitsdaten z.B. in Krankenhäusern)**

Präventiv sowie reaktiv

Überschneidungen bei Schutzzielen von ISMS und DSMS



Betrachtung von Informationssicherheits- und Datenschutzstandards

- **z.B. ISO 27000, BSI-Grundschutz, Standard-Datenschutzmodell, EuroPriSe:**
- **Keine Konfliktfälle aus Standards abzuleiten → Grds. Integrierbarkeit**
- **Aber: Konflikte können aus Umsetzung hervorgehen und sind jeweils im konkreten Anwendungsfall zu bewerten (z.B. ISO 27002 12.4.1 Event-Logging)**

Konfliktfelder zwischen DSMS und ISMS und deren Auflösung

Logging/Protokollierung technischer Ereignisse

- **ISMS: So viele und genaue Daten wie möglich sammeln und so lange wie möglich speichern, um Hackerangriffe exakt analysieren zu können**
- **DSMS: Nach Möglichkeit keine personenbezogenen Daten sammeln, es gilt das Prinzip der Datensparsamkeit und der schnellstmöglichen Löschung**

➔ **Individuelle Lösung mit DSB, ISB und Betriebsrat erforderlich**

➔ **Ausgewählte Protokollierung auf separatem Server**

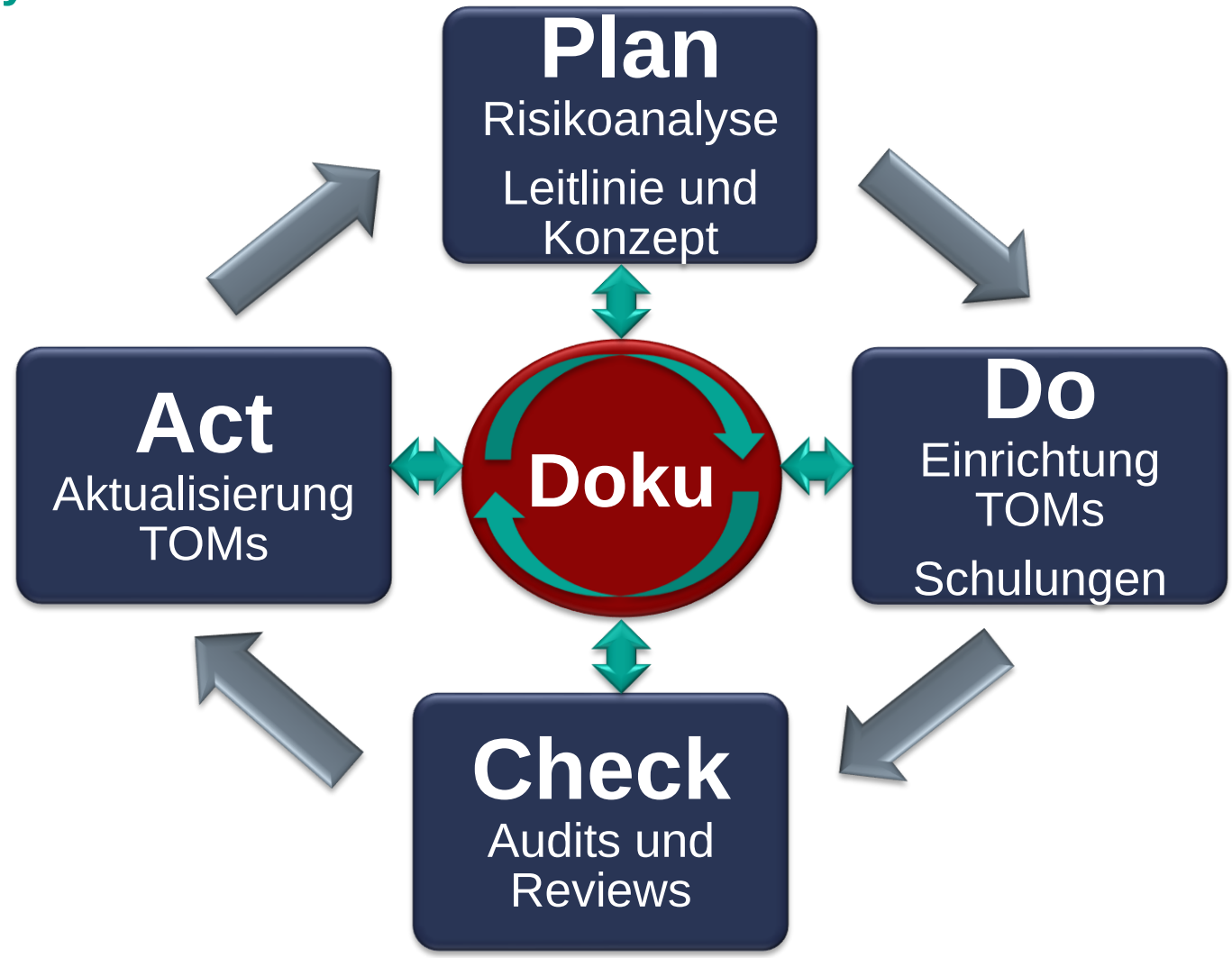
➔ **Schnellstmögliche Auswertung und Löschung falls keine Auffälligkeiten**

Kernprozesse von ISMS und DSMS [Vgl. Haufe u.a., 2016; Loomans u.a., 2014]

- **Risikobewertung**
- **Mitarbeitersensibilisierung**
- **Dienstleisterkontrolle**
- **Audits/Reviews**
- **Incident-Management-Prozess**

➔ **Innerhalb PDCA-Zyklus (ständige Optimierung)**

Deming-Zyklus

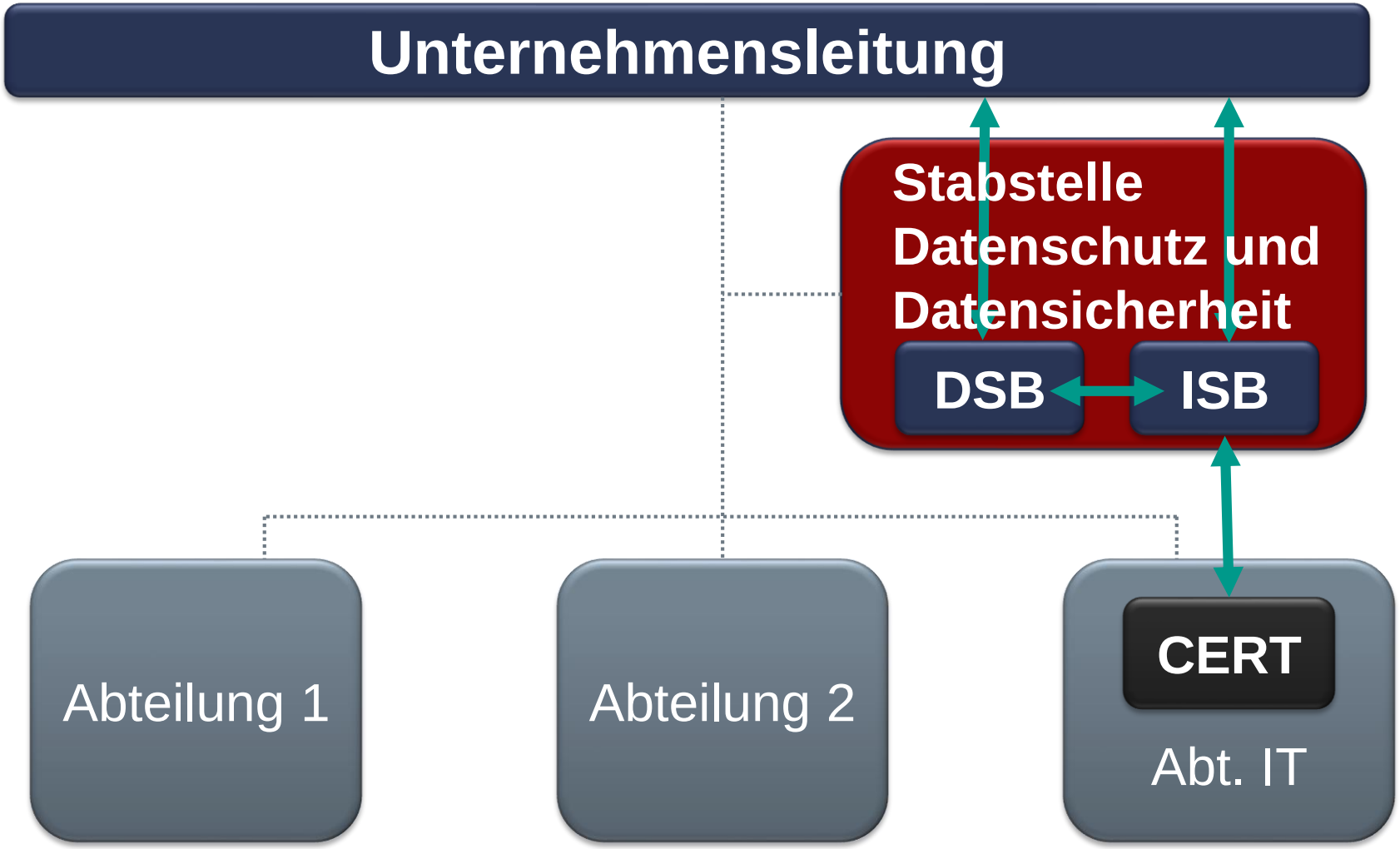


Kernanforderungen an ein integriertes DSMS und ISMS (Ablauforganisation)

Einordnung	Anforderung	Gewichtung
Ablauf-1	Dokumentationserfordernis/ Rechenschaftspflicht	12%
Ablauf-2	Risikoanalyse für Assets und die Intensität des Eingriffs in die Rechte natürlicher Personen	9%
Ablauf-3	Etablierung eines Incident-Management Prozesses	8%
Ablauf-4	Kontinuierliche Weiterentwicklung durch regelmäßige Audits und Reviews des Managementsystems	8%
Ablauf-5	Planung, Durchführung und Dokumentation von Sensibilisierungsmaßnahmen für Mitarbeiter	7%
Ablauf-6	Exakte vertragliche Fixierung von Auftragsverarbeitungen	6%
Ablauf-7	Berücksichtigung der Datenschutzprinzipien Privacy by Design sowie Privacy by Default	6%
Ablauf-8	Besonderer Stellenwert des Mitarbeiterdatenschutzes	5%
Ablauf-9	Etablierung von Prozessen für die Umsetzung von Betroffenenrechten	5%
Ablauf-10	Gemeinsame Maßnahmenkonzeptionierung mit ISM und DSM, Erstellung eines integrierten Informationssicherheits- und Datenschutzkonzepts	4%

Ergebnis der Auswertung von 7 Experteninterviews sowie 10 Informationssicherheits- sowie Datenschutzstandards

Aufbauorganisation und Rollenverteilung



Rollentrennung zur Vermeidung von Interessenskonflikten

- **Datenschutzbeauftragter (DSB) und Informationssicherheitsbeauftragter (ISB) sollten eng zusammenarbeiten (siehe Effizienzgewinne Folie 19)**
- **Der ISB benötigt eine primär technische, der DSB dagegen eine eher technische Qualifikation**
- **ISB und DSB benötigen Organisationskenntnisse**

Kernanforderungen an ein integriertes DSMS und ISMS (Aufbauorganisation)

Einordnung	Anforderung	Gewichtung
Aufbau-1	Enge Zusammenarbeit zwischen ISM und DSM	8%
Aufbau-2	DSB besitzt keine umsetzenden Aufgaben, sondern eine Kontrollfunktion	7%
Aufbau-3	Integriertes Risiko- oder Compliance-Managementsystem als Ziel	6%
Aufbau-4	Unmittelbare Leitungsunterstellung für ISB und DSB mit direktem Berichtsweg	5%
Aufbau-5	Personelle Trennung zwischen ISB und DSB	4%

Ergebnis der Auswertung von 7 Experteninterviews sowie 10 Informationssicherheits- sowie Datenschutzstandards

Vorteile der Integration

- **Erweiterung eines bestehenden Managementsystems**
- **Effizienzgewinne durch gemeinsame**
  - Sensibilisierungsmaßnahmen
  - Dokumentation
  - Prüfung
  - Behandlung von Vorfällen
  - etc.
- **Effektivitätsgewinne durch gezielten Einsatz von Kompetenzen**
- **Umsetzungsnachweis mit positiver Kundenwirkung**

5. Fazit und Diskussion

- **Integriertes DSMS und ISMS erleichtert Einführung und Betrieb des Managementsystems**

- **Rollentrennung zwischen ISB, DSB und IT-Leitung muss erhalten bleiben um Interessenskonflikte zu vermeiden**

- **Dokumentation „steuert“ das Managementsystem und ist Grundlage für die permanente Weiterentwicklung**

Haben Sie noch Fragen?

Welche Erfahrungen haben Sie mit der Integration von Informationssicherheits- und Datenschutzmanagement gemacht?

Quellen

- Bock, K., Ernestus, W., Kramp, M., Konzelmann, L., Naumann, T., Robra, U., Rost, M. Schulz, G., Stoll, J., Vollmer, U., Wilms, M. (2016): Das Standard-Datenschutzmodell, Kühlungsborn 2016

- Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., Stanchev, V. (2016): ISMS core processes: A study, in: Procedia Computer Science, 100. Jg., 2016, S. 339-346

- Kersten, H., Klett, G. (2015): Der IT Security Manager – Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden, 4. Aufl., Wiesbaden 2015

- Loomans, D., Matz, M., Wiedemann, M. (2014): Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, Wiesbaden 2014

- Quiring-Kock, G. (2012): Anforderungen an ein Datenschutzmanagementsystem, in: Datenschutz und Datensicherheit, 36. Jg., 2012, S. 832-836

- Rost, M. (2013): Datenschutzmanagementsystem, in: Datenschutz und Datensicherheit, 37. Jg., 2013, S. 295-300

- Schrahe, D. (2018): ISMS und DSMS als gemeinsamer Managementansatz – Vorgehensmodell anhand der EU-DSGVO und der ISO 27.000-Normenreihe, Masterthesis, FOM München