Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

Informationssicherheitsmanagement
Update aus QM-Perspektive

GQMGaktuell

Onlineveranstaltung, 22.03.2022

Publikationen mit Erstautorenschaft (Auszug)

Kritische Anmerkungen zu Urteilen des SG Dresden (S 38 KR 674/1 und S 18 KR 530/18) aus dem Jahr 2020
Becker A, Gärtner E
das Krankenhaus. 2021; 113 (11): 1028–1044
+ PDF 457,5 KB | 17 Seiten

Anforderungen an die Informationssicherheit in deutschen Krankenhäusern (Teil 2)
Becker A
Journal für Medizin- und Gesundheitsrecht. 2021; 6 (2): 6–11
+ PDF 165,5 KB | 6 Seiten

Anforderungen an die Informationssicherheit in deutschen Krankenhäusern (Teil 1)
Becker A
Journal für Medizin- und Gesundheitsrecht. 2021; 6 (1): 39–48
+ PDF 544,5 KB | 11 Seiten

Anmerkungen und Empfehlungen zu Interhospitalverlegungen intensivmedizinischer Patienten
Becker A, Gärtner E
Ärzteblatt Rheinland-Pfalz. 2021; 7: 19–23
+ PDF 1,2 MB | 5 Seiten

Handwerkliche Fehler im § 75b SGB V als Grundlage der KBV-Richtlinie über die Anforderungen zur Gewährleistung der IT-Sicherheit – Auswirkungen für medizinische Labore
Becker A, Gärtner E
Veröffentlicht im Profil des Erstautors bei Linkedin am 25.05.2021
+ PDF 170,2 KB | 10 Seiten

Der neue § 75c SGB V.
Anforderungen an die Informationssicherheit in Krankenhäusern
Becker A, Gärtner E
das Krankenhaus. 2021; 113 (4): 292–310
+ PDF 397,7 KB | 10 Seiten

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen (BSIG)

Betreiber Kritischer Infrastrukturen sind verpflichtet, [….] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. […]

§ 75c IT-Sicherheit in Krankenhäusern (SGB V)

[…] sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

§ 75b Richtlinie zur IT-Sicherheit in der vertragsärztlichen […] Versorgung

[…] Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung […].

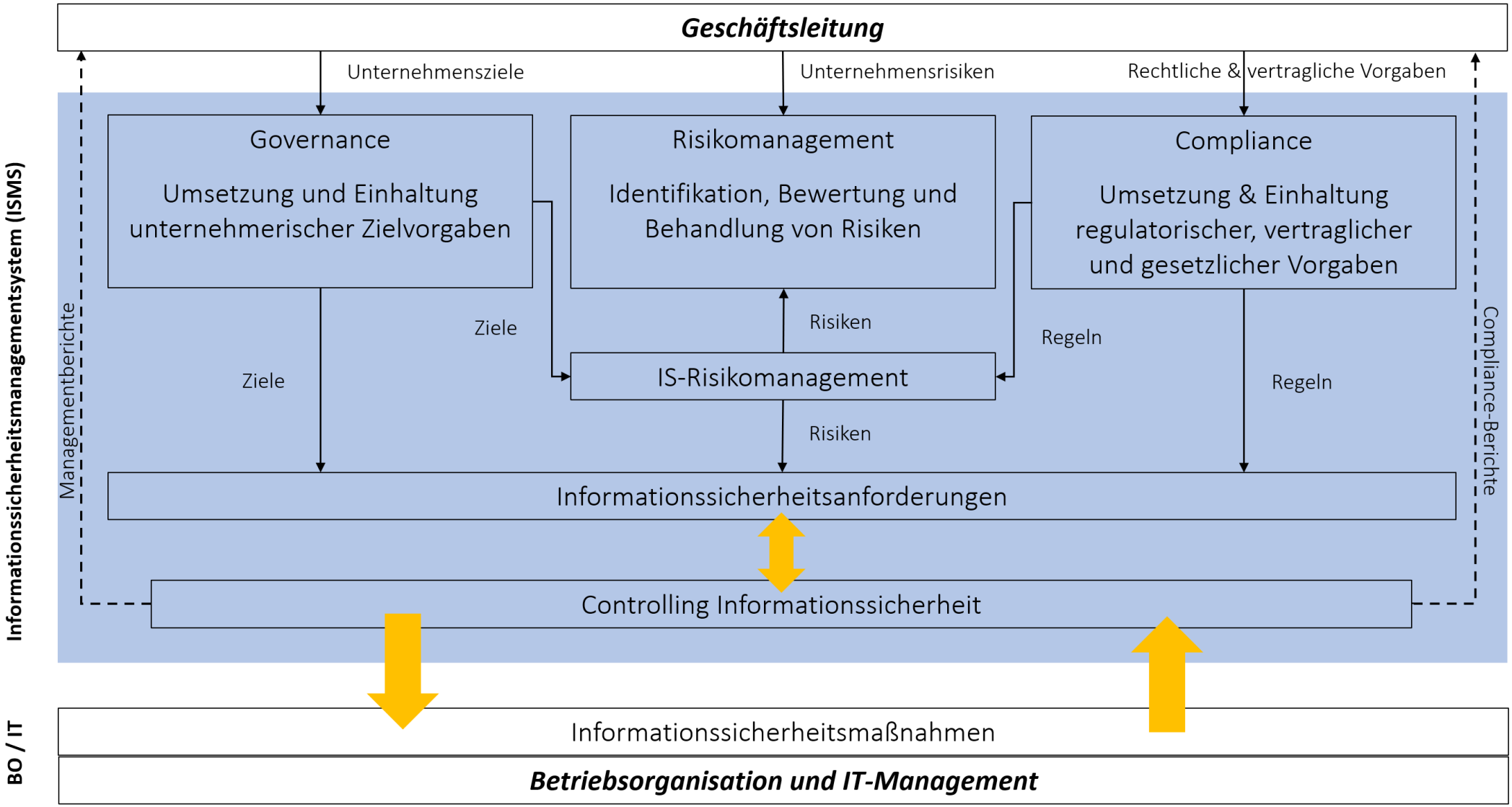
IT-Sicherheit und Informationssicherheit

- Als IT-Sicherheit oder IT-Security definiert man gemeinhin den Schutz von IT-Systemen vor Schäden und Bedrohungen. Das erstreckt sich von der einzelnen Datei über Computer, Netzwerke, Cloud-Dienste bis hin zu ganzen Rechenzentren.

- Die DIN EN ISO/IEC 2700x-Normenreihe spricht nur von Informationssicherheit („Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Information“, ggf. ergänzt um weitere Schutzziele).

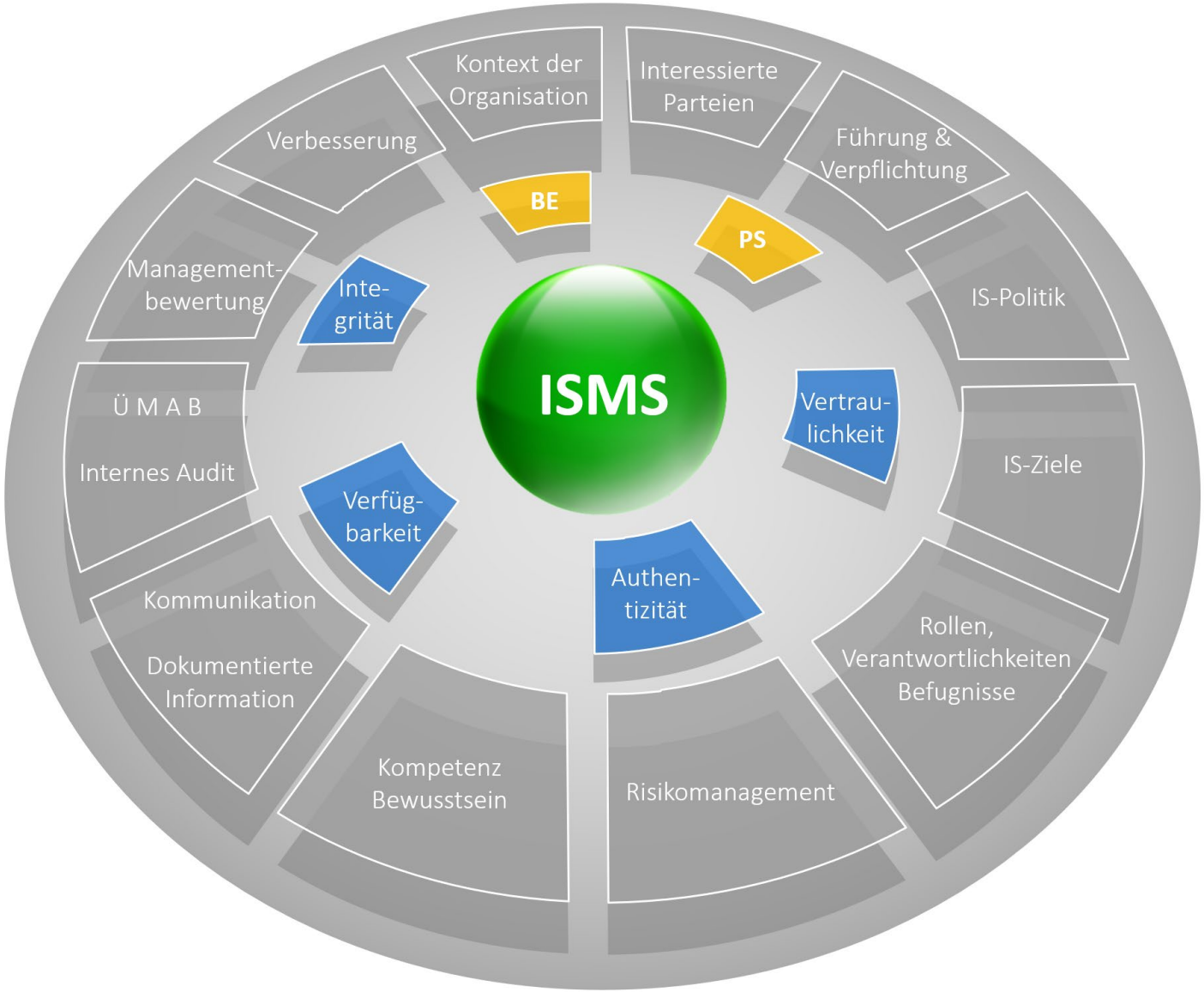
- „Ziel der „Informationssicherheit“ ist es, sowohl die Informationen selbst als auch die Prozesse, Anwendungen, Systeme, Services, Kommunikation und Einrichtungen zu schützen, welche die Informationen enthalten, verarbeiten, speichern, transportieren oder liefern.“ (B3S, Seite 16)

- „Informationssicherheit dient dem Schutz von (digitalen und nicht digitalen) Informationen, sie umfasst dabei die logische und technische Sicherheit, physische Sicherheit, organisatorische Maßnahmen, Betriebsverfahren, Notfallplanung, Vertragsbeziehungen, inkl. Outsourcing und wichtige Schnittstellen, wie IT-Management, Datenschutz, Risikomanagement und Personal.“ (B3S, Seite 43/44)



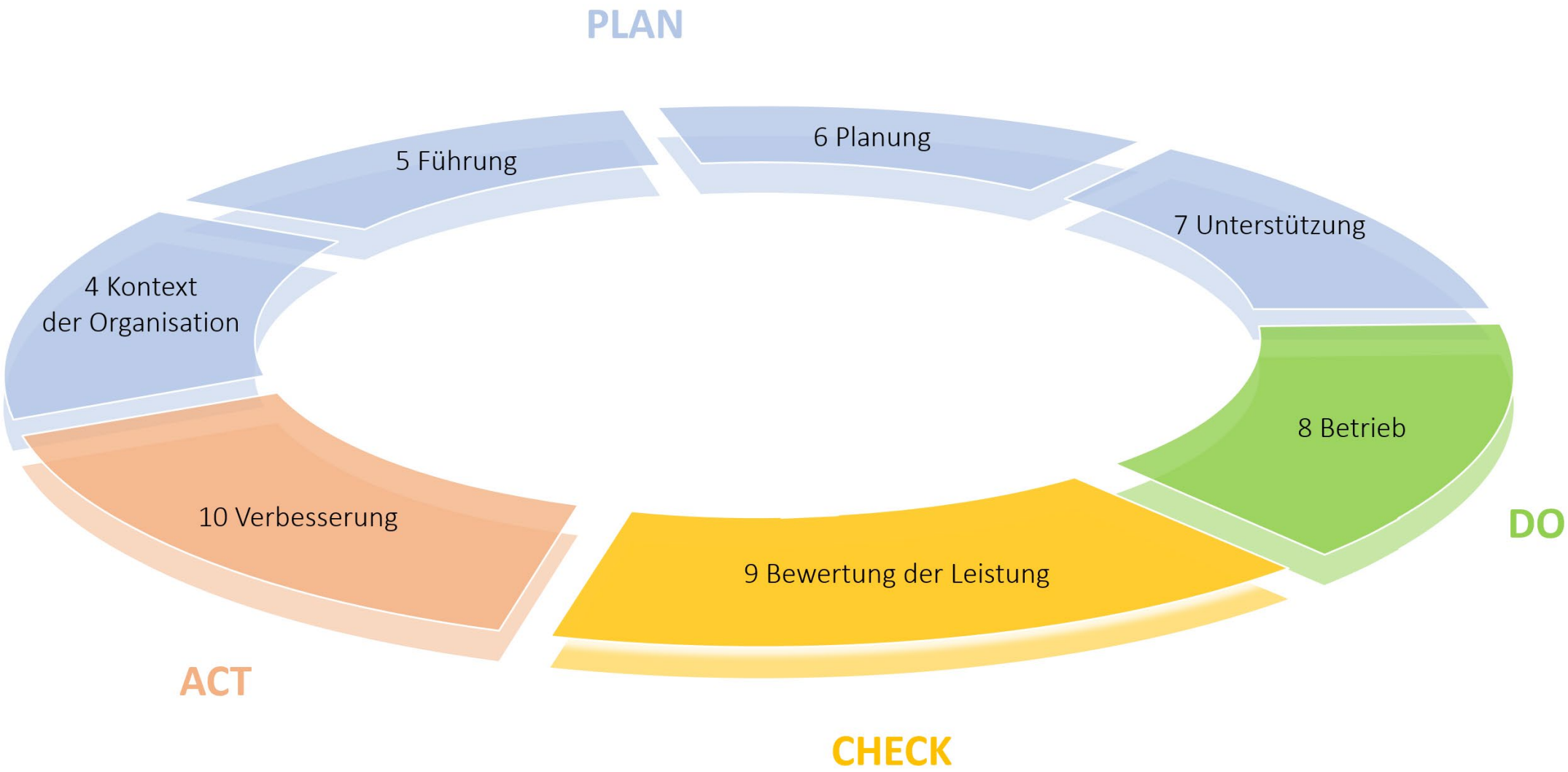
Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

DIN EN ISO/IEC 27001



Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

DIN EN ISO/IEC 27001



Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

Leitsätze zur Prüfung eins ISMS

[1] Das ISMS mit allen Bestandteilen muss erkennbar eingeführt sein und **erkennbar gelebt** werden.

[2] Daraus folgt, dass in der Organisation bestimmte Merkmale in der dokumentierten und gelebten Praxis feststellbar sind, die für einen externen Beobachter den **Unterschied zwischen dieser Organisation und einer Organisation ohne ISMS** ausmachen.

[3] Ein effektives und effizientes ISMS kann natürlich in bestehende Systeme integriert werden, es muss jedoch als **funktionales Managementsystem im Sinne des „Lenken und Leiten mit Fokus auf Informationssicherheit“** erkennbar sein.

[4] Es geht bei der Einführung und Aufrechterhaltung des ISMS **nicht um die Frage, wie das ISMS mit „möglichst geringstem Aufwand“** umgesetzt bzw. in bestehende Systeme integriert wer-den kann.

[5] Einführung und Aufrechterhaltung sollen unter dem Merkmal der „**Angemessenheit**“ betrachtet werden, dabei geht es insbesondere um die Angemessenheit der TOM im konkreten Kontext der Organisation, der durch den Geltungs-/Anwendungsbereich abgebildet wird.

Gemeinsamer Bundesausschuss

Richtlinie

des Gemeinsamen Bundesausschusses
über grundsätzliche Anforderungen an ein
einrichtungsinternes Qualitätsmanagement für
Vertragsärztinnen und Vertragsärzte,
Vertragspsychotherapeutinnen und
Vertragspsychotherapeuten, medizinische
Versorgungszentren, Vertragszahnärztinnen und
Vertragszahnärzte sowie zugelassene Krankenhäuser

(Qualitätsmanagement-Richtlinie/QM-RL)

in der Fassung vom 17. Dezember 2015
veröffentlicht im Bundesanzeiger (BAnz AT 15.11.2016 B2)
in Kraft getreten am 16. November 2016

zuletzt geändert am 17. September 2020
veröffentlicht im Bundesanzeiger (BAnz AT 08.12.2020 B2)
in Kraft getreten am 9. Dezember 2020

§ 3 Grundelemente

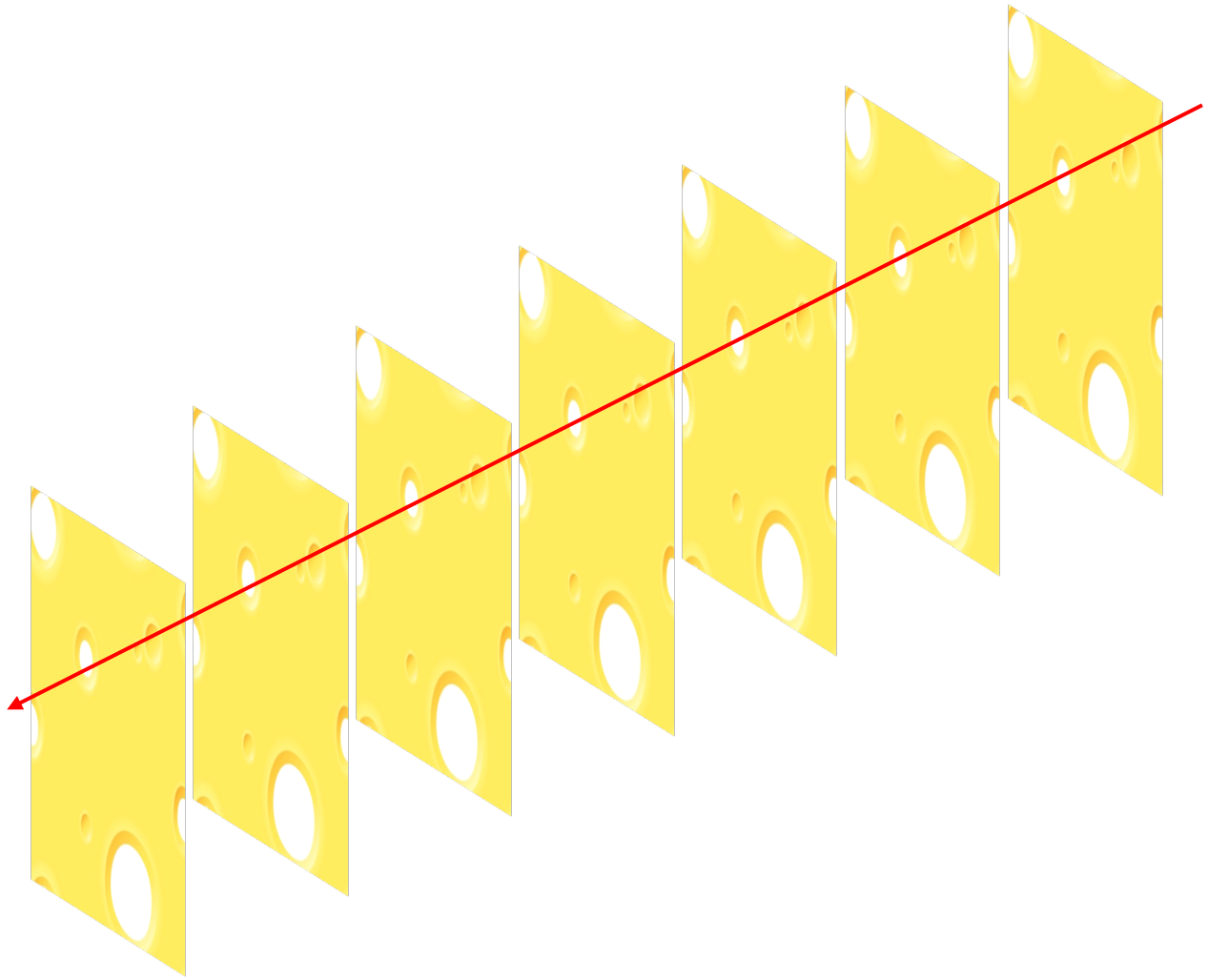
Qualitätsmanagement umfasst insbesondere folgende grundlegenden Elemente:

- Patientenorientierung einschließlich Patientensicherheit
- Mitarbeiterorientierung einschließlich Mitarbeitersicherheit
- Prozessorientierung
- Kommunikation und Kooperation
- Informationssicherheit und Datenschutz
- Verantwortung und Führung

Methoden und Instrumente (§ 4 Abs. 1 QM-RL, Auszug)

- Messen und Bewerten von Qualitätszielen
- Erhebung des Ist-Zustandes und Selbstbewertung (insbesondere Audits)
- Regelung von Verantwortlichkeiten und Zuständigkeiten
- Prozess- bzw. Ablaufbeschreibungen
- Schnittstellenmanagement
- Risikomanagement

Angemessene organisatorische und technische Vorkehrungen

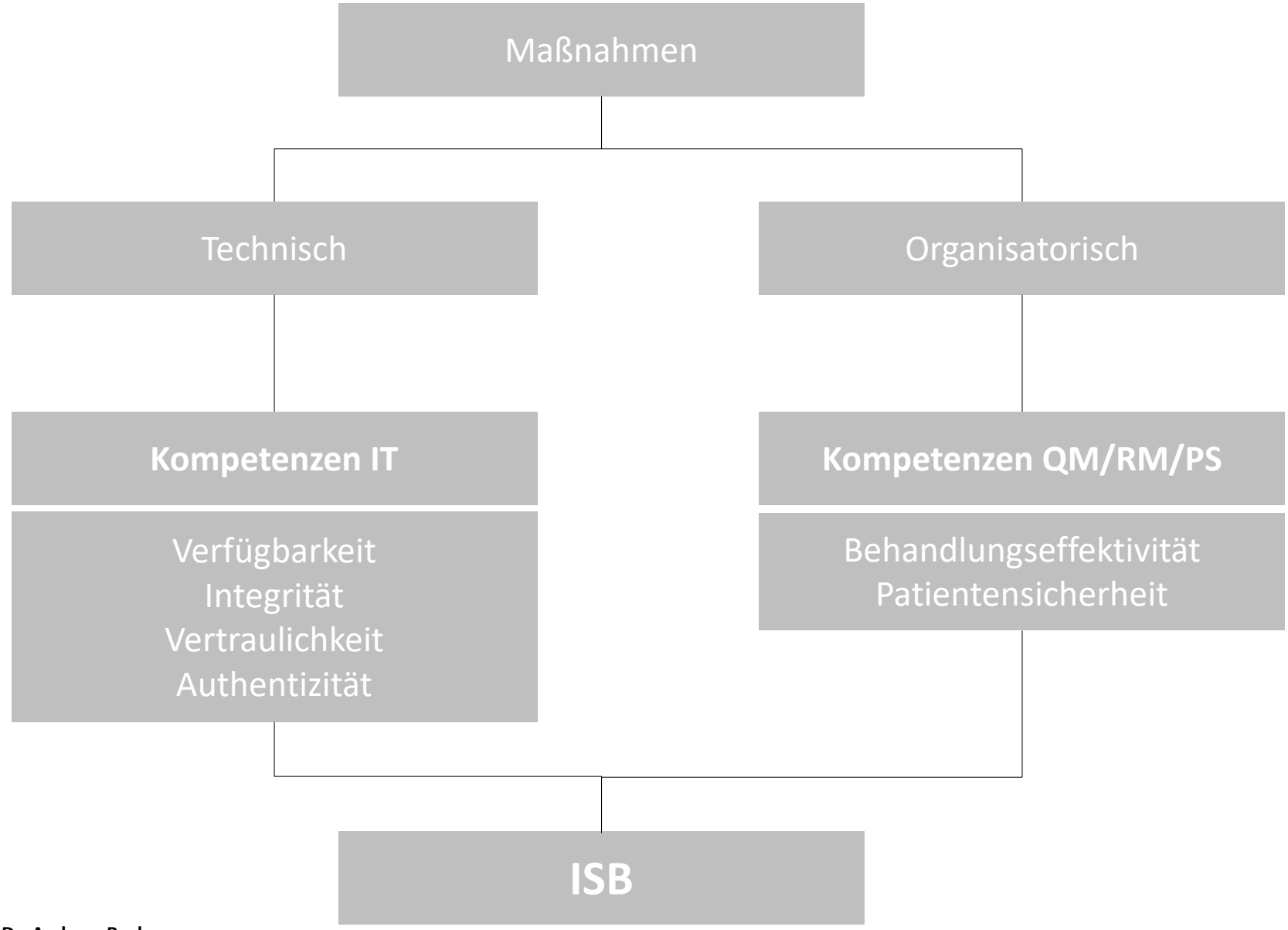


Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

Erfahrung aus der Beratungs- und Prüfungspraxis

- Schwerpunkt bisher: technische Maßnahmen.

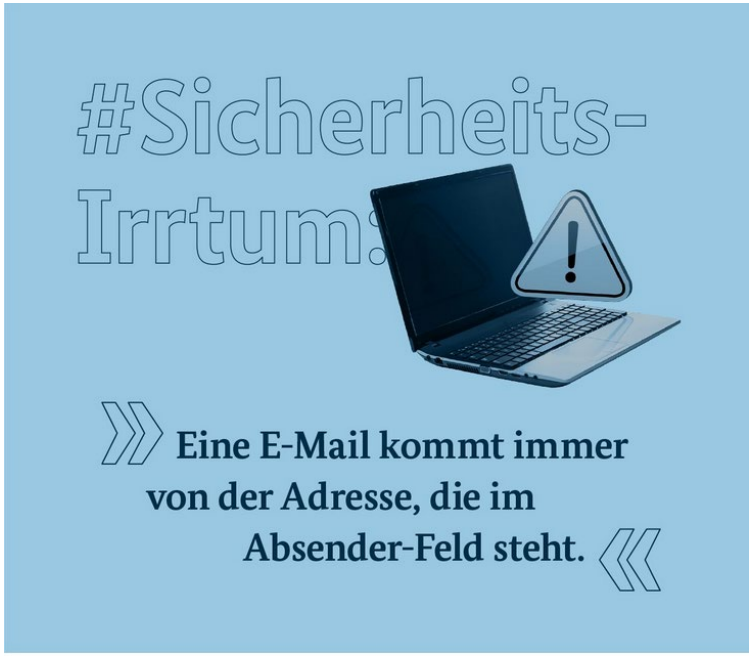
Eine Übersicht



Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

Top five attack vectors to look out for in 2022

- **Social engineering**
- Stolen credentials
- API Exploits (Application Programming Interface)
- Remote Technology
- IoT Devices



Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger für Qualitäts-, Informationssicherheits- und Risikomanagement in Krankenhäusern

https://securityaffairs.co/wordpress/123636/security/top-5-attack-vectors-2022.html (Zugriff: 21.03.2022)

Erfahrung aus der Beratungs- und Prüfungspraxis

- Schwerpunkt bisher: technische Maßnahmen.

- Der Faktor Mensch wird bei den Planungen und Maßnahmen nicht angemessen adressiert.

- Bei den organisatorischen Maßnahmen werden bestimmte Themen bisher nicht angemessen berücksichtigt, sie werden oftmals als „nachgeordnet“ betrachtet:
  - Übungen auf Leitungsebene
  - Bewusstseinsbildende bzw. –fördernde Maßnahmen
  - **Planungen für den Ausfall branchenspezifischer Systeme (z. B. Telemetrie, CTG)**

Prof. Dr. Andreas Becker
Öffentlich bestellter und vereidigter Sachverständiger
für Qualitäts-, Informationssicherheits- und
Risikomanagement in Krankenhäusern

Vielen Dank!

T +49 2205 920 460
F +49 2205 920 462
M +49 172 29 88 040
E becker@becker-sachverstaendiger.de
W www.becker-sachverstaendiger.de

Prof. Dr. Andreas Becker
Nonnenweg 120a
51503 Rösrath