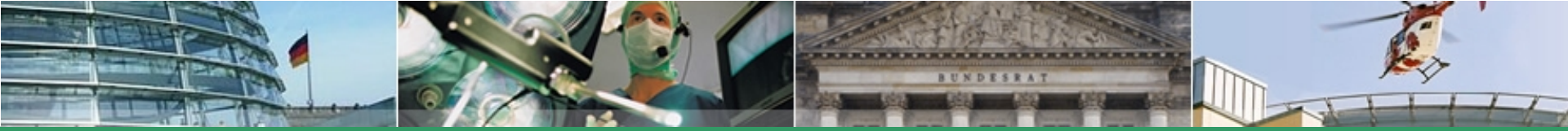


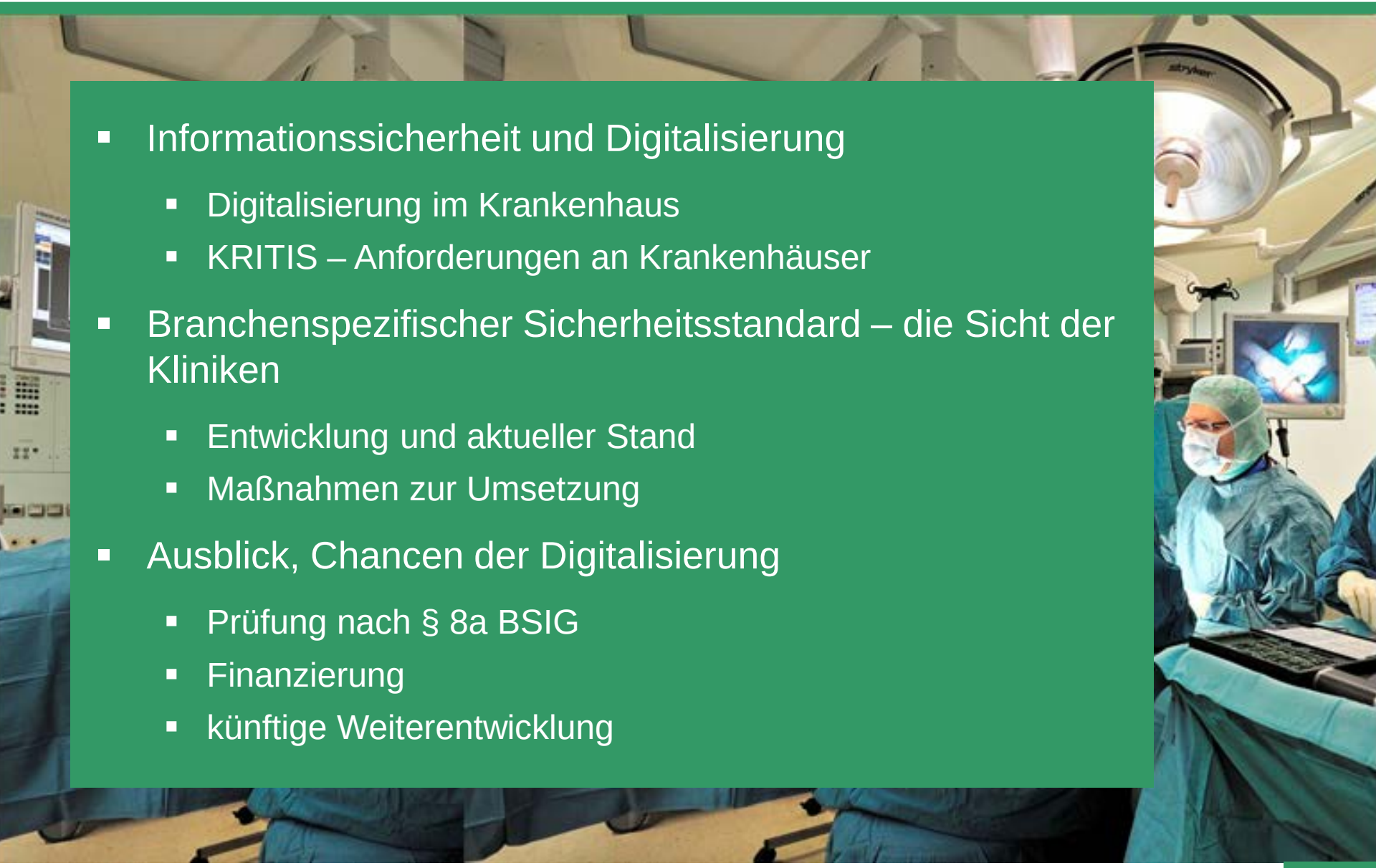
KRITIS – die Sicht der Kliniken, Chancen der Digitalisieurng

7. Mai 2019 - Wiesbaden

Markus Holzbrecher-Morys
Stellv. Geschäftsführer (IT, Datenaustausch, eHealth)

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Agenda



- Informationssicherheit und Digitalisierung
  - Digitalisierung im Krankenhaus
  - KRITIS – Anforderungen an Krankenhäuser
- Branchenspezifischer Sicherheitsstandard – die Sicht der Kliniken
  - Entwicklung und aktueller Stand
  - Maßnahmen zur Umsetzung
- Ausblick, Chancen der Digitalisierung
  - Prüfung nach § 8a BSIG
  - Finanzierung
  - künftige Weiterentwicklung

Herausforderung für Krankenhäuser

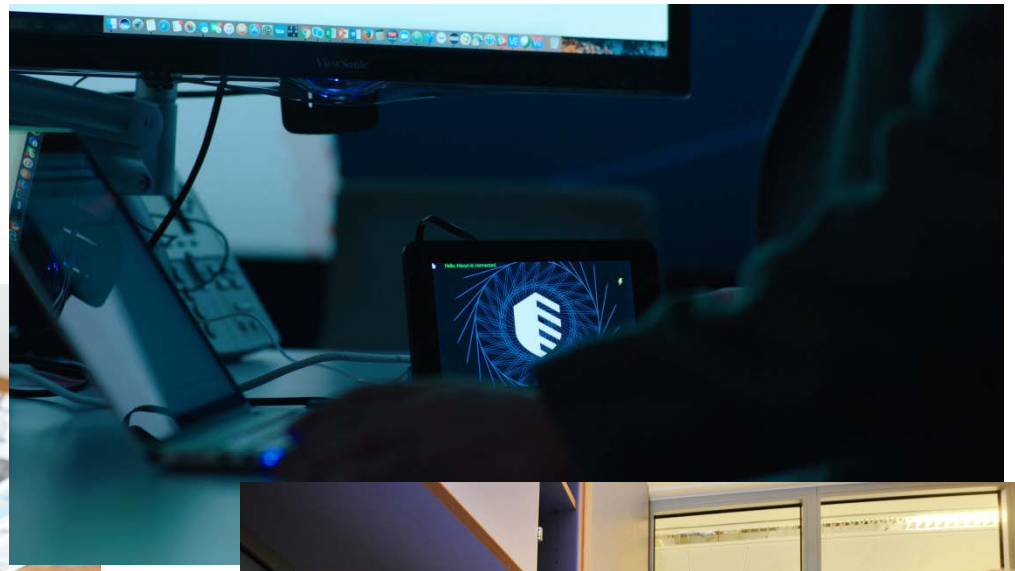
„IT-Sicherheit? Wir haben ganz andere Probleme!“

Von Olaf Kosinsky - Eigenes Werk, CC BY-SA 3.0 de, https://commons.wikimedia.org/w/index.php?curid=66705996

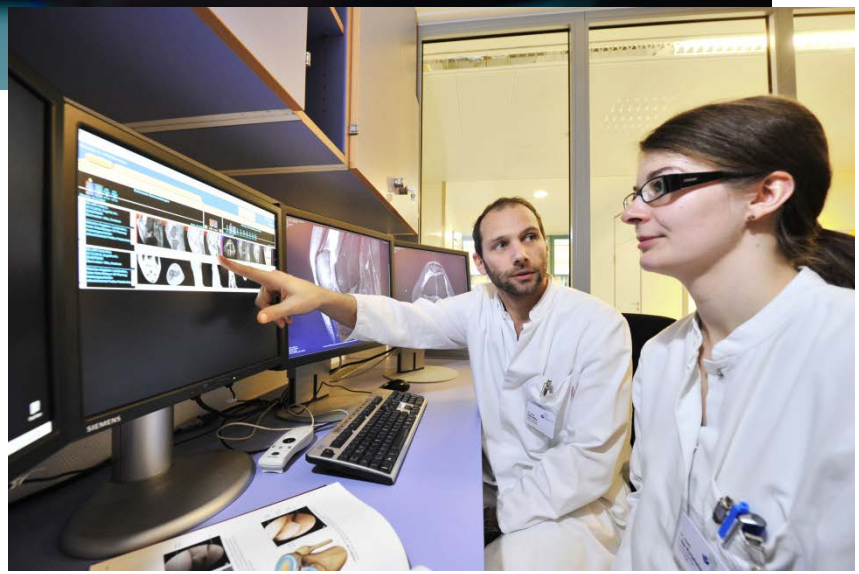
- Koalitionsvertrag bleibt in Bezug auf Digitalisierung weit hinter den Erwartungen zurück
- Ausgliederung der Pflege bedeutet „Meteoriteneinschlag“ im DRG-System
- Investitionsfinanzierung dürfte noch prekärer ausfallen
- Personalbedarf kann an vielen Stellen nicht adäquat gedeckt werden

Evolution der Informationstechnik

…in Wissenschaft und Forschung



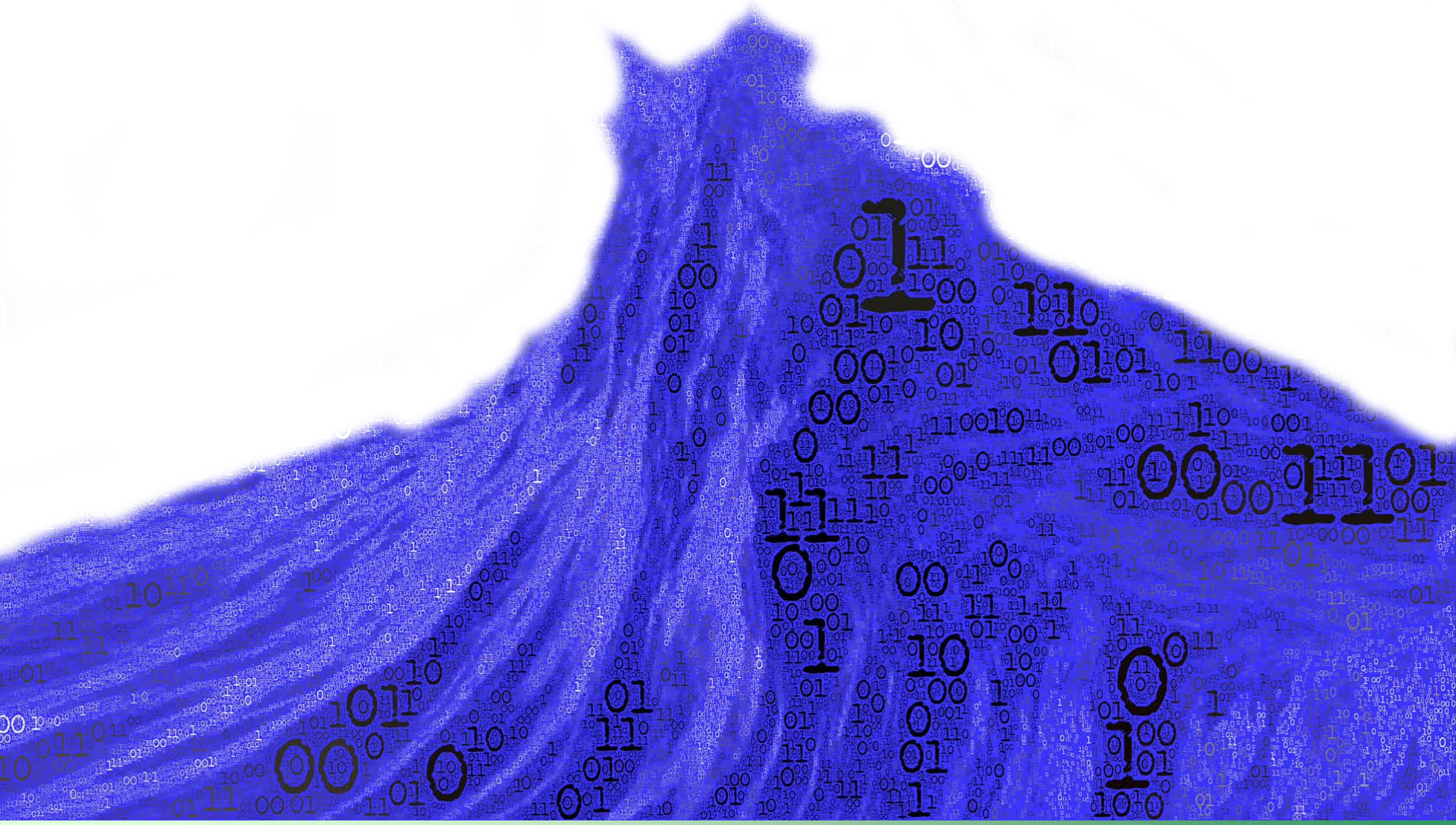
im privaten Bereich…



…im Krankenhaus

Digitalisierung im Gesundheitswesen

DEUTSCHE KRANKENHAUS GESELLSCHAFT

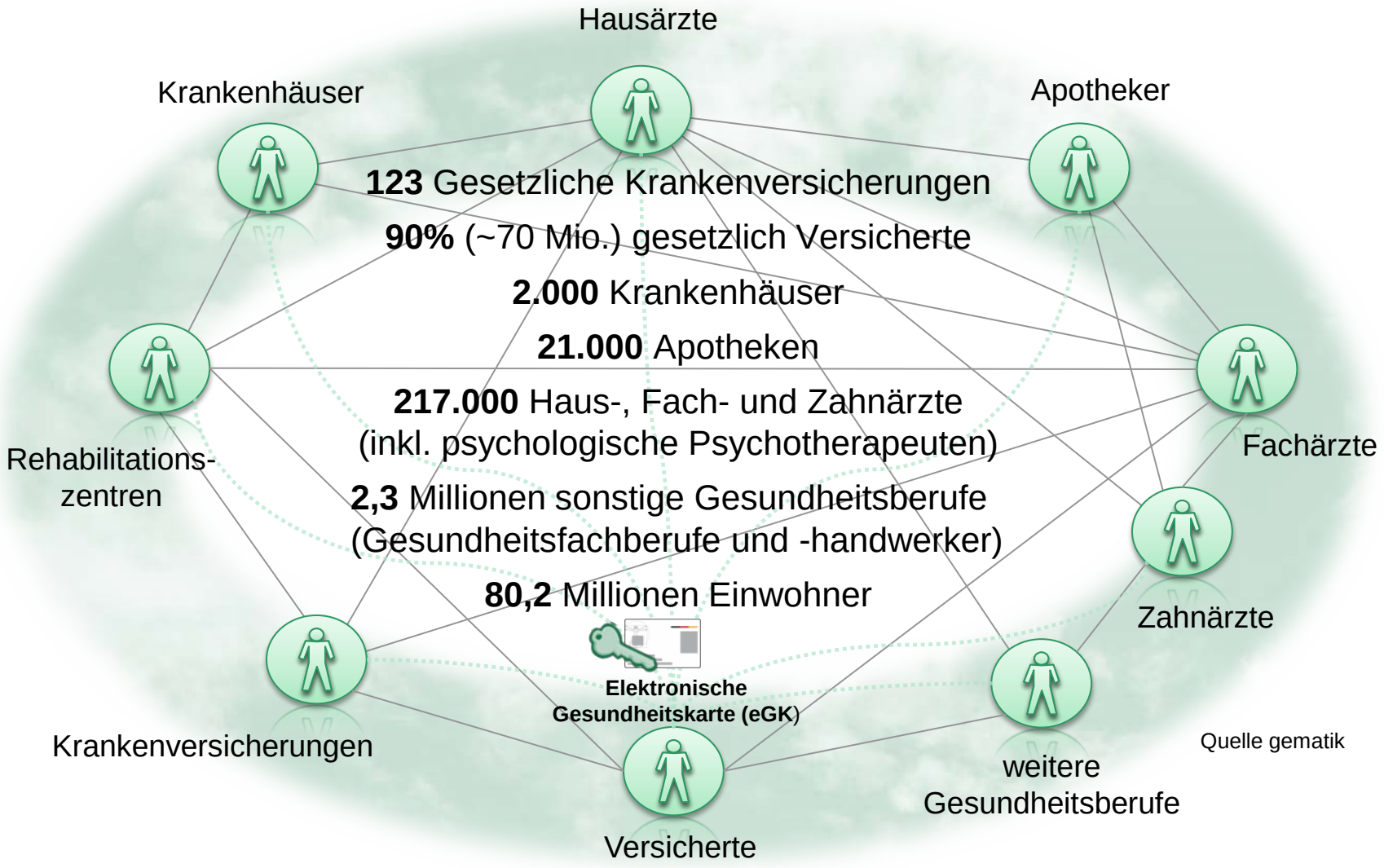


Digitalisierung im Gesundheitswesen - Trends

iOS 11.3 Austausch von Patientenakten zwischen Patienten und Leistungserbringern

Apple baut Klinik für eigene Mitarbeiter

Vernetzung im Gesundheitswesen



Quelle gematik

DEUTSCHE KRANKENHAUS GESELLSCHAFT

„Größter Erpresser-Software Angriff der Geschichte“

Quelle: www.spiegel.de vom 13.5.2017

Tens of thousands of computers in 99 countries have been infected by a ransomware virus which extorts users by blocking Windows files and demanding payment to restore access.

Quelle: www.rt.com vom 13.5.2017

Veränderte Bedrohungslage

Ransomware

Cyberkriminalität

Datendiebstahl

Cyberterrorismus

Offenbarung von Patientendaten

Notfallversorgung bei Großschadenslagen (MANV)

Trojaner

Zero-Day-Exploits

Social Engineering

DoS (Denial of Service)

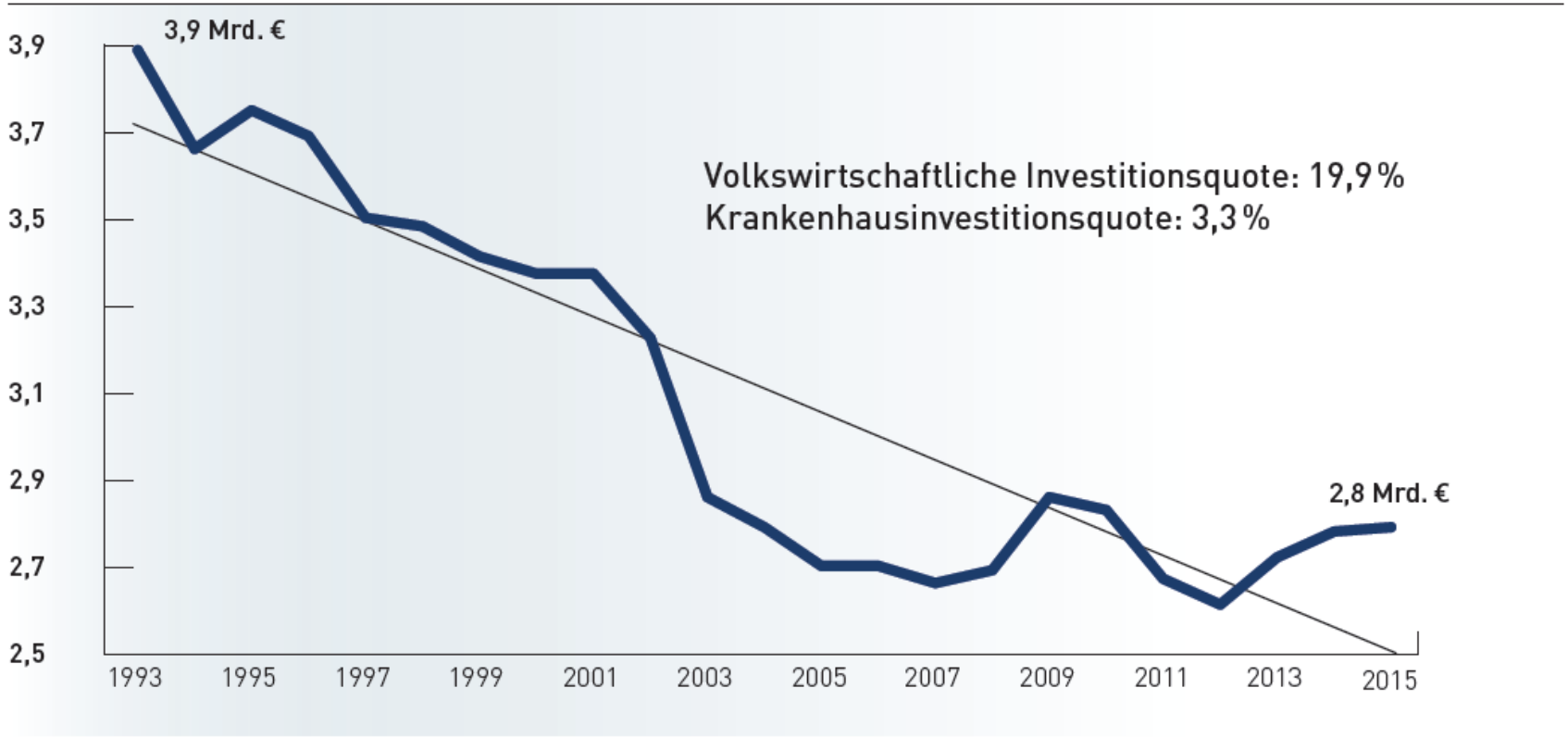
Advanced Persistent Threats

der Nutzer selbst

Krankenhausinvestitionsquote

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Entwicklung der Investitionsförderung seit 1993



Quelle: AOLG

Krankenhäuser sind in vielen Regionen der größte Arbeitgeber und ein zuverlässiger Beschäftigungsmotor!

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Informationssicherheit

Schutz von Daten und Informationen jeglicher Art

IT-Sicherheit

Primärer Schutz elektronisch gespeicherter Informationen und deren Verarbeitung

Datenschutz

Schutz personenbezogener Daten

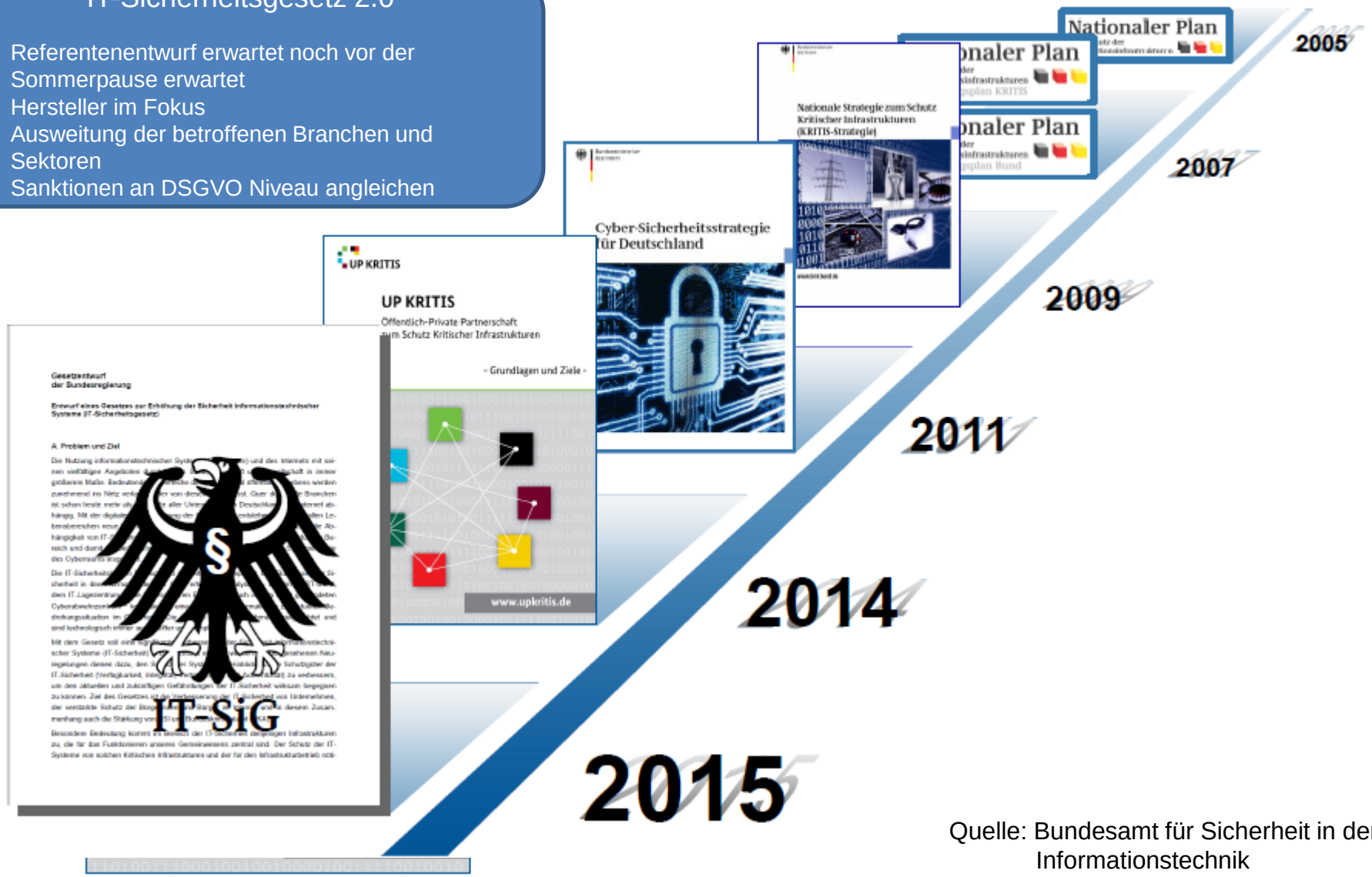
z.B. Verfahrensverzeichnis

Das IT-Sicherheitsgesetz

DEUTSCHE KRANKENHAUS GESELLSCHAFT

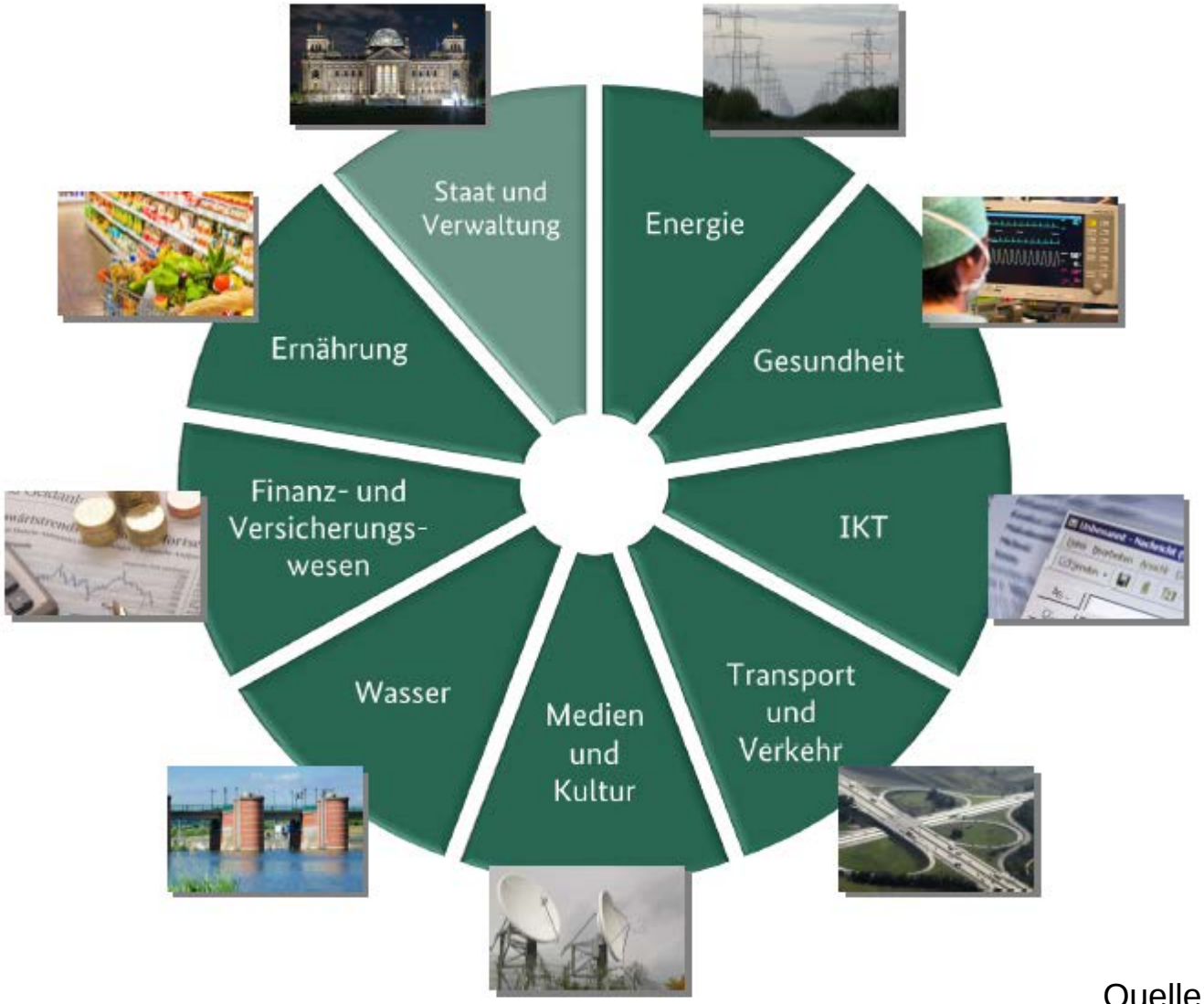
IT-Sicherheitsgesetz 2.0

- Referentenentwurf erwartet noch vor der Sommerpause erwartet
- Hersteller im Fokus
- Ausweitung der betroffenen Branchen und Sektoren
- Sanktionen an DSGVO Niveau angleichen



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Die Kritischen Infrastrukturen Deutschlands



Quelle: kritis.bund.de

BSI-Gesetz: Zusammenfassung

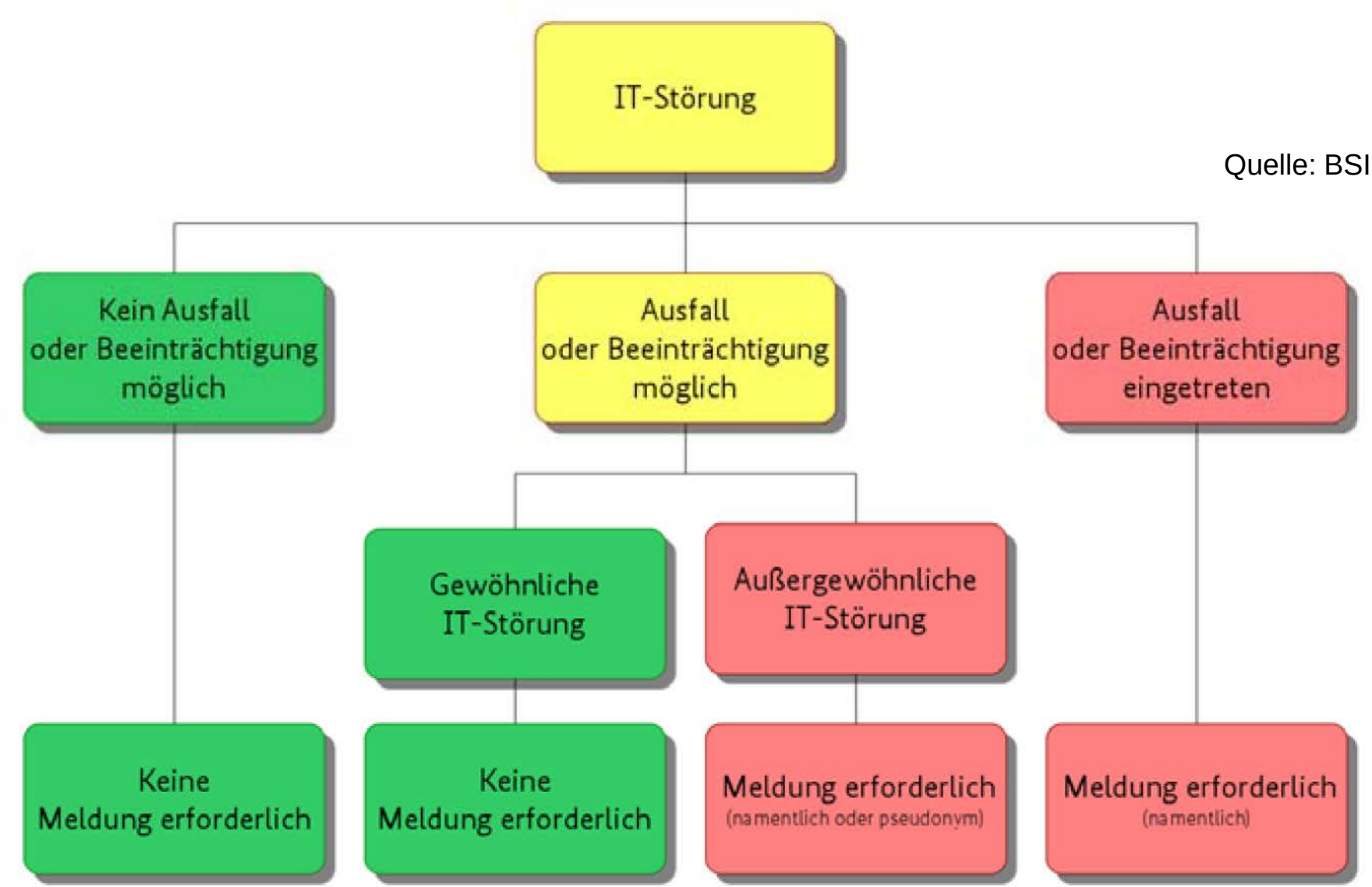
- Betreiber sind nach § 8a Abs. 1 BSIG zur **Umsetzung von angemessenen Sicherheitsmaßnahmen** verpflichtet („Stand der Technik“)
- Betreiber müssen nach § 8a Abs. 3 BSIG die **Umsetzung** entsprechender Maßnahmen **regelmäßig** (spätestens alle 2 Jahre) **nachweisen**
- das **BSI** nimmt nach § 8b BSIG die Aufgabe einer **zentralen Meldestelle** für sicherheitsrelevante Informationen wahr
- **Betreiber** haben nach § 8b Abs. 2 BSIG ein **Informationsrecht** gegenüber dem BSI
- **Betreiber müssen** nach § 8b Abs. 4 BSIG IT-Störungen an das BSI **melden**

BSI-KritisVO: Zusammenfassung

Festlegungen für die Branche „medizinische Versorgung“

- Anlagenkategorie: Krankenhäuser
- Bemessungskriterium: Anzahl vollstationärer Behandlungen
- Schwellenwert: 30.000 / Jahr
- ambulante Versorgung derzeit nicht betrachtet (keine relevante Größenordnung einzelner Betreiber)
- Föderalismus: Standort eines Krankenhauses nicht einheitlich
  (Verzeichnis nach § 293 Abs. 6 SGB V?)
- ca. 5 – 10 % aller Kliniken betroffen

Meldepflichten nach § 8b BSIG



Quelle: BSI

Entwicklung B3S – Zeitlicher Verlauf

Mai 2016: BSI-Kritisverordnung („Korb 1“)

Mai 2017: 1. Änderungsverordnung BSI-KritisV – „Korb 2“ [1)]
Beauftragung der DKG zur Erstellung eines B3S

November 2017: Kontaktstelle einrichten (§ 8b Abs. 3 BSIG) Meldung erheblicher Störungen an BSI [1)]

Freigabe des B3S-Entwurfs für die Abstimmung mit BAK / BSI: **März 2018**

Antrag auf Eignungsfeststellung bei BSI: **18. Dezember 2018**

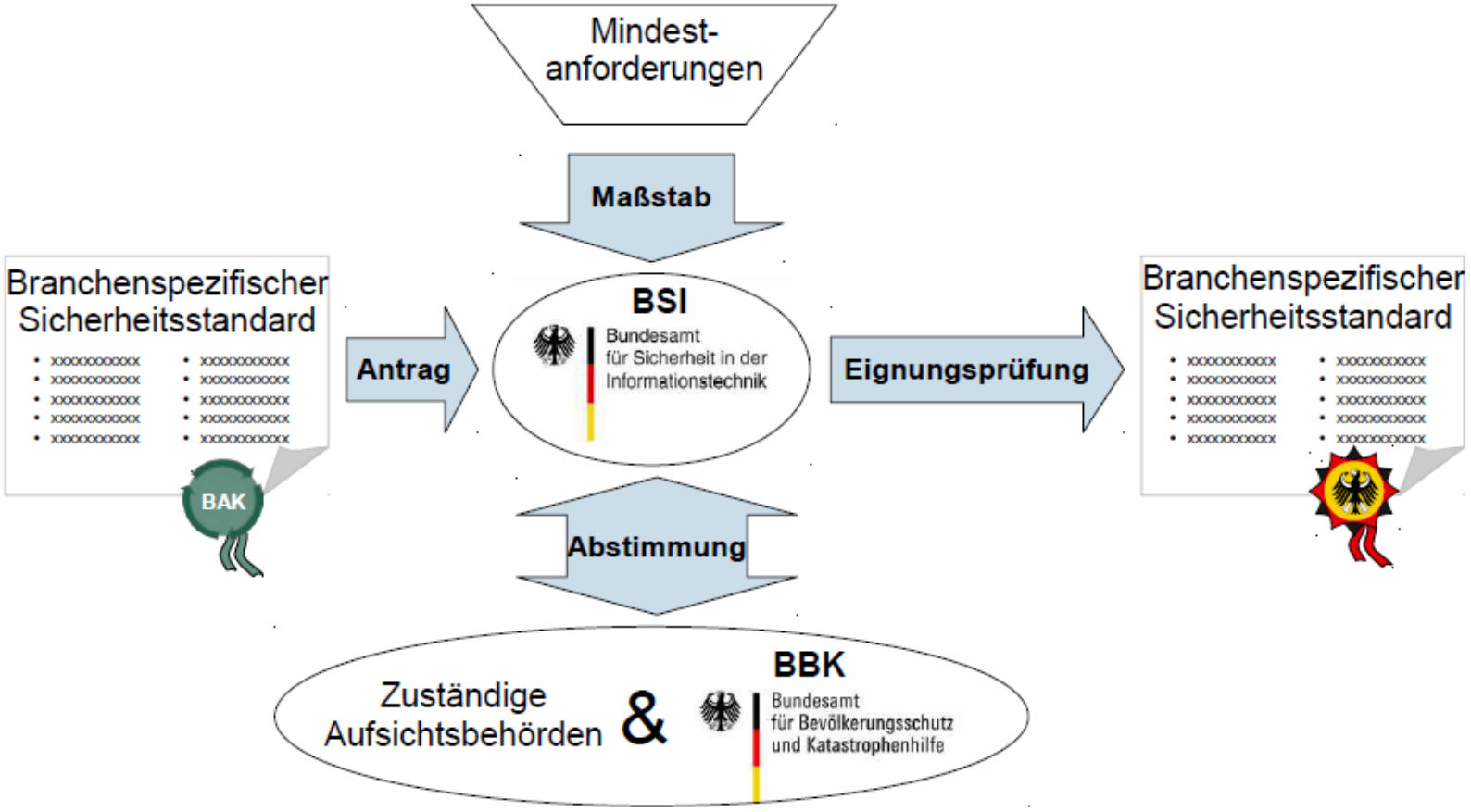
Nachweis geeigneter Maßnahmen (§ 8a Abs. 3 BSIG): **bis 30. Juni 2019**

Nachweispflichten bei Überschreitung des Schwellenwerts in **2 aufeinander folgenden Jahren**

[1)] gültig für Schwellenwertüberschreitung in 2016

Entwicklung des B3S - Eignungsprüfung

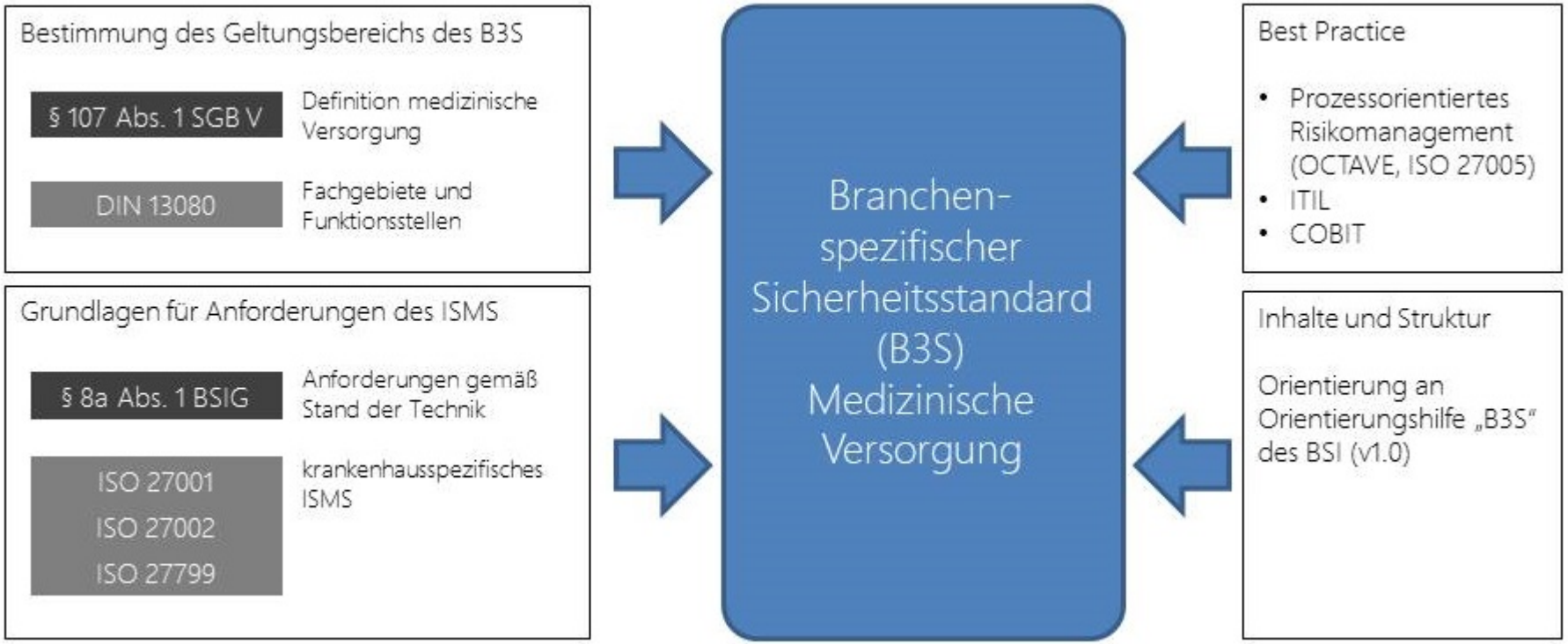
Branchenverbände können branchenspezifische Sicherheitsstandards (B3S) vorschlagen (§ 8a Abs. 2 BSI-Gesetz)



Quelle: BSI

Entwicklung des B3S

- im Zuge der 1. Änderungsverordnung der BSI- KritisVO erfolgte Beauftragung der Geschäftsstelle der DKG durch ihre Gremien mit der Erarbeitung eines B3S (2017)
- aktive Einbeziehung des BAK „Medizinische Versorgung“ (Erarbeitung, Kommentierung)



Standard-Risikomanagement-Prozessmodell

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Umsetzung des Standard-Risikomanagement-Prozessmodelles

1. Informationswerte (Risikoobjekte) und Verantwortliche (Risiko-Eigentümer) ermitteln
2. Kritikalität der Informationswerte festlegen
3. Kriterien zur Identifikation von Risiken festlegen
4. Bedrohungen und Schwachstellen identifizieren
5. Risiken bewerten (Eintrittswahrscheinlichkeit und Schadenspotenzial)
6. Risiken behandeln (akzeptieren, vermeiden, transferieren oder reduzieren)
7. Risiken kommunizieren und überwachen

B3S definiert zunächst allgemeine Anforderungen an die Umsetzung des Risikomanagements (Management-Rahmen), anschließend werden die Teilprozesse des Standard-Risikomanagement-Prozesses im Einzelnen dargestellt.

Schutzziele (allgemein)

- VEFÜGBARKEIT
  von Dienstleistungen, Funktionen eines Informationssystems, IT-Systems, IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- INTEGRITÄT
  bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Bei AUTHENTISCHEN Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.
- VERTRAULICHKEIT
  stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.

Schutzziele (branchenspezifisch)

- PATIENTENSICHERHEIT
  als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen meint auch die Vermeidung einer nachhaltigen psychischen Belastung.

- BEHANDLUNGSEFFEKTIVITÄT
  stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.

kritische branchenspez. Technik & Software

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Gefährdungsanalyse für kritische branchenspezifische Technik und Software

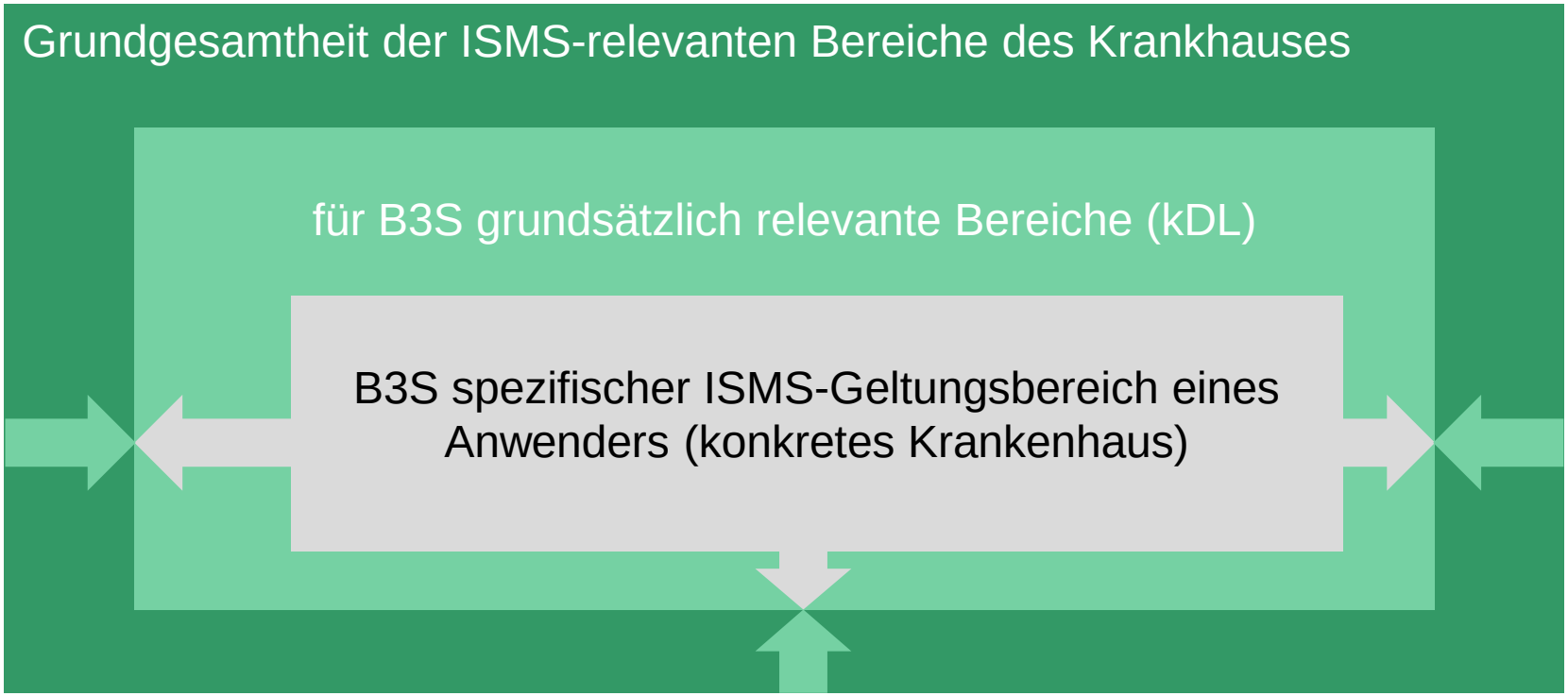
- Krankenhausinformationssystem (KIS)
- Laborinformationssystem (LIS)
- Radiologieinformationssystem (RIS)
- Picture Archive and Communication System (PACS)
- Dokumentenmanagementsystem (DMS/ECM)
- Medizintechnik
- Transportlogistik
- Versorgungsdienste / Versorgungstechnik
- Sonder- und Spezialsoftwarelösungen

IT-Systemlandschaft in KH nach Kritikalität

- Bewertung der Kritikalität von Systemen auf Grundlage der Zeitdauer, in der nach Ausfall oder Beeinträchtigung des Systems noch keine relevante Einschränkungen der med. Versorgung zu erwarten sind
  - Klasse 1: Ausfall der Systeme kann nur kurzfristig kompensiert werden
  - Klasse 2: Ausfall der Systeme kann mittelfristig kompensiert werden
  - Klasse 3: Ausfall der Systeme kann längerfristig kompensiert werden
- differenzierte Anforderungen entsprechend der individuellen Kritikalität
- konkrete Ausgestaltung der Zeitspannen nach individuellen Erfahrungswerten

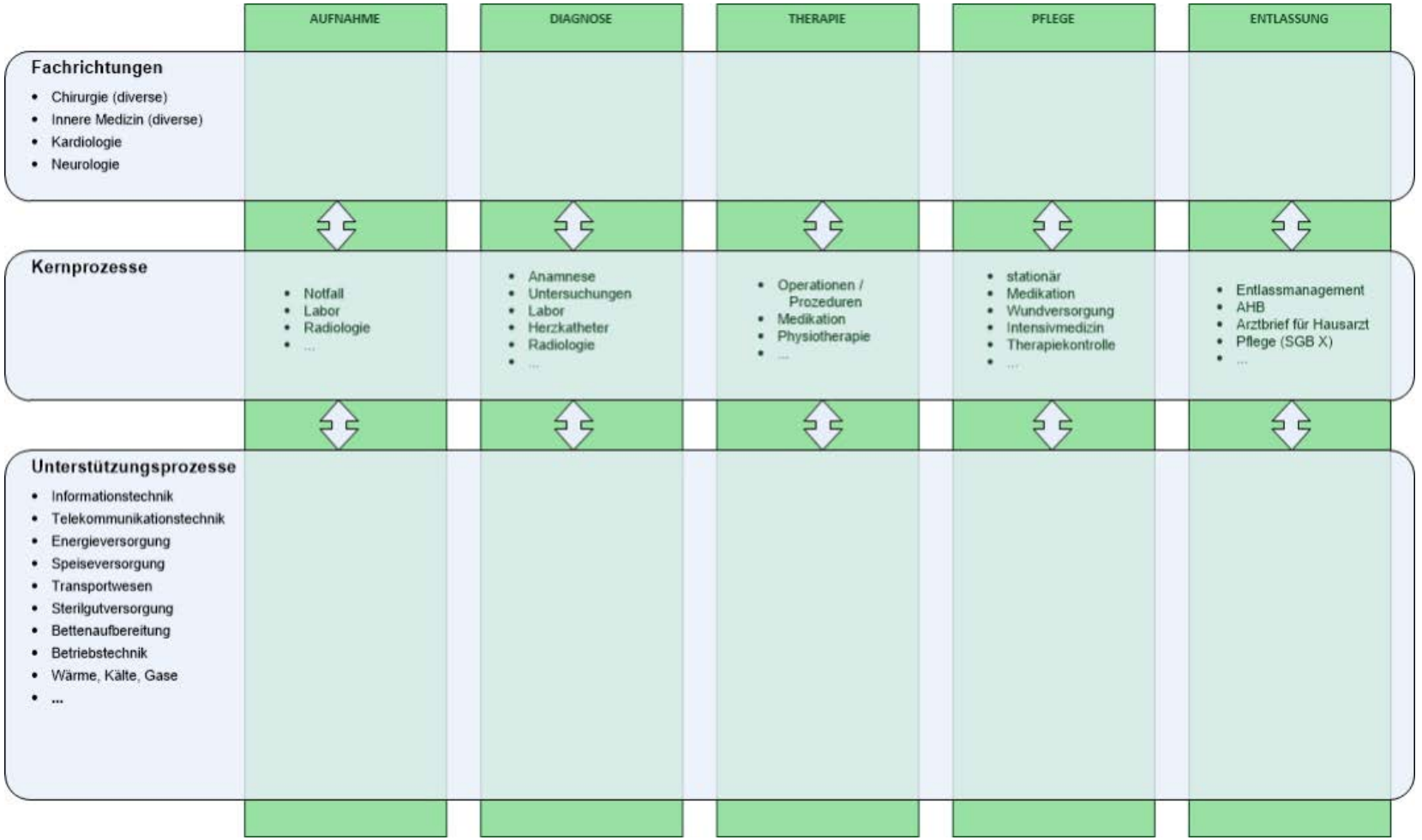
Geltungsbereich (Scope-Definition)

- der krankenhausspezifische Geltungsbereich ist innerhalb der grundsätzlich relevanten Bereiche der kDL zu benennen
- Ausschlüsse sind zu begründen
- B3S beschreibt Vorgehensmodell zur individuellen Festlegung



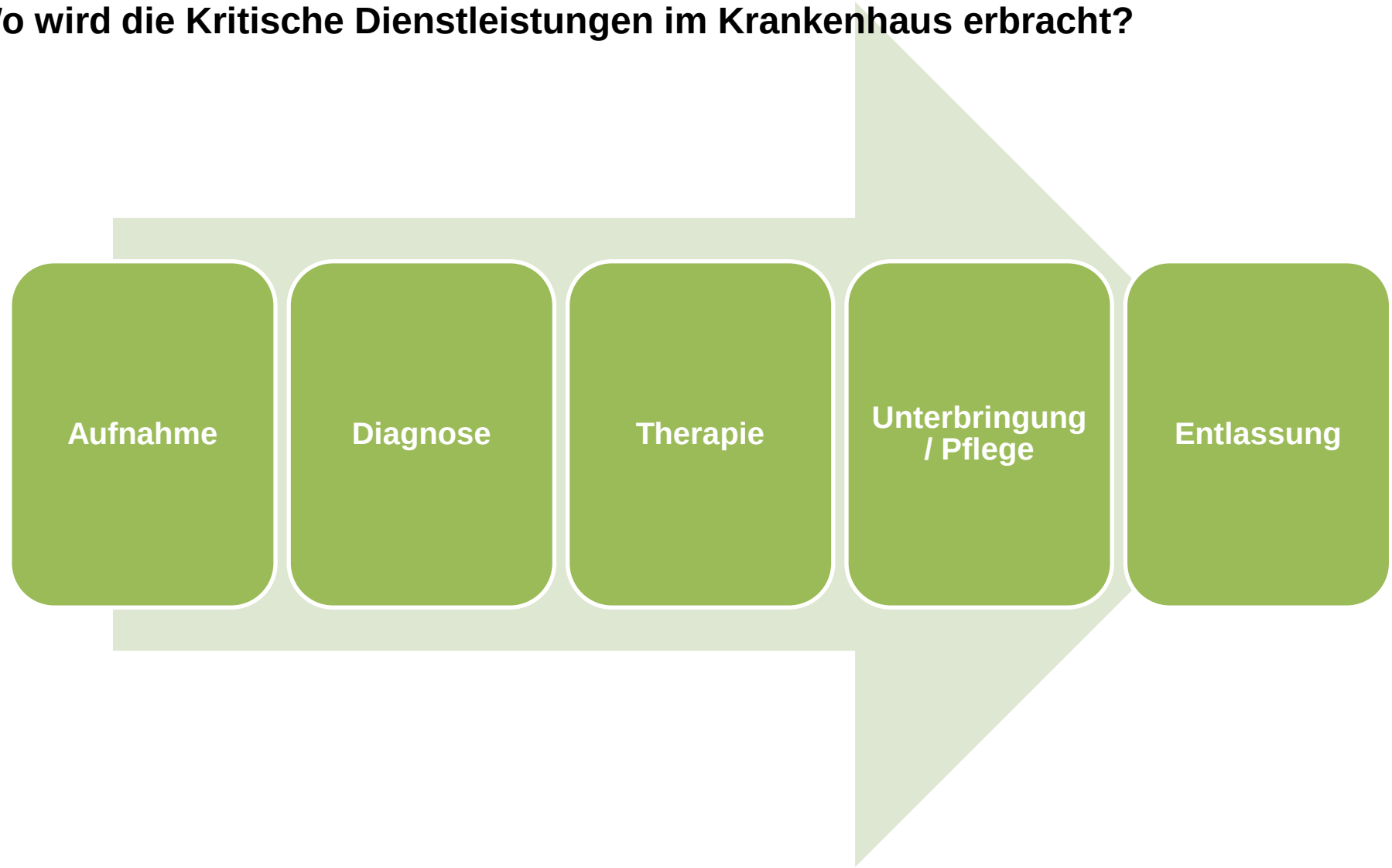
Geltungsbereich (Scope - Definition)

- Bewertung der identifizierten Prozesse und Systeme nach Kritikalität
- Identifikation der für die kDL relevanten Prozesse und Systeme

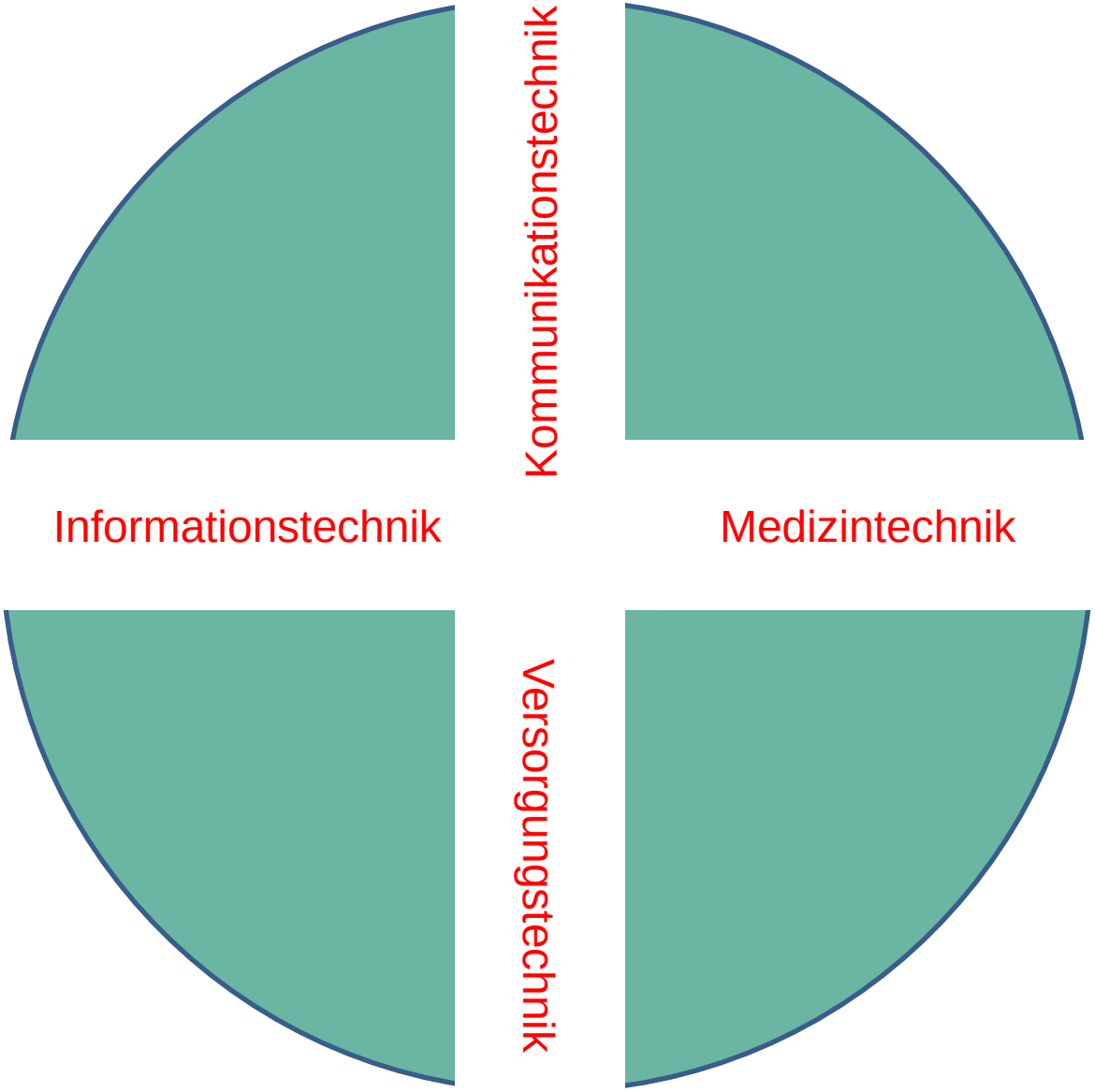


Kritische Dienstleistung (kDL)

Wo wird die Kritische Dienstleistungen im Krankenhaus erbracht?

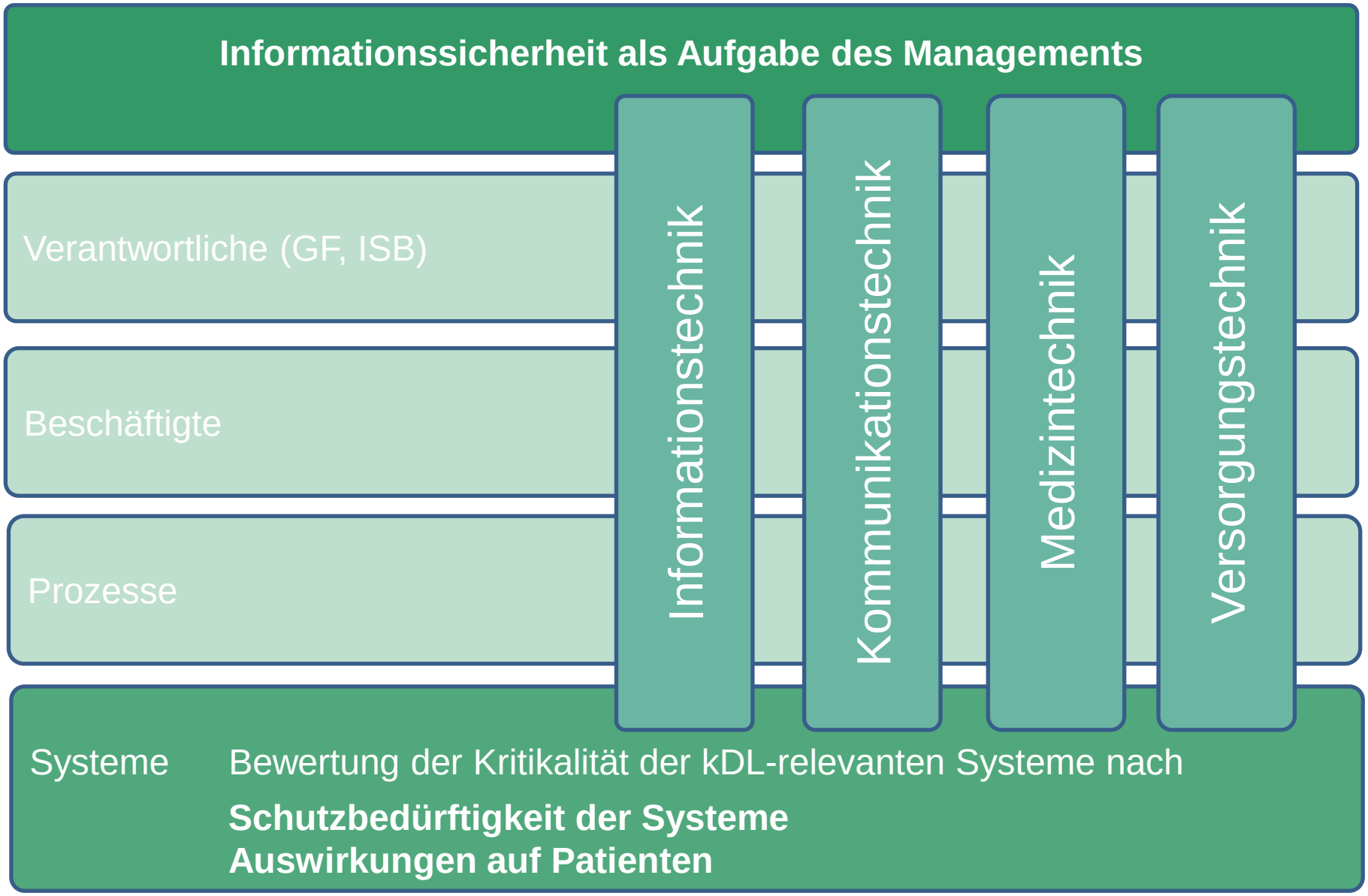


Technische Unterstützungsprozesse im KH



- heterogene Organisation in den Krankenhäusern
- in der Regel nur durch Erhebung vor Ort ermittelbar
- Zuständigkeiten können im Einzelfall auch mehreren Bereichen zugeordnet

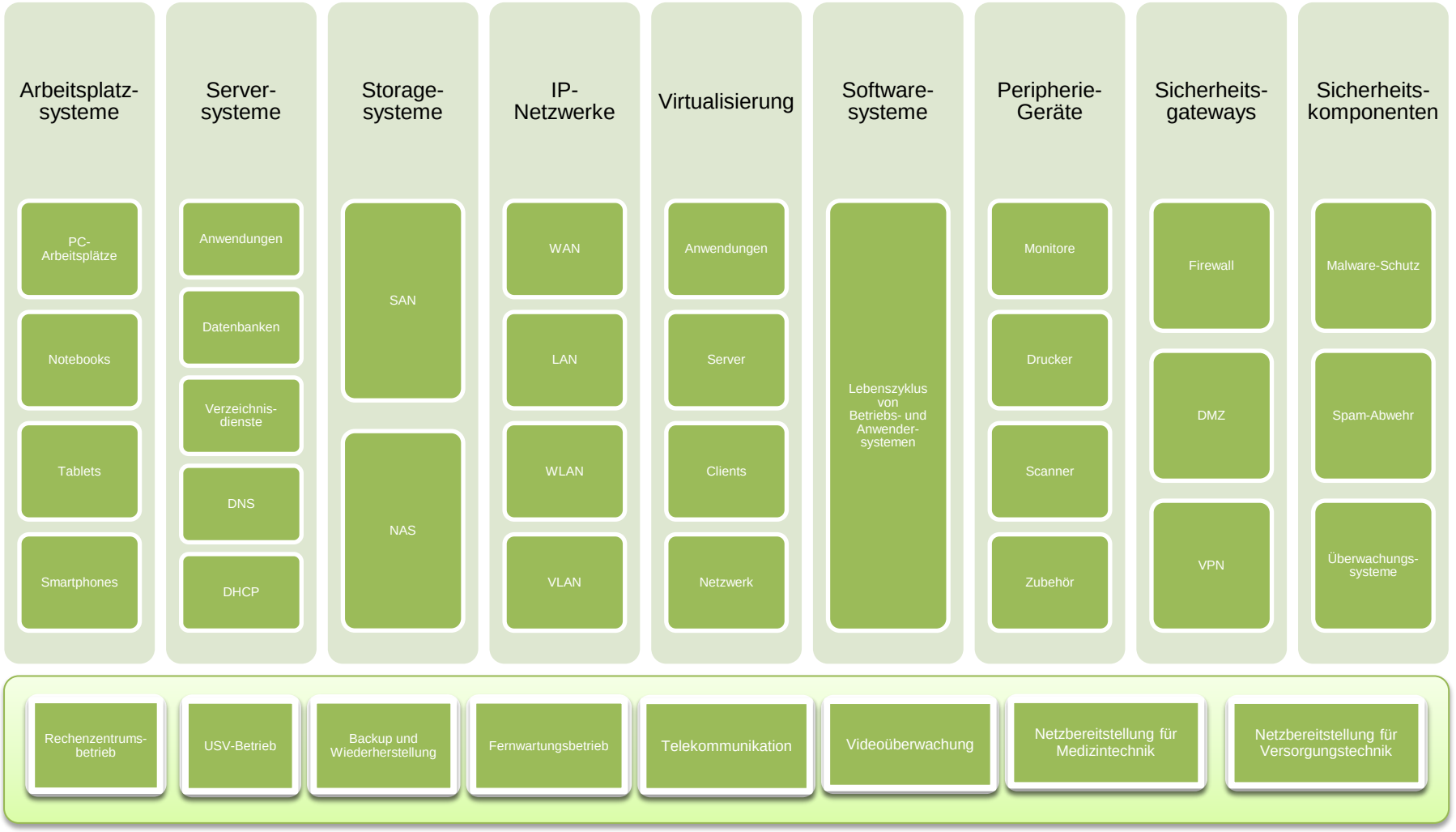
kDL-relevante IT-Systeme und Komponenten



Unterstützungsprozesse: Informationstechnik

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Betrachtung mindestens der folgenden Aufgaben und Systeme:



Unterstützungsprozesse: Informationstechnik

Betrachtung mindestens der folgenden Aufgaben und Systeme:

- Rufsysteme, Diensttelefonie (Festnetz)
  - Endgeräte
  - VoIP-Telefone (PPoE)
  - DECT/GSM
  - TK-Anlagenserver
- Diensttelefonie (Mobil)
  - Endgeräte z. B. Mobiltelefonie / Smartphones
  - DHCP
- Fax-Betrieb
  - Faxserver
  - klassische Fax-Anlagen
  - Multifunktions-geräte
- Wechselsprechtechnik
  - Redundanz-Konzept für Störfälle z. B. Mobiltelefonie
  - Zugangslösungen z. B. Klingel- und Sprechanlagen für geschlossene Bereiche
- Warn- und Alarmierungs-systeme
  - für Kühlsysteme (Blut- und Plasmapräparate)
  - für Inkubatoren

Unterstützungsprozesse: Medizintechnik

Betrachtung mindestens der folgenden Aufgaben und Systeme:

Patientendaten-managementsystem und Informationsverarbeitung medizintechnischer Systeme	Telemedizinische Systeme Telemetriesysteme	patientengebundene Alarmierungssysteme	Steuerung der Instandhaltung medizintechnischer Anlagen	Instandhaltung und Austausch von Einzelgeräten
für diagnostische bzw. therapeutische Zwecke benötigte und zur Verfügung gestellte Daten	Überwachung wichtiger Parameter bei Erhöhung von Freiheitsgraden in der Patientenversorgung	häufig gekoppelt mit IT-Komponenten im Einzelfall auch Teil der Kommunikationstechnik	für Diagnostik für Therapie herstellerbasierte Leistungserbringung	z. B. „Kleingeräte“, wie Infusionspumpen o.ä

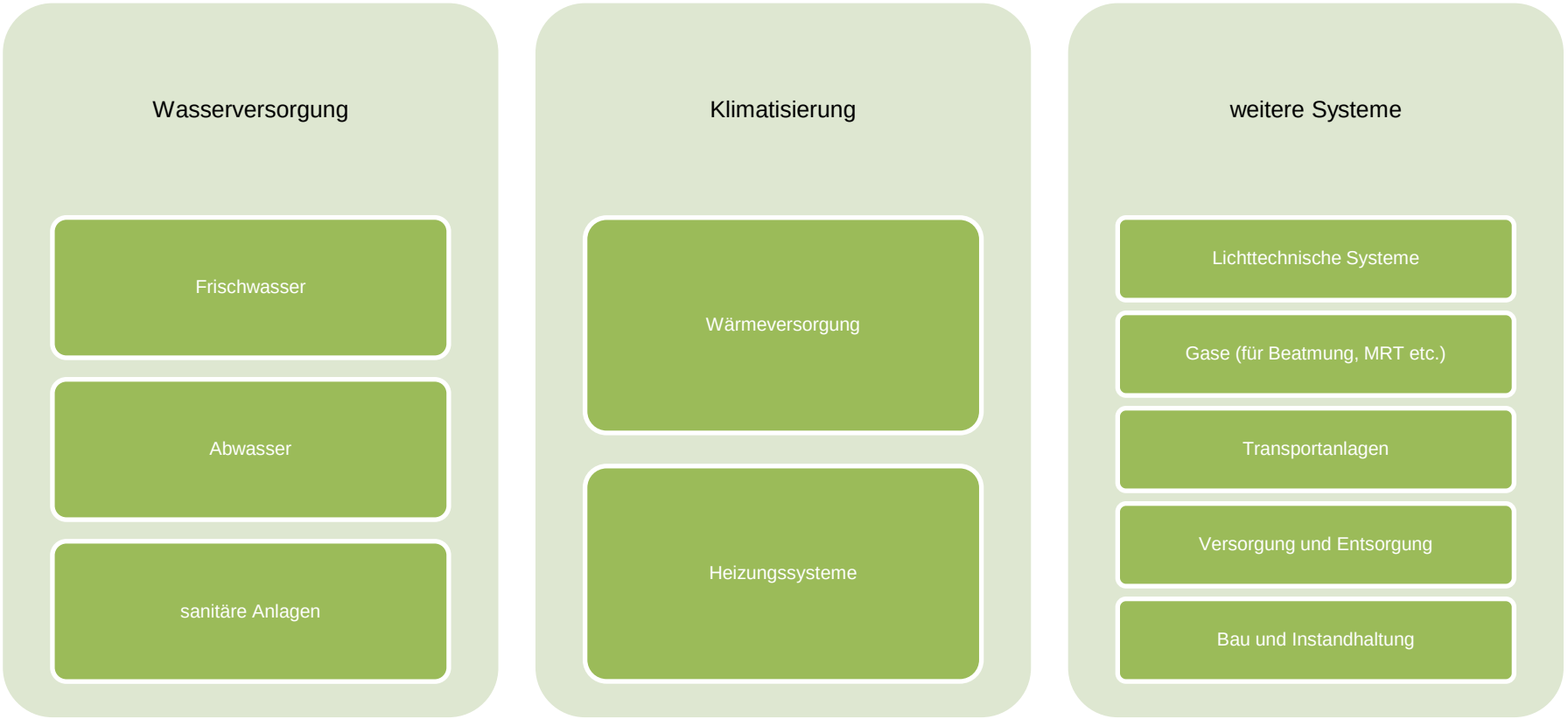
Unterstützungsprozesse: Versorgungstechnik

Betrachtung mindestens der folgenden Aufgaben und Systeme:

Energieversorgung	Klimatisierung	Videoüberwachung	Gebäudeleittechnik
Elektroversorgung	Kühlung, z. B. OP's	wenn organisatorisch im Bereich Versorgungstechnik angesiedelt	Digitale Zugangs- und Schließsysteme
Netzversorgung (Einspeisung)	technische Anlagen	Schnittstelle zur IT	Zufahrts- und Schrankensysteme
Ersatzversorgung (Notstromdiesel)			Gebäudeautomatisierungs-technik

Unterstützungsprozesse: Versorgungstechnik

Betrachtung der folgenden Aufgaben und Systeme optional[1]



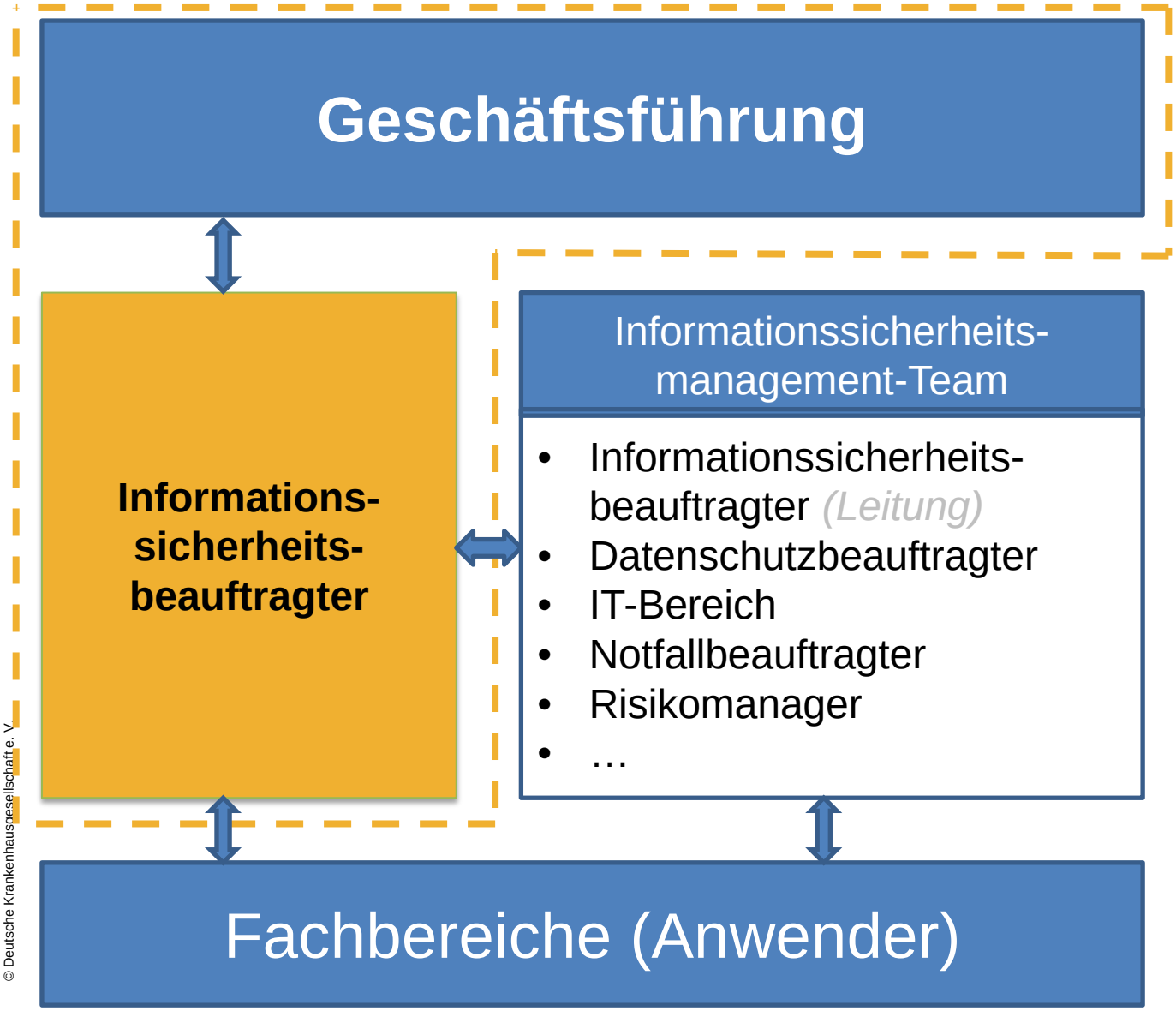
1) da in der Regel bereits in übergeordnetem BCM-System enthalten

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Allgemeine Hinweise zum B3S

- B3S = Katalog an Maßnahme-Empfehlungen
- Ziel: sichere und resiliente IT-Infrastruktur im Bereich der vollstationären medizinischen Versorgung
- Abstraktionsgrad variiert aufgrund heterogener Voraussetzungen in den Krankenhäusern
- individuelle Ausgestaltung notwendig, kein „Checklisten-Charakter“
- gestuftes Vorgehen (Iterationen) notwendig, um sukzessive alle notwendigen Maßnahmen umzusetzen
- risikoorientierte Priorisierung bei stufenweiser Umsetzung
- ISMS ist ein wesentlicher Aspekt der Umsetzung, jedoch allein nicht ausreichend

Organisatorische Umsetzung im Krankenhaus



Vorgabe von Leitlinien zur Informations-sicherheit

Vorgabe von Richtlinien zur Informations-sicherheit

Vorgabe von Handlungsan-weisungen zur Informations-sicherheit

Überblick über wesentliche Anforderungen

Organisatorische Anforderungen

- ISMS
- BCM
- Physische Sicherheit
- Überprüfung im laufenden Betrieb
- Organisation der Informationssicherheit
- Asset Management
- Personelle und organisatorische Sicherheit
- Externe Informations-versorgung und Unterstützung
- Meldepflichten nach § 8b BSIG
- Robuste / Resiliente Architektur
- Vorfallerkennung und Behandlung
- Lieferanten, Dienstleister und Dritte

Überblick über wesentliche Anforderungen

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Technische Informationssicherheit

Netz- und Systemmanagement (Netztrennung und Segmentierung)	Identitäts- und Rechtemanagement	Vernetzung von Medizingeräten	Umgang mit Datenträgern, Austausch von Datenträgern
Absicherung Fernzugriffe	Sichere Authentisierung	Beschaffungsprozesse	Sicheres Löschen und Entsorgung von Datenträgern
Härtung und sichere Basiskonfiguration der Systeme und Anwendungen	Kryptographische Absicherung (data in rest, data in motion)	Datensicherung, Datenwiederherstellung und Archivierung	Softwaretests und Freigaben
Schutz vor Schadsoftware	Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (BYOD)	Ordnungsgemäße IT-Administration	Datenschutz
Intrusion Detection / Prevention	Patch- und Änderungs-management	Protokollierung	ggf. weitere individuelle Maßnahmen

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Zur Umsetzung des B3S müssen die folgenden Fragen beantwortet werden:

- Welche Systeme müssen betrachte werden? (Scope-Definition, kDL)
- Welche Risiken für die Systeme / Infrastruktur müssen betrachtet werden? (Gefährdungslage)
- Welche Risikoeinstufung erfolgt für die Systeme anhand der potentiellen Schadenswirkung? (Risikobewertung)
- Welche Maßnahmen müssen umgesetzt werden, um die identifizierten Risiken zu minimieren? (Maßnahmenkatalog)

Prüfung nach § 8a BSIG - Überblick

Rollen und Verantwortlichkeiten im Prüfprozess

Bundesamt für Sicherheit in der Informationstechnik

Übermittlung des Nachweis

ggf. Anforderung zusätzlicher Informationen

Betreiber einer kritischen Infrastruktur

Beauftragung

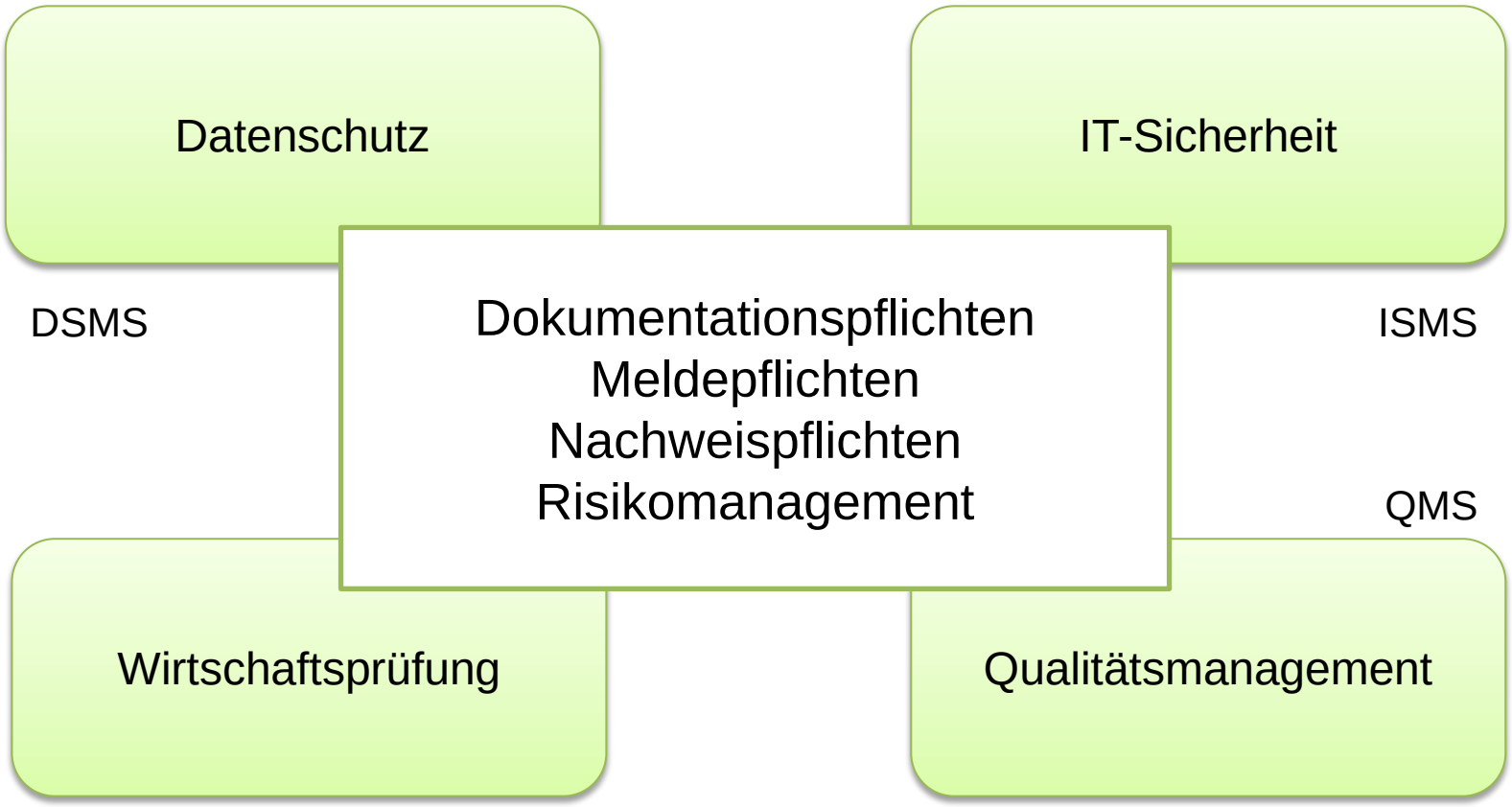
Prüfung

Prüfende Stelle

Prüfteam

Empfehlung an Krankenhäuser: IT-Strategie

*Krankenhäuser **benötigen eine IT-Strategie**, die übergreifende Compliance-Anforderungen adressiert*



Finanzierung entstehender Aufwände

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Erwartete Mehrkosten für Umsetzung von Anforderungen an Informationssicherheit

Investitionskosten

in Verantwortung der Bundesländer

Betriebskosten

ggf. im Rahmen der Budgetplanung zu berücksichtigen

Personalkosten

heterogenes Anforderungsprofil

allgemeine Marktsituation schwierig

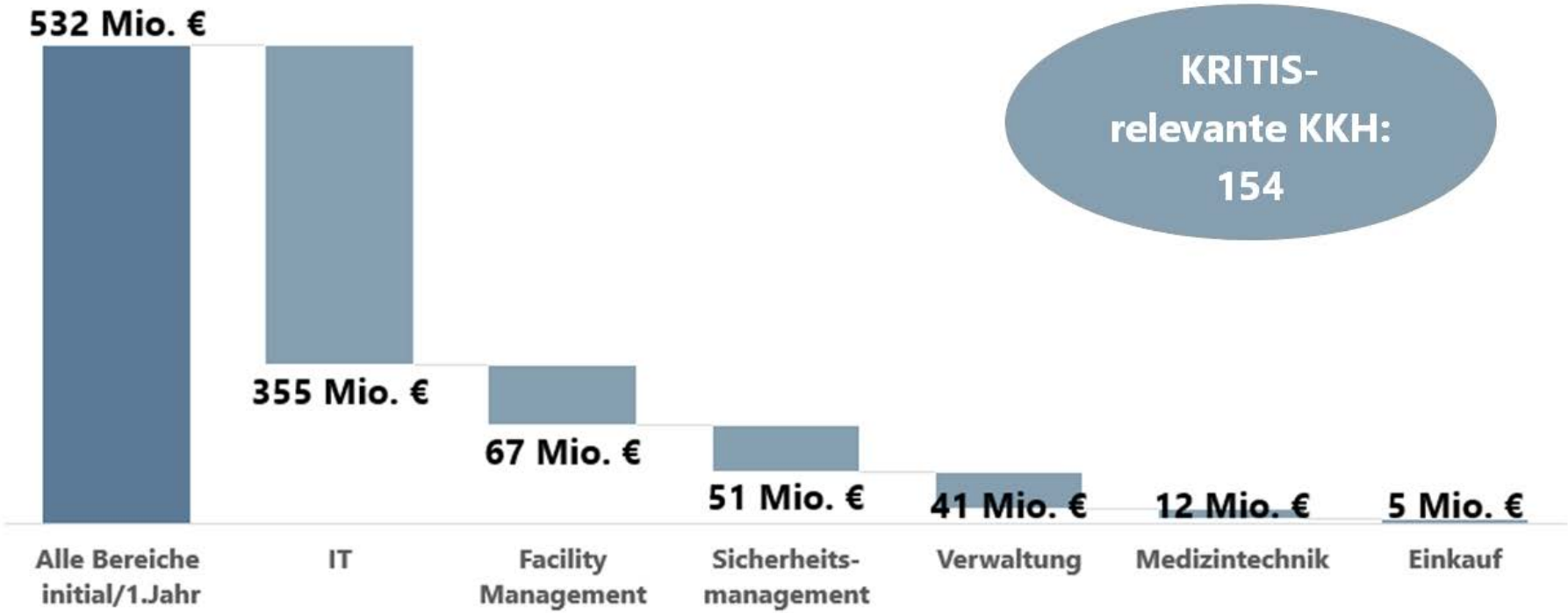
Finanzierung entstehender Aufwände

- Regelungen des Pflegepersonalstärkungsgesetz greifen nicht:
  - Uniklinika grundsätzlich nicht förderfähig
  - Bundesländer greifen derzeit die neuen Möglichkeiten des Strukturfonds nicht auf
  - gesetzliche Krankenkassen müssten den zu fördernden Vorgaben auf Ortsebene zustimmen (Veto!)
- Ausgliederung der Pflege aus dem DRG-System soll explizit die „zweckfremde Mittelverwendung“ (z. B. für Investitionskosten) beenden
- **Bedarf an qualifiziertem Fachpersonal ungelöst!**

Kostenerhebung DKG (noch nicht veröffentlicht)

DEUTSCHE KRANKENHAUS GESELLSCHAFT

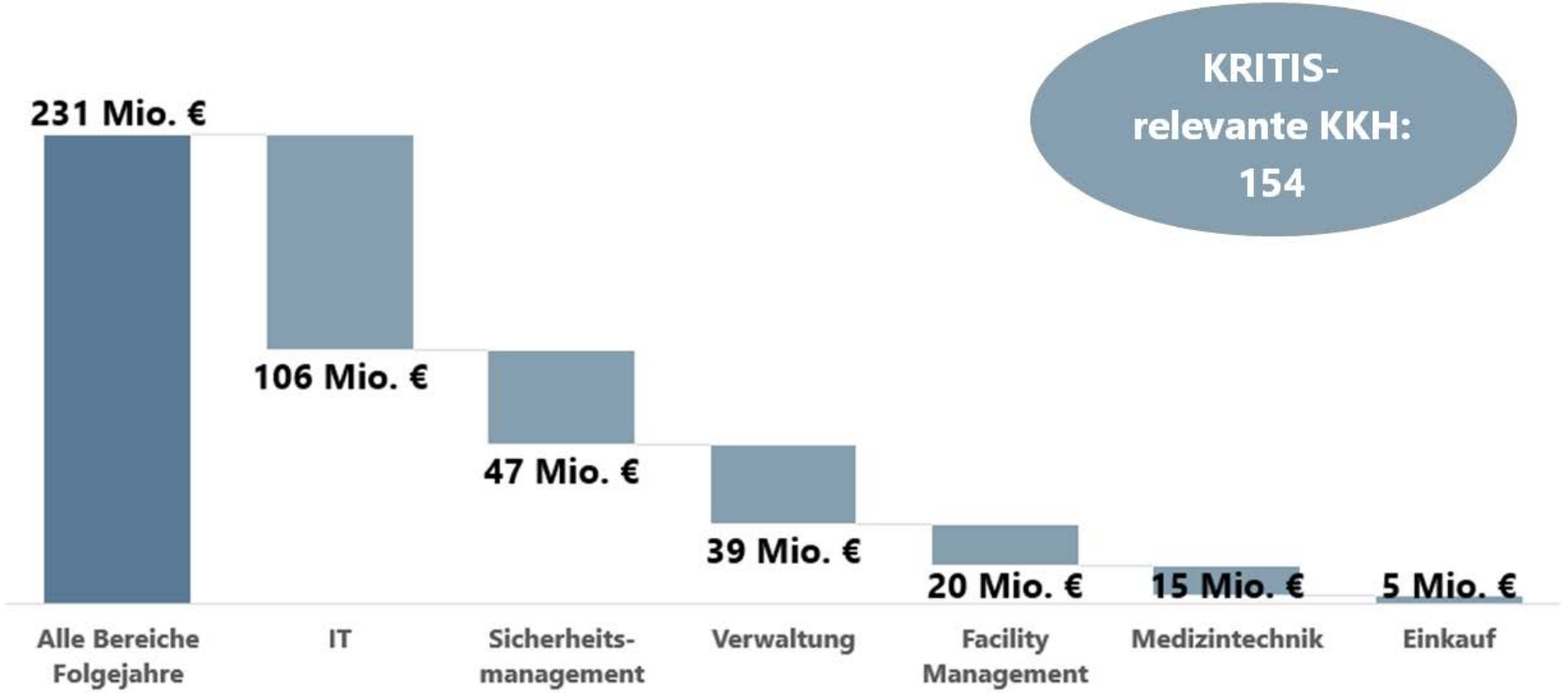
3.2 Initiale Kosten im 1. Jahr für 154 KritisV-relevante Krankenhäuser*, in Mio. EUR



Kostenerhebung DKG (noch nicht veröffentlicht)

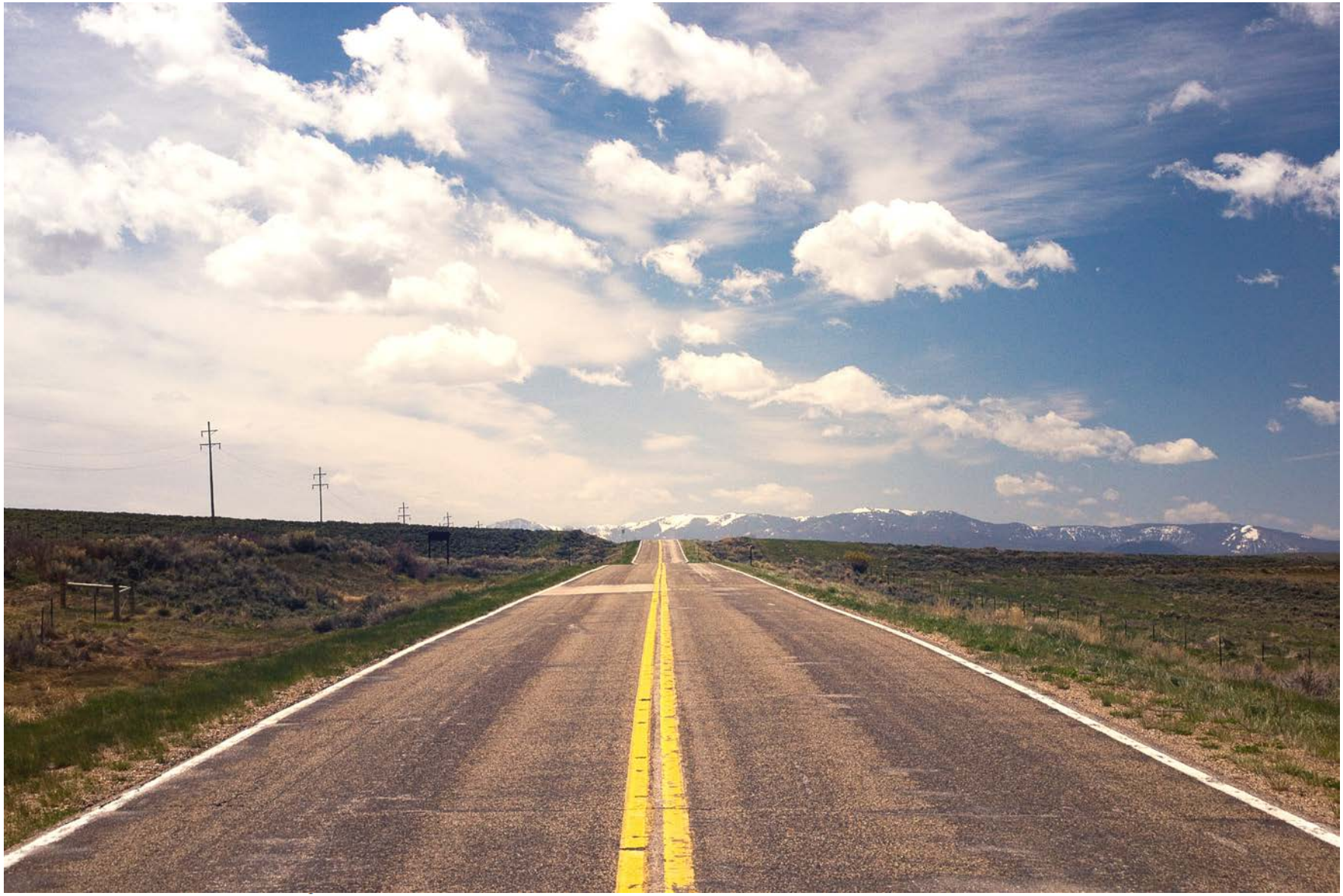
DEUTSCHE KRANKENHAUS GESELLSCHAFT

3.3 Wiederkehrende Kosten für 154 KritisV-relevante Krankenhäuser*, in Mio. EUR/Jahr



Ausblick:
ITSiG 2.0 / 2. Änderungsverordnung BSI-KritisV

DEUTSCHE KRANKENHAUS GESELLSCHAFT



Vielen Dank für Ihre Aufmerksamkeit!

DEUTSCHE
KRANKENHAUS
GESELLSCHAFT