Deutsche Krankenhaus Gesellschaft

Autoren:

Dennis Graf
Rüdiger Gruetz
Rainer Hirt

Anwendungshinweis:

Dieses Dokument sowie die vorliegenden Empfehlungen und Arbeitshilfen wurden mit größter Sorgfalt erstellt und geprüft, erheben jedoch keinen Anspruch auf Vollständigkeit. Sie geben ausschließlich den Stand zum Zeitpunkt ihrer Erstellung wieder und ersetzen keine individuelle Prüfung. Insofern übernimmt die Deutsche Krankenhausgesellschaft keine Haftung für die Anwendung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen.

Inhaltsverzeichnis

Vorbemerkung

Durch die Anforderungen des §75c SGB V sind alle Krankenhäuser verpflichtet den Stand der Technik anzuwenden, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind“.

Eine der wichtigsten Handlungsgrundlagen bei der Einführung und der kontinuierlichen Verbesserung eines Informationssicherheitssystems (ISMS) ist die Definition des zu betrachtenden Bereiches, des so genannten Scopes oder Geltungsbereich des ISMS.

Die vorliegende Arbeitshilfe soll dabei Hilfestellung geben die entsprechende Unterlage zu erstellen.

Definition Scope

Der Begriff Scope wird häufig als Bereich, Ziel oder Umfang insbesondere im Projektmanagement übersetzt.[1]

Im Zusammenhang[2] mit der Einführung und der kontinuierlichen Verbesserung eines Informationssicherheitssystems ist hier

- der räumliche Geltungsbereich (Standorte),
- Art und Umfang der Dienstleistungen (Prozesse),
- die verwendete technische Infrastruktur

zu sehen.

Inhalte

Im Folgenden werden die Inhalte eines Scope beschrieben und Hinweise zur Darstellung gegeben.
Die Abbildungen sind ausdrücklich als Muster / Beispiele zu verstehen und stellen **keine** Vorgabe dar.

[1] https://de.wikipedia.org/wiki/Scope

[2] Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSI Version 1.1 vom 21.08.2020 Absatz 2.1 Beschreibung des Prüfungsgegenstandes; Seite 9 ff

Räumlicher Geltungsbereich

Hierbei handelt es sich um eine Darstellung der Standorte / Liegenschaften / Einrichtungen, die für die Sicherstellung der medizinischen Versorgung der Patienten erforderlich sind und unter der Verantwortung der Organisation stehen.

Dies können beispielsweise sein (Aufzählung nicht abschließend):

- Fachkliniken
- MVZ
- Kooperationspartner mit IT Anbindung
  - Labore
  - Belegärzte
  - Radiologische Praxen (auch Teleradiologie)
- Leitstellen
- Externe Rechenzentren
- Cloud Dienstleister
- Externe Dienstleister
  - Schreibdienste
  - Sicherheitsdienst
  - Einkaufgenossenschaften
  - Lieferanten
  - Überwachung medizinischer Geräte
  - KIS Systembetrieb
  - Betreiber extern bereitgestellter Software
    - E-learning
    - Dokumentenmanagement
    - Firewall

Beispiele für räumliche Darstellungen (fiktives Beispiel)

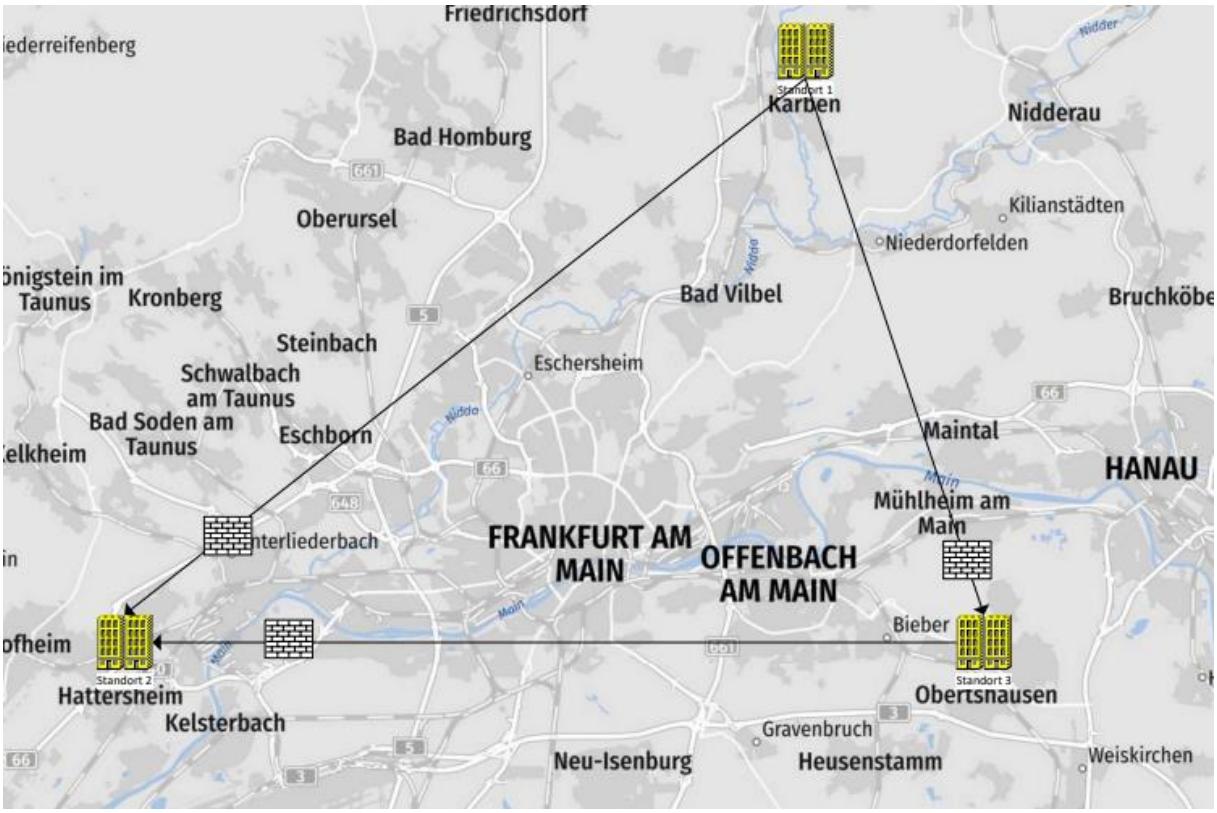

Abbildung 1 Beispiel geographische Verteilung

Es empfiehlt sich bei der Betrachtung der räumlichen Ausdehnung auch die Anbindung der IT-Infrastruktur (Standleitungen, Richtfunk oder Mobilfunk) mit zu betrachten.

IT-Infrastruktur innerhalb des Scope

Bei der Darstellung der IT-Infrastruktur ist **kein** umfänglicher Netzwerkplan erforderlich. Die Zusammenhänge der Standorte und der Komponenten incl. der Sicherheitsmaßnahmen sollten allerdings erkennbar sein.

Beispiele für Netzwerkdarstellung

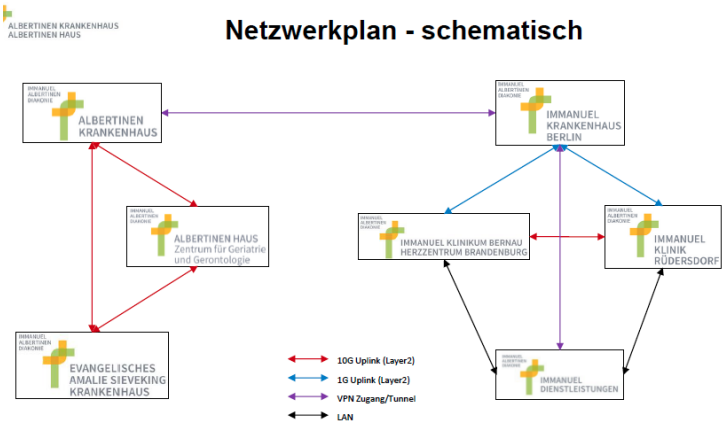

Abbildung 2 Verbindungen der Standorte untereinander

Beispiele Schnittstellen Darstellung im Krankenhaus Netzwerk

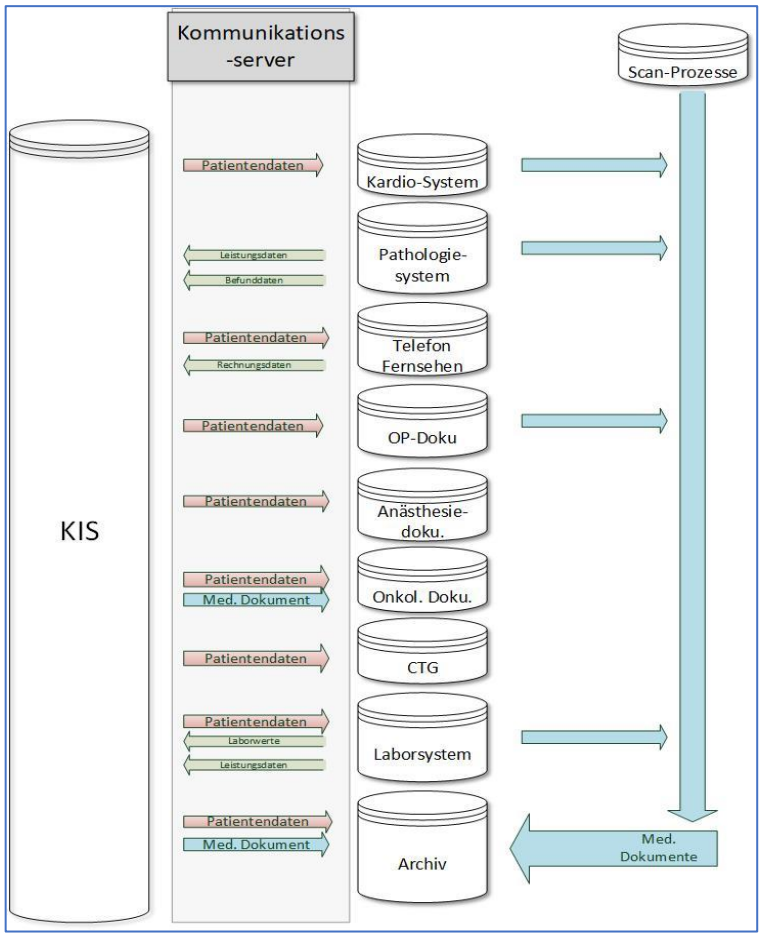

Abbildung 3 Beispiel 1 Schnittstellenübersicht

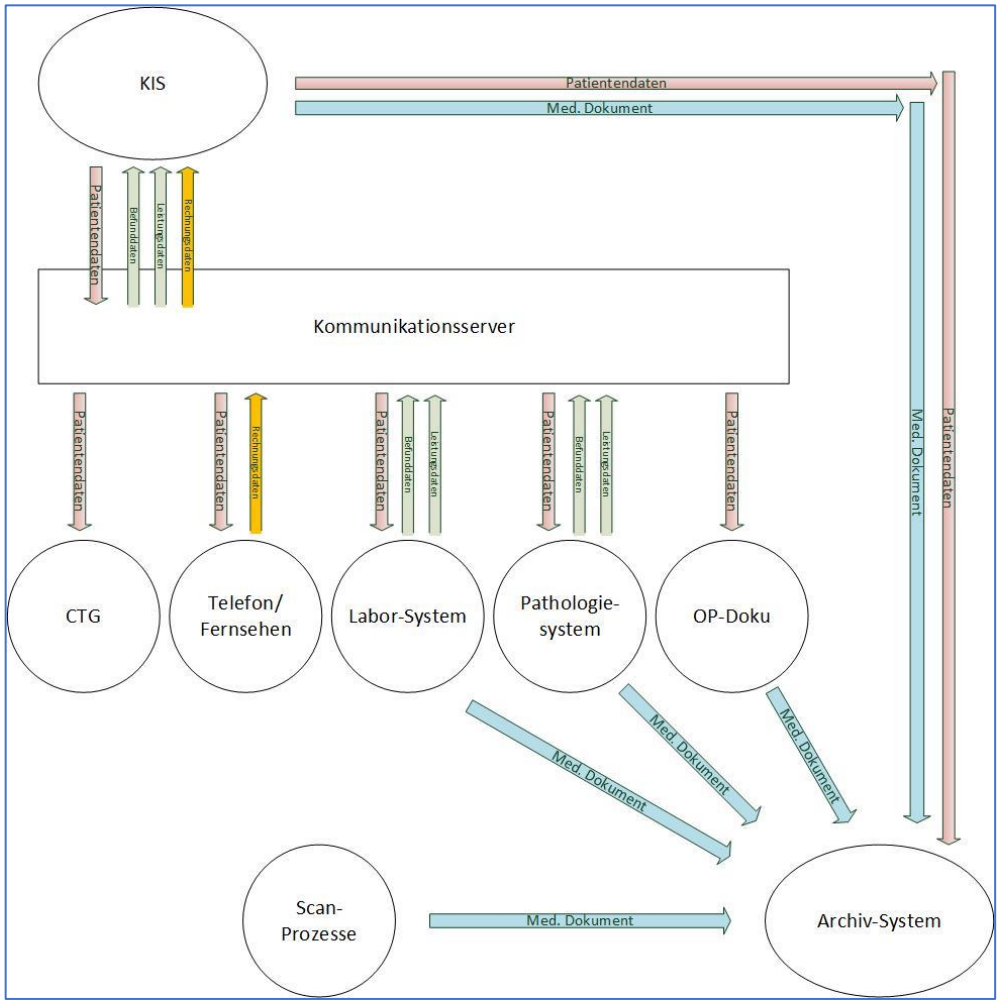

Abbildung 4 Beispiel 2 Schnittstellenübersicht

Beispiel Darstellung Anbindung Kooperationspartner

Anbindung von Kooperationspartnern		
Dienstleister	**Art der Anbindung**	**Bemerkung**
Externe Labore (Name)	VPN-Tunnel	
Apotheke		
Gerätelieferant A		
Gerätelieferant B		
Dienstleister A		
Dienstleister B		
Schreibdienst		
Pathologisches Institut	Videokonferenz	
Radiologie	Teleradiologie	

Abbildung 5 Beispiel für Übersicht Anbindung Kooperationspartner

Beispiel Netzwerkübersicht mit Firewall

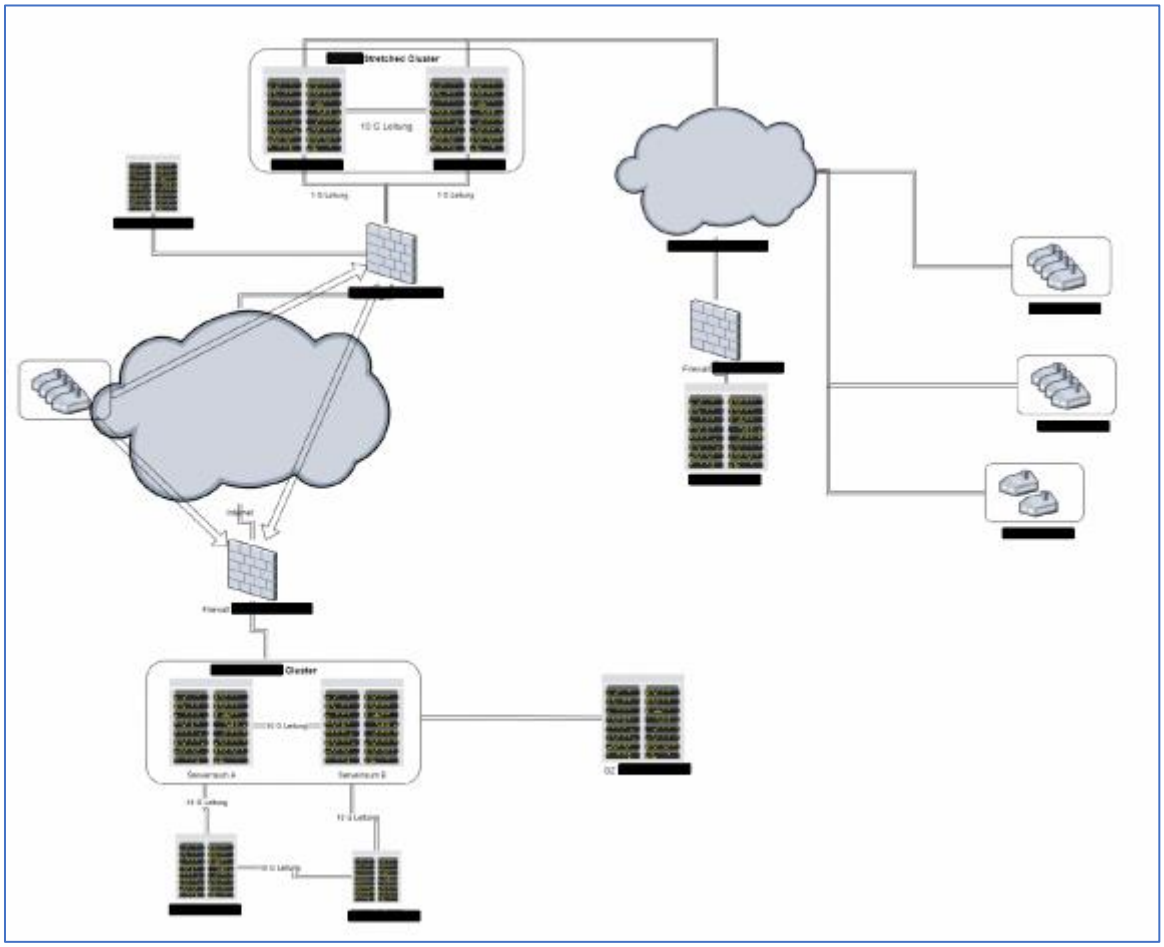

Abbildung 6 Beispiel für eine Darstellung der mit Firewall

Sachlicher Geltungsbereich

Hier sollte eine Beschreibung der Leistungen erfolgen, die für die Sicherstellung der medizinischen Patientenversorgung erforderlich sind. Dabei ist das jeweilige Versorgungsniveau zu beachten.

Beispiel für den sachlichen Geltungsbereich

Die medizinische Versorgung von Patienten stellt einen Kernprozess dar und umfasst sämtliche Prozesse und Aufgaben am Krankenhaus, die der Erhaltung und Wiederherstellung der Gesundheit der Patienten dienen. Im Scope enthalten sind alle kritischen Bereiche, Prozesse und Systeme, die für die sichere Erbringung der medizinischen Patientenversorgung notwendig sind.[3]

- Die folgenden kritischen Prozesse (Kernprozesse) der stationären Versorgung werden betrachtet:
  - Aufnahme
  - Diagnose
  - Therapie
  - Pflege
  - Entlassung

- Zusätzlich zu den Kernprozessen werden die folgenden technischen Unterstützungsprozesse betrachtet:

  - Informationstechnik (IT)
  - Kommunikationstechnik (KT)
  - Medizintechnik (MT)
  - Versorgungstechnik (VT

- Zusätzlich werden die folgenden kritischen Anwendungssysteme betrachtet:

  - Krankenhausinformationssystem (KIS)
  - Laborinformationssystem (LIS)
  - Radiologie Informationssystem (RIS)
  - Picture Archive and Communication System (PACS)
  - Dokumenten-Management-System (DMS/ECM)
  - OP-Planungssystem
  - Systeme für Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransporte)
  - Systeme der Versorgungstechnik
  - Systeme der Versorgungsdienste
  - Medizintechnik/-produkte
  - Spezialisierte Anwendungen im klinischen Umfeld

Die Bereiche Labor („Klinisches Labor“) und Arzneimittel („Krankenhausapotheke“) werden berücksichtigt, soweit diese den primären Aufgaben des Krankenhauses in Erfüllung des Versorgungsauftrages zuzurechnen sind.

Prozesse und Systeme in den zentralen Notfallambulanzen und -aufnahmen werden berücksichtigt, da Patienten über diesen Zugang in die medizinische Versorgung aufgenommen werden.

[3] Aufzählung nicht abschließend und ist von der Größe der Organisation und dem Versorgungsauftrag abhängig

Prozesse die innerhalb des Scopes erbracht werden

Hierbei handelt es sich um die klassischen Kern- und Unterstützungsprozesse, die einem Krankenhaus erbracht werden.

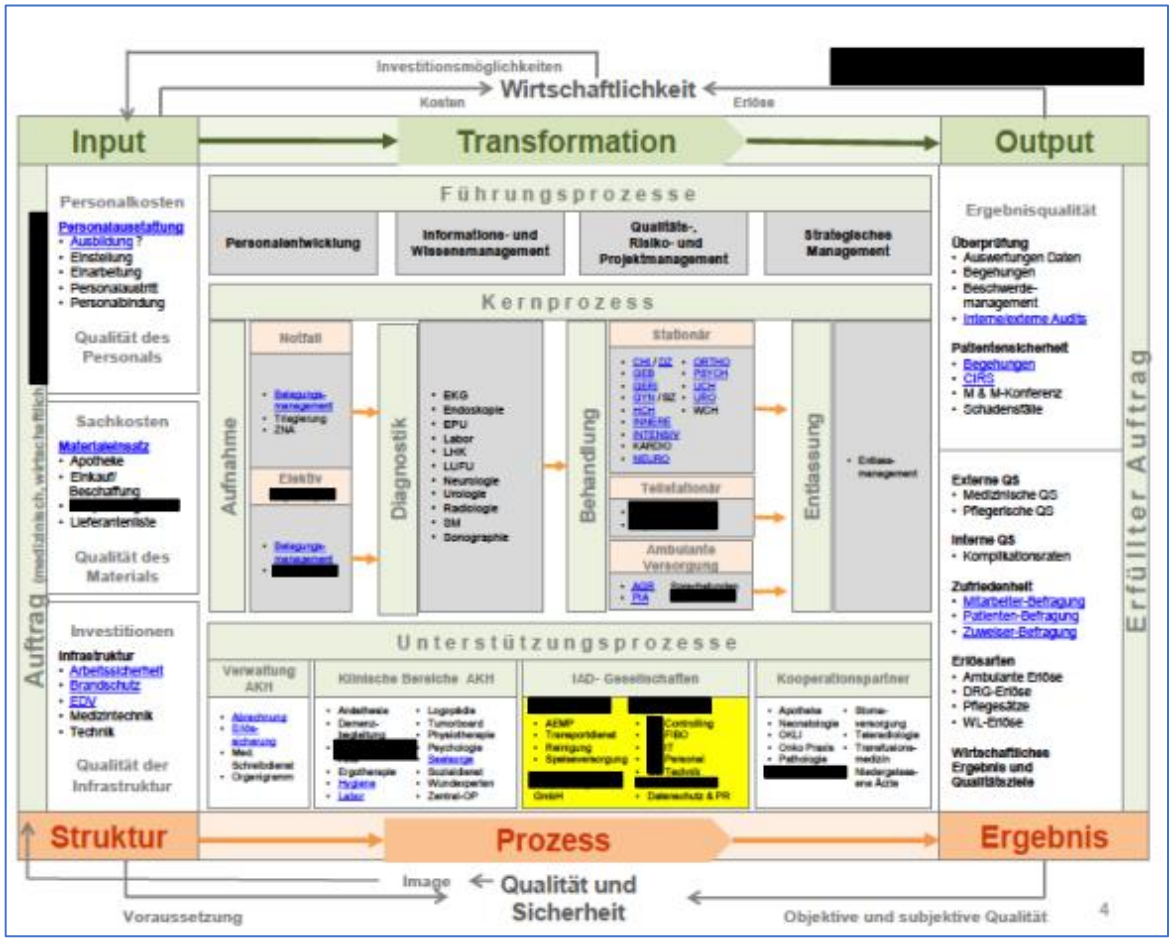

Abbildung 7 Beispiel 1 Prozessübersicht

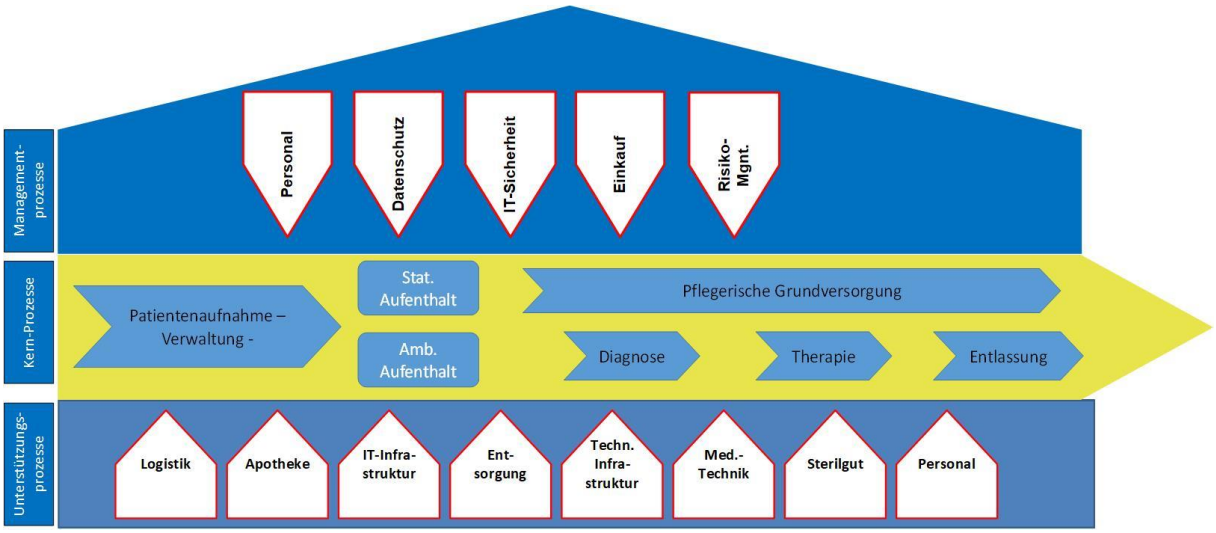

Abbildung 8 Beispiel 2 Prozessübersicht

Im Qualitätsmanagement wird dies als „Prozesslandkarte“ beschrieben. Im Folgenden ein Beispiel einer Prozesslandkarte, die gleichzeitig aufzeigt, welche Prozesse nicht betrachtet werden.

Prozesse und Bereiche die **nicht** vom Scope erfasst werden.

Die vorhergehende Darstellung zeigt die Prozesse auf, betrachtet werden müssen.

Es empfiehlt sich analog der Forderung der DIN EN ISO 9001:2015 Ziff. 8.4 ff. „Steuerung von extern bereitgestellten Prozessen“ eine Übersicht **aller** Prozesse, die durch Dritte erbracht werden, aber für die stationäre Patientenversorgung von Bedeutung sind, aufzustellen.

Ein Vorteil dieser „Arbeit“ ist es eine aktuelle Ist-Aufnahme zu haben und dabei die Prozesse hinsichtlich ihrer Sicherheit und Widerstandsfähigkeit zu beleuchten. U.a. können sich hier auch Fragen nach Ausfallkonzepten von Dienstleistern ergeben.

Dies kann auch in einer vorhandenen Übersicht erfolgen, in dem die ausgelagerten Prozesse in der Tabelle farblich gekennzeichnet und schriftlich begründet sind.

Eine weitere Informationsquelle zur Identifizierung externer Prozessbeteiligter kann das sog. Verzeichnis von Verarbeitungstätigkeiten[4] aus dem Bereich Datenschutz sein. Hierfür nehmen Sie mit Ihrer(m) Datenschutzbeauftragte(n) Kontakt auf.

Beispiel für eine Übersicht ausgelagerter Prozesse in Tabellenform

Bereich	Kontaktdaten	Grundlage	Prozesse	Kontrolle
Arbeitssicherheit & Brandschutz	Kontaktdaten und Ansprechpartner	Vertrag	Unterstützung des Arbeitgebers gemäß Arbeitssicherheitsgesetz (ASiG) § 1 auf dem Gebiet des Arbeitsschutzes und der Unfallverhütung. Unterstützung bei der Einhaltung der Unfallverhütungsvorschriften (UVV) Technische Regeln (TRG, TRGS, TRB usw.) Verordnung über elektr. Anlagen (Explosionen) uva. Gesetze bzw. Verordnungen und Normen.	Es werden Protokolle der Arbeitssicherheits- und Brandschutz-Begehungen angefertigt.
Datenschutz	Kontaktdaten und Ansprechpartner	Vertrag	Datenschutz: Unterstützung der Verantwortlichen Stelle als gesetzlich vorgeschriebener Datenschutzbeauftragter gem. Art. 39 DSGVO und den dort festgelegten Aufgaben.	Protokollierung von allen eingehenden Datenschutzanfragen und den daran anschließenden Prozessen bzw. Antworten Protokollierung von Datenschutzbegehungen Wöchentliches Jour Fixe zu aktuellen Themen mit Vertreter der GF/internem Mitglied des Datenschutz-Teams bzw. Vertreter des Bereiches Recht Laufende Aktualisierung von Projekt- und Maßnahmenplänen
Konsiliarärzte	(Art und Name)	Vertrag	Auslöser: Konsilanforderung. Zusammenarbeit: Erbringung der Konsilanforderung Die Durchführung erfolgt an definierten Anwesenheitstage.	Im Rahmen der Durchführung von Konsiltätigkeiten
Transporte zwischen den Standorten	Kontaktdaten und Ansprechpartner	Vertrag	Patiententransporte Gütertransporte zwischen den Standorten Inhousetransport der Speisewagen Küche Inhousetransport der Apothekengüter Stadtfahrten für alle Standorte: Standesamt, Labore, Bank und Sonstiges auf Abruf	Besprechungen Tourenplan

Abbildung 9 Beispiel Übersicht ausgelagerter Prozesse

[4] Art. 30 DSGVO „Verzeichnis von Verarbeitungstätigkeiten“ oder vergleichbare kirchliche Vorschriften

Kleine Checkliste zum Scope

Die folgende Checkliste kann helfen, die Anforderungen an einen Scope zu berücksichtigen

- ✓ Räumliche Darstellung, die zum Scope gehören (Landkarte / Stadtplan).
- ✓ Begründung und Darstellung, welche räumlichen Bereiche nicht zum Scope gehören (auch innerhalb der KH).

- ✓ Alle Prozesse der medizinischen Dienstleistungen sind beschrieben.
- ✓ Alle Prozesse, die nicht berücksichtigt werden, sind beschrieben und begründet.
- ✓ Darstellung der Systeme (IT), die zum Scope gehören (Netzwerk Übersicht).
- ✓ Darstellung der Systeme (IT), die nicht zum Scope gehören (z.B. Forschung).
- ✓ Ausgelagerte Prozesse sind dargestellt wie z.B. Druckersysteme / -wartung, IT Dienstleister.
- ✓ Kooperationspartner, die für die medizinische Versorgung wichtig sind (Labor, Pathologie, Einkauf), sind dargestellt; ggf. Überschneidung mit Darstellung der Prozesse.

Empfohlene Literatur

1. BSI-Gesetzes (BSIG)
2. BSI-Kritisverordnung (BSI-KritisV)
3. Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus
4. Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3
5. BSI Grundschutz Dokumente

Abbildungsverzeichnis