IT-Governance in der integrierten Versorgung – eine risikobezogene Betrachtung

Lena Otto[1], Hannes Schlieter[1]

[1] Professur für Wirtschaftsinformatik, insb. Systementwicklung, Technische Universität Dresden, Dresden, Deutschland
{lena.otto, hannes.schlieter}@tu-dresden.de

Abstract. IT-Governance ist in der Industrie wie auch in der Gesundheitswirtschaft inzwischen eine zentrale Aufgabe zur Sicherstellung rechtskonformer und sicherer Prozesse. IT-Governance-Rahmenwerke und die darin vorgeschlagenen Risikomanagementansätze helfen dabei, die Risiken, die mit der Einrichtung und dem Betrieb von IT-Systemen verbunden sind, aktiv in die Managementprozesse einzubeziehen. Jedoch kommt durch die Fokussierung auf das unternehmensinterne Risikomanagement die netzwerkbezogene Betrachtung in bestehenden Governance-Rahmenwerken häufig zu kurz. Im vorliegenden Beitrag wird daher untersucht, inwieweit bestehende Risikomanagementansätze angewendet werden können, um die Verfügbarkeit, Integrität und Vertraulichkeit von Unternehmens- und Patientendaten in Anwendungssystemen der integrierten Versorgung sicherzustellen. Dabei wird deutlich, wie insbesondere der erhöhte Koordinationsbedarf und die rechtliche Autonomie der Netzwerkpartner das Risikomanagement in interorganisationalen Anwendungssysteme beeinflussen. Abschließen werden Schwachstellen in den bestehenden Rahmenwerken aufgezeigt.

Keywords: Integrierte Versorgung, IT-Risikomanagement, IT-Governance-Rahmenwerke, COBIT, ITIL

1 Einleitung

Durch zunehmende Komorbiditäten, Kostendämpfungszwänge und den Anspruch einer durchgehenden Patientenversorgung rücken Modelle der integrierten Versorgung immer stärker in den Fokus. Die relativ geringe Durchdringung des Gesundheitswesens mit integrierten Versorgungsmodellen und kooperativen Versorgungsformen führt dazu, dass sich bisher noch keine Standards für den Aufbau und Betrieb von Netzwerken der integrierten Versorgung durchgesetzt haben. Dies ist v. a. bei der Gestaltung von integrierten Anwendungssystemlandschaften relevant, mithilfe derer große Mengen sensibler Daten übertragen bzw. gemeinsam verarbeitet werden [1]. Für medizinische Versorgungsprozesse wird eine hohe Kompatibilität von Anwendungssystemen benötigt, deren Grundlage verfügbare und integre Daten darstellen [2]. Die hohe Intimität der Patientendaten [3] erfordert zusätzlich die Sicherstellung der Vertraulichkeit. Darüber hinaus können Risiken wie Feuer,

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Cyberangriffe oder Fehlbedienung die Informationssicherheit gefährden [4]. Zur frühzeitigen Vermeidung des Eintritts von Risiken verankert ein Risikomanagement Regeln zur Prävention von und zum Umgang mit solchen Risiken [5]. IT-Governance-Rahmenwerke leiten typischerweise den Aufbau und die Durchführung von Risikomanagement an [6]. Bestehende IT-Governance-Rahmenwerke adressieren jedoch häufig nur den unternehmensinternen Governance-Aspekt [7] und wurden bisher wenig für Netzwerkverbünde, insbesondere in der integrierten Versorgung, untersucht.

Das Ziel des Beitrages ist es, die Anwendung solcher IT-Governance-Rahmenwerke für die Gestaltung von Risikomanagementsystemen in Netzwerkorganisationen zu verbessern. Dafür wird die Möglichkeit des Einsatzes der Rahmenwerke für Anwendungssysteme in Netzwerkorganisationen literaturgestützt evaluiert und Gestaltungsempfehlungen zu deren Nutzung abgeleitet. Damit leistet die vorliegende Arbeit einen Beitrag zum Thema IT-Governance innerhalb der integrierten Versorgung, womit die Wahrung von Verfügbarkeit, Vertraulichkeit und Integrität als wesentliche Schutzziele einhergeht. Folgende Forschungsfrage steht damit im Zentrum der Untersuchung:

- Wie können bestehende IT-Governance-Rahmenwerke für das Management von IT-Risiken in integrierten Versorgungsnetzwerken eingesetzt werden und wo weisen sie ggf. Schwachstellen auf?

Der Beitrag ist wie folgt aufgebaut: Zunächst wird der Stand der Forschung aufgearbeitet. Dazu werden die am weitesten verbreiteten IT-Governance-Rahmenwerke mit Bezug zum Risikomanagement [8,9] (COBIT [10], ITIL [11] und ISO/IEC 27005:2011 [12]) betrachtet sowie die terminologischen Grundlagen gelegt. Weiterhin werden die Charakteristika der integrierten Versorgung aufgezeigt. Im Abschnitt 3 wird auf Basis der zuvor aufgearbeiteten Kriterien ein Evaluationsrahmen aufgebaut, anhand dessen im Abschnitt 4 die Evaluierung hinsichtlich der Ausgestaltung von Risikomanagement untersucht und die Anwendung ausgewählter IT-Governance-Rahmenwerke in der integrierten Versorgung analysiert wird. Die Arbeit schließt mit einer Diskussion der Ergebnisse und präsentiert Gestaltungsempfehlungen für eine bedarfsgerechte Nutzung der IT-Governance-Rahmenwerke.

2 Begriffliche Grundlagen

2.1 IT-Governance und IT-Risikomanagement

Das Ziel von IT-Governance ist es, Geschäftsziele mit Hilfe von IT-Prozessen zu erreichen, indem Werte generiert und Risiken minimiert werden [13,14]. Im engeren Sinn sind nicht alle der ausgewählten Rahmenwerke reine Instrumente der IT-Governance[1], obwohl sie in der Literatur als solche bezeichnet werden [8].

Entsprechend ihres initialen Entwicklungskontextes sind die ausgewählten IT-Governance-Rahmenwerke recht unterschiedlich ausgerichtet. COBIT liefert beispielsweise einen Governance-Ansatz für das gesamte Unternehmen [7]. ITIL hingegen fokussiert auf den Lebenszyklus von IT-Services und stellt dafür Best Practices zur Verfügung [16]. Demgegenüber definiert die ISO 27005 einen generischen Rahmen zur Ausgestaltung von IT-Risikomanagement und adressiert dabei den Aspekt der Informationssicherheit [17].

Risikomanagement dient der präventiven Abschwächung potentieller Risiken und beschreibt die Prozessschritte Definition einer Risikostrategie, Identifikation und Analyse, Bewertung, Steuerung und Überwachung von Risiken [18,5]. Gleichzeitig sind Informationen und deren Schutz ein zentraler Aspekt von Anwendungssystemen, an dem auch die Risikoidentifikation ansetzt. Insbesondere werden Informationssicherheit, und damit Verfügbarkeit, Integrität und Vertraulichkeit [2], als wesentliche Schutzziele benannt. Unterschiedlichste Ereignisse im Unternehmensalltag können eine Gefahr für diese genannten Schutzziele und somit ein unmittelbares Risiko darstellen. So können bspw. Brände die Verfügbarkeit oder Schadsoftware die Integrität bzw. Vertraulichkeit von Daten beeinträchtigen, woraus auch wirtschaftliche und rechtliche Risiken erwachsen können. Wenn von IT-Risiken gesprochen wird, steht der automatisierte Teil des Informationssystems, das sogenannte Anwendungssystem, im Vordergrund. Somit muss ein IT-Risikomanagement auch dessen wesentliche Bestandteile Hardware, System- und Anwendungssoftware beachten [19].

Die zentralen Risikokategorien ergeben sich dabei aus der internen Betrachtungsebene, welche die Risiken durch beteiligte Personen, Prozesse und Systeme adressiert, sowie den externen Risiken, welche die umliegenden Gegebenheiten berücksichtigen [20,4].

2.2 Besonderheiten in der integrierten Versorgung

Der Begriff der integrierten Versorgung ist im Zuge der Hinwendung zu einer kooperativen Versorgungslandschaft entstanden [21]. Er adressiert insbesondere die Spezifika von Netzwerkorganisationen, die Gestaltung unternehmensübergreifender Anwendungssystemlandschaften und die Besonderheiten von Interorganisations-

[1] Der Fokus von ITIL liegt primär auf dem Lebenszyklus-Management von Anwendungssystem-landschaften [15]. In der ISO 2700x Normenfamilie wird ausschließlich Risikomanagement von Informationssicherheit behandelt. Somit adressieren beide Rahmenwerke nur Teildisziplinen der IT-Governance [8].

systemen im Allgemeinen. Unter einem Interorganisationssystem, oder synonym auch interorganisationalen Informationssystem, werden Informationssysteme verstanden, die von mehreren Unternehmen gemeinsam genutzt werden [22]. Informationen werden dabei auch über Unternehmensgrenzen hinweg verarbeitet [23]. Somit ist ein interorganisationales Anwendungssystem der automatisierte Teil eines unternehmensübergreifend genutzten Informationssystems [19]. Die Datenhaltung kann sowohl zentral als auch dezentral (durch Integration der einzelnen Informations-/ Anwendungssysteme) erfolgen.

Aufbau. Im Aufbau ist neben der größeren Anzahl an Komponenten (Hard- und Software) sowie involvierten Administratoren und Benutzern insbesondere die notwendige sichere Verbindung zwischen den einzelnen Anwendungssystemen charakteristisch für interorganisationale Anwendungssysteme [23].

Organisationsform. Auch die veränderte Organisationsform, der Zusammenschluss in einem Unternehmensnetzwerk, bringt spezielle Charakteristika und Herausforderungen mit sich. So zeichnen sich Unternehmensnetzwerke durch komplexe, relativ stabile gegenseitige Beziehungen mit vertraglicher Bindung zwischen rechtlich selbstständigen, wirtschaftlich jedoch abhängigen Teilnehmern aus, denen ein spezieller Zweck zugrunde liegt (und die somit wieder trennbar sind) [24]. Dabei hat das Management keine Weisungsbefugnis [25], wodurch alle Leistungserbringer im Rahmen der Führung eingebunden werden [26]. Damit für alle Teilnehmenden am Netzwerk Vorteile generiert werden, ergeben sich Herausforderungen, die eine sinnvolle Organisation von Unternehmensnetzwerken mit sich bringt. Sie befinden sich in den Spannungsfeldern zwischen Markt und Hierarchie, Wettbewerb und Kooperation, Autonomie und Abhängigkeit, Flexibilität und Spezifität, Vielfalt und Einheit, Vertrauen und Kontrolle, Stabilität und Fragilität, Formalität und Informalität sowie ökonomischem Handeln und Herrschaftssicherung [27]. Jedes Unternehmensnetzwerk positioniert sich in all diesen Spannungsfeldern unterschiedlich. Im Rahmen der integrierten Versorgung in Deutschland sieht diese Positionierung wie folgt aus: Nach §140a SGB V [28] können Verträge der besonderen Versorgung zwischen Krankenkassen und verschiedenen Leistungserbringern geschlossen werden. Die integrierte Versorgung ist somit marktbezogen und die einzelnen Leistungserbringer kooperieren, obwohl sie bei gleicher Versorgungsstufe auch konkurrieren können. Die einzelnen Leistungserbringer agieren sehr autonom, spezifisch und vielfältig, da der Zusammenschluss zum Zwecke der Aufgabentrennung je nach Spezifikation vorgenommen wird. Ähnliches gilt für das Vertrauen, da keine überwachende Kontrollinstanz i.e.S. vorgesehen ist. Die vertragliche Bindung mit der Krankenkasse garantiert einen stabilen Zusammenschluss und hohe Formalität zwischen den Leistungserbringern sowie ökonomisches Handeln.

Interorganisationssysteme. Durch die Informationsverarbeitung über Unternehmensgrenzen hinweg ergeben sich auch bei Interorganisationssystemen Unterschiede im Vergleich zu Informationssystemen innerhalb eines einzelnen Unternehmens. Diese sind zusammengefasst in Tabelle 1 zu finden.

Es bleibt festzuhalten, dass insbesondere die Systeme und Prozesse in der integrierten Versorgung anders ausgestaltet sind als in einer einzelnen Einrichtung. In der Realität der integrierten Versorgung sind die Merkmale vornehmlich wie in Tabelle 1, Spalte 3 ausgeprägt, was Auswirkungen auf die spätere Evaluation hat.

Tabelle 1. Spezifika interorganisationaler Informationssysteme

	Allgemeine Ausprägungsmerkmale	*Typ. Ausprägung in der integrierten Versorgung*
(I)	Austausch / gemeinsame Verwendung von Daten und Anwendungen [29,24]	Lose gekoppelte Anwendungssysteme
(II)	Gefahr heterogener Sicherheitskonzepte [29]	Fokus auf unternehmens-internen Sicherheits-konzepten
(III)	Zentrale / dezentrale Datenhaltung [29,24]	Dezentrale Datenhaltung
(IV)	Kontrollbefugnis bei mehreren Unternehmen [30]	Kontrollbefugnis durch jeweiligen Netzwerkpartner
(V)	Schnittstellenmanagement notwendig (kann bei falscher Ausführung zu System- / Medienbrüchen und Dateninkonsistenzen führen) [29,24]	Keine standardisierten Schnittstellen
(VI)	(einseitige) Abhängigkeitsverhältnisse möglich [29]	Geringe Abhängigkeit
(VII)	Meist standardisierte Systeme [29]	Wenig standardisiert
(VIII)	Zentrale / dezentrale Verfügungsrechte [29]	Sowohl zentral als auch dezentral
(IX)	Hohe Systemsicherheit bzgl. Daten und Transaktionen [29]	
(X)	Flexible Teilnehmerzahl möglich [29]	Flexible Teilnehmerzahl
(XI)	Räumliche Verteilung der Netzwerkbeteiligten [29]	Regionale Verteilung
(XII)	Intensitätsgrad der Zusammenarbeit [24]	Geringe Intensität

3 Ableitung Evaluationsrahmen

Zum Aufbau des Evaluationsrahmens müssen einheitliche Evaluationskriterien definiert werden, anhand derer im weiteren Verlauf der Evaluationsgegenstand (COBIT, ITIL und ISO 27005) geprüft wird. Eine wesentliche Herausforderung des Risikomanagements ist dessen Integration in einen geregelten Unternehmensprozess (siehe Abs. 2.1). Demnach sollte ein IT-Governance-Rahmenwerk Gestaltungsempfehlungen für den IT-Risikomanagementprozess geben. Typischerweise erstrecken sich diese über die Phasen: *Definition einer Risikostrategie* (1), *Identifikation und Analyse* (2), *Bewertung* (3), *Steuerung* (4), *Überwachung* (5) der Risiken (siehe Kategorie: *Abdeckung des gesamten Risikomanagementprozesses*). Weiterhin muss die Berücksichtigung der Schutzziele *Verfügbarkeit, Integrität und Vertraulichkeit* (6) verankert sein. Durch den Betrachtungsfokus auf Anwendungssystemen ist es notwendig, dass in IT-Governance-Rahmenwerken auf die Komponenten *Hard-* (7) und *Software* (8) sowie auf beteiligte *Personen* (9) als möglichen Gegenstand der Untersuchung eingegangen wird.

Weitere zu evaluierende Kriterien sind die genannten *Risikokategorien der Personen-* (10), *Prozess-* (11) und *System-* (12) sowie *externen Risiken* (13) und die *generelle Passfähigkeit aufgrund der Charakteristika* der Rahmenwerke (14).

Anhand der definierten Kriterien werden die drei gewählten Rahmenwerke einem Vergleich bezüglich ihrer Anwendbarkeit auf Risikomanagement intraorganisationaler Anwendungssysteme in Abschnitt 4.1 unterzogen. Nach der prinzipiellen Eignungsfeststellung erfolgt die Prüfung der Übertragbarkeit auf interorganisationale Anwendungssysteme im Kontext der integrierten Versorgung. Zur Feststellung der Übertragbarkeit der Ergebnisse müssen die Charakteristika der integrierten Versorgung einbezogen werden.

4 Evaluation

4.1 Analyse der intraorganisationalen Anwendung

Mit Blick auf die Evaluationskriterien stellt sich COBIT als eines der umfänglichsten IT-Governance-Rahmenwerke dar. COBIT adressiert alle der zuvor aufgestellten Kriterien und gibt detaillierte Erläuterungen zu einzelnen Schritten und Komponenten [7]. Dennoch besteht die Gefahr, dass die Komplexität des Rahmenwerkes dessen Anwendbarkeit negativ beeinflusst [15]. Da bei ITIL der Lebenszyklus von IT-Services und deren Management im Vordergrund stehen, weist ITIL einige Schwachstellen bei der Betrachtung des Risikomanagementprozesses auf [31]. So wird zwar von Risiken im Allgemeinen gesprochen, aber nicht auf konkrete Risikokategorien, wie Prozess- oder Systemrisiken eingegangen. Anders ist es hingegen in der ISO 27005, welche die definierten Evaluationskriterien umfassend berücksichtigt (siehe Tabelle 2).

Tabelle 2. Zusammenfassung der Evaluationsergebnisse bzgl. der Passfähigkeit für das unternehmensinterne IT-Risikomanagement

Kategorie	*COBIT*	*ITIL*	*ISO 27005*
Abdeckung des Risikomanagementprozesses:			
(1) Definition einer Risikostrategie	✓	□	✓
(2) Identifikation und Analyse	✓	✓	✓
(3) Bewertung	✓	✓	✓
(4) Steuerung	✓	✓	✓
(5) Überwachung	✓	□	✓
(6) Fokus auf Verfügbarkeit, Integrität, Vertraulichkeit	✓	✓	✓
Einbeziehung der Komponenten			
(7) Hardware	✓	✓	✓
(8) Software	✓	✓	✓
(9) Personen	✓	✓	✓
Berücksichtigte Risikokategorien:			
(10) Personenrisiken	✓	✓	✓
(11) Prozessrisiken	✓	□	✓
(12) Systemrisiken	✓	□	✓
(13) Externe Risiken	✓	□	✓
(14) Prinzipielle Eigenschaften	x	x	✓

Legende:

Kriterium vollständig erfüllt	Kriterium teilweise erfüllt	Kriterium nicht erfüllt
✓	□	x

Wie dargestellt, unterstützen die untersuchten Rahmenwerke das Risikomanagement unternehmensinterner Anwendungssysteme weitestgehend. Kleinere Abstriche müssen bei ITIL gemacht werden, da hier die Definition einer Risikostrategie sowie der Umgang mit Prozess-, System- und externen Risiken nur wenig berücksichtigt werden.

4.2 Analyse der interorganisationalen Anwendung

Zur Evaluierung der Einsatzfähigkeit der Rahmenwerke für das Risikomanagement innerhalb von Netzwerken der integrierten Versorgung werden nun die in Abschnitt 2.2 erarbeiteten Besonderheiten (I-XII) der integrierten Versorgung mit in die Bewertung einfließen. Ergänzend zu den bestehenden Bewertungskategorien wird dem Evaluierungsrahmen in Tabelle 3 eine weitere Kategorie hinzugefügt. Dies soll eine bessere Differenzierung der Ergebnisse ermöglichen. Wird ein Kriterium mit „-“ bewertet, so adressiert das Rahmenwerk das Kriterium zwar abstrakt, konkretisiert es aber nicht hinsichtlich der Einsetzbarkeit in integrierten Versorgungsnetzwerken.

Obwohl die Prozessschritte des Risikomanagements weiterhin in den Rahmenwerken berücksichtigt werden (siehe Tabelle 2), erfüllen sie dennoch nicht die Ansprüche integrierter Versorgungsnetzwerke. Für jeden der Schritte ist mindestens teilweise eine Konsensbildung zwischen allen Netzwerkteilnehmern erforderlich, da diese trotz rechtlicher Unabhängigkeit wirtschaftlich voneinander abhängig sind. Die

Risikostrategie muss einheitlich definiert werden und Risiken, die durch den Zusammenschluss der einzelnen Beteiligten entstehen, müssen übergreifend identifiziert und analysiert werden. Für eine einheitliche Bewertung, Steuerung und Überwachung sind auch dort gemeinsame Absprachen wichtig, insbesondere da in integrierten Versorgungsnetzwerken geringe Abhängigkeit (VI) und Intensität der Zusammenarbeit (XII) sowie hohe regionale Verteilung der Netzwerkteilnehmer (XI) herrschen. Auf diese Besonderheiten der Unternehmensnetzwerke wird in keinem der Rahmenwerke explizit eingegangen. In COBIT erfolgt eine Berücksichtigung von Anforderungen von Statusgruppen, aber keine ausdrückliche Beachtung von Unternehmensnetzwerken. ITIL erwies sich bereits für intraorganisationale Anwendungssysteme als nur teilweise geeignet. In ISO 27005 existiert ein Verweis, dass es für alle Arten von Unternehmen geeignet ist, ohne dass Besonderheiten von Unternehmensnetzwerken berücksichtigt werden. Anleitungen zur Durchführung der einzelnen Schritte bleiben (v. a. in COBIT und ISO) erhalten, teilweise mit Beispielen. Dennoch werden notwendige integrierte Managementprozesse und Absprachen zwischen mehreren Unternehmen nicht berücksichtigt. Es werden auch keine Lösungen für die Probleme der fehlenden Weisungsbefugnis des Managements, der wenigen Kontrollbefugnis bei (IV) sowie der Abhängigkeit von anderen Unternehmen (insbesondere beim Sicherheitskonzept – VI/II), flexibler Teilnehmerzahl (X) und zusätzlichem Schnittstellenmanagement (V), die Änderungen im Risikomanagement hervorrufen, bereitgestellt. Daher wird die Bewertung verringert (1-5).

Das Kriterium der Verfügbarkeit, Integrität und Vertraulichkeit (6) ist für intra- und interorganisationale Anwendungssysteme gleichermaßen adressiert und damit als erfüllt einzustufen. Aus der integrierten Versorgung erwachsen keine weiteren Aspekte. Herausforderungen sind in der operativen Sicherstellung der Merkmale zu erwarten.

Ein weiterer Aspekt ist die Interoperabilität, die möglichst ohne Risikozuwachs auf allen Ebenen (rechtlich, organisatorisch, semantisch und technisch) sichergestellt werden muss [32]. Obwohl sich intra- und interorganisationale Anwendungssysteme hinsichtlich der Komponenten (Hard- und Softwaresysteme) nicht unterscheiden, erhöht sich bei interorganisationalen die Anzahl involvierter Hard- und Softwaresysteme. Zwischen diesen müssen adäquate Schnittstellen (V) etabliert werden. Insbesondere durch die nur lose gekoppelten Anwendungssysteme (I) sowie die fehlenden standardisierten Schnittstellen und Systeme (VII) innerhalb der integrierten Versorgungsnetzwerke ist dieser Aspekt bedeutend. Zusätzlich erhöht sich auch die Anzahl involvierter Nutzer und Administratoren gegenüber einem einzelnen intraorganisationalen Anwendungssystem. Die Einbeziehung all dieser, teilweise evtl. auch an Schnittstellen eingesetzten, Personen in das Risikomanagement muss sichergestellt werden. Keines der Rahmenwerke gibt explizite Anleitungen für eine dieser Gestaltungsebenen. Im Gegenteil liegt der Fokus auf einzelnen Organisationen und deren ganzheitlicher Betrachtung [7]. Zwar wird für die ISO 27005 deren Anwendbarkeit auf alle Arten von Organisationen festgelegt, eine Berücksichtigung der Charakteristika von Unternehmensnetzwerken fehlt dennoch. Der wesentliche Unterschied liegt in der Unabhängigkeit der einzelnen Netzwerkteilnehmer (VI), die primär ihre eigene Perspektive einnehmen. Eine explizite Berücksichtigung der Netzwerkperspektive und somit der Gesamtsicht muss garantiert werden. Jedoch gibt

es auch dafür keine adäquate Anweisung in einem der Rahmenwerke. Auch hier muss die Bewertung der Kriterien (7-9) entsprechend verringert werden.

Die Risikokategorien und ihre Berücksichtigung in den Rahmenwerken bleiben auch für Unternehmensnetzwerke in der integrierten Versorgung gleich (insbesondere in COBIT und ISO). Die komplexen Beziehungen, regionale Verteilung (XI) wenig intensiv zusammenarbeitender Partner (XII) und die geringe Abhängigkeit (VI) unter den Netzwerkteilnehmer können zu Problemen hinsichtlich notwendiger Absprachen führen. Zusätzlich ergeben sich Änderungen in der Bewertung, insbesondere der Eintrittswahrscheinlichkeit dieser Risikokategorien. Bspw. kann Misstrauen zwischen den einzelnen Netzwerkteilnehmern die Personenrisiken verstärken, während die lose Kopplung der Anwendungssysteme (I) mit nicht standardisierten Schnittstellen (VII) in der integrierten Versorgung eine hohe Gefahr für inkonsistente Daten innerhalb der Prozessrisiken darstellen. Ergänzend dazu sind weitere Absprachen zur einheitlichen Bewertung notwendig. Keines dieser Charakteristika ist in den Rahmenwerken enthalten, was zu entsprechender Verringerung der Kriterienbewertung (10-13) führt.

Unabhängig von der genannten fehlenden Berücksichtigung von Unternehmensnetzwerk-Spezifika ändert sich an der Bewertung der prinzipiellen Eigenschaften (14) nichts. Die gesamte Bewertung ist in Tabelle 3 dargestellt.

Tabelle 3. Übertragbarkeit der Passfähigkeit der Rahmenwerke auf die integrierte Versorgung

Kategorie	*COBIT*	*ITIL*	*ISO 27005*
Abdeckung des Risikomanagementprozesses:			
(1) Definition einer Risikostrategie	–	□	–
(2) Identifikation und Analyse	–	–	–
(3) Bewertung	–	–	–
(4) Steuerung	–	–	–
(5) Überwachung	–	□	–
(6) Fokus auf Verfügbarkeit, Integrität, Vertraulichkeit	✓	✓	✓
Einbeziehung der Komponenten			
(7) Hardware	–	–	–
(8) Software	–	–	–
(9) Personen	–	–	–
Berücksichtigte Risikokategorien:			
(10) Personenrisiken	–	–	–
(11) Prozessrisiken	–	□	–
(12) Systemrisiken	–	□	–
(13) Externe Risiken	–	□	–
(14) Prinzipielle Eigenschaften	x	x	✓

Legende:

Kriterium vollständig erfüllt	Kriterium teilweise erfüllt	Kriterium nicht erfüllt	Kriterium erfüllt, aber ohne Berücksichtigung von Besonderheiten in Unternehmensnetzwerken
✓	□	x	–

Es bleibt festzuhalten, dass von den drei evaluierten Rahmenwerken keines die Kriterien vollumfänglich erfüllt. COBIT und ITIL waren mit Blick auf das intraorganisationale Risikomanagement von Anwendungssysteme bereits nur teilweise oder nicht passfähig. Durch die Besonderheiten der integrierten Versorgung verringert sich die Bewertung und auch die ISO 27005 kann nur teilweise den Anforderungen gerecht werden (insbesondere im Umgang mit spezifischen Schutzzielen).

5 Diskussion und Fazit

Die drei am meisten verwendeten und auf Risikomanagement ausgerichteten Rahmenwerke COBIT, ITIL und ISO 27005 wurden hinsichtlich ihrer Verwendbarkeit für Unternehmensnetzwerke in der integrierten Versorgung untersucht. Es konnte gezeigt werden, dass die Anwendung der evaluierten IT-Governance-Rahmenwerke mit einer Vielzahl von Einschränkungen einhergeht. Insbesondere muss dabei festgestellt werden, dass durch den gewählten Abstraktionsgrad und die mangelnde Explikation des Netzwerkes als Gestaltungsgegenstand die konkrete Anwendung weitestgehend offenbleibt. Nicht erfüllte Anforderungen der Rahmenwerke umfassen insbesondere die Berücksichtigung von Absprachen, fehlende Weisungsbefugnis und Kontrolle (des Managements) sowie die flexible Teilnehmerzahl und zusätzliche Interoperabilität, inkl. Schnittstellenmanagement, die sich aus einem Zusammenschluss im Unternehmensnetzwerk der integrierten Versorgung ergeben. Alle untersuchten Rahmenwerke beschreiben zwar die Schritte des Risikomanagementprozesses und berücksichtigen den Fokus auf Verfügbarkeit, Integrität und Vertraulichkeit sowie alle Arten von Betriebsrisiken allgemein, die Betrachtung der Anwendung in Unternehmensnetzwerken bleibt jedoch aus. In der weiteren Forschung können die gewonnen Ergebnisse in den Gestaltungsprozess für die Entwicklung eines spezifischen, auf die integrierte Versorgung ausgerichteten Risikomanagement-Werkzeugs einfließen. Hierzu sollte ein Ansatz erarbeitet werden, der die Stärken bestehender Rahmenwerke zusammenfasst und um Anforderungen der interorganisationalen Arbeit erweitert. Beispielsweise bietet sich eine Verbindung aus der klaren Struktur der ISO, ergänzt um ausführliche Erläuterungen aus COBIT und praxiserprobte Angaben von ITIL an. Die Generalisierung und Übertragbarkeit der Ergebnisse auf Unternehmensnetzwerke weiterer Branchen und verschiedene Organisations- und Netzwerkgrößen ist zu untersuchen.

Ausgehend von den identifizierten Defiziten ist die Berücksichtigung folgender fünf Anforderungen vorzunehmen, die in den Erstellungsprozess eines domänenspezifischen Rahmenwerkes einfließen können:

- Anf. 1 - **Unternehmensübergreifende Managementprozesse**: Ein expliziter Hinweis auf die erhöhte Notwendigkeit von Absprachen im Rahmen der meisten Schritte des Risikomanagementprozesses
- Anf. 2 - **Übertragung von Verantwortung**: Anleitungen zum Festlegen von Verantwortlichkeiten bzgl. ganzheitlicher Kontrolle aller gemeinsamen Prozesse
- Anf. 3 - **Regeln bei Veränderungen der Beteiligten**: Die Sicherstellung von Verantwortlichkeiten auch bei wechselnden Teilnehmern (bspw. über eine

ausreichende Anzahl festgelegter Stellvertreter oder dem Einführen von Prozessschritten, die bei Austritt von verantwortlichen Personen greifen)
- Anf. 4 - **Interoperabilität**: Ein expliziter Hinweis auf die verschiedenen Ebenen der Interoperabilität und der Notwendigkeit, diese sicherzustellen
- Anf. 5 - **Ganzheitliche Managementprozesse**: Ein expliziter Hinweis auf die Notwendigkeit eines ganzheitlichen Schnittstellenmanagements (evtl. durch Definition von Verantwortlichen).

Zusammenfassend ist zu konstatieren, dass mit der vorliegenden Untersuchung gezeigt werden konnte, welche Einschränkungen mit der Anwendung bestehender IT-Governance-Rahmenwerke in Netzwerken der integrierten Versorgung einhergehen. Mit der finalen Ableitung von Kernanforderungen wurde die Basis für das Zusammenwachsen der IT-Landschaften in der integrierten Versorgung gelegt.

Referenzen

1. Henriksen, E., Burkow, T., Johnsen, E., Vognild, L.: Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. BMC Medical Informatics & Decision Making, 13, 1-13 (2013)
2. Zambon, E., Etalle, S., Wieringa, R.J., Hartel, P.: Model-based qualitative risk assessment for availability of IT infrastructures. Software Systems Modeling 10, 553-580 (2011)
3. Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097) geändert worden ist
4. Wolke, T.: Risikomanagement. De Gruyter Oldebourg, Berlin (2015)
5. Jakolow-Standke, A.: Beschwerde- und Risikomanagement. In: Debatin, J:F:, Ekkernkamp, A., Schulte, B., Tecklenburg, A. (Hrsg.) Krankenhausmanagement : Strategien, Konzepte, Methoden. 2., aktualisierte und erweiterte Auflage. MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin (2013)
6. Helmke, S., Uebel, M.: Leit- und Leistungsbild der IT. In: Helmke, S., Uebel, M. (Hrsg.): Managementorientiertes IT-Controlling und IT-Governance, 15-37, Springer Gabler, Wiesbaden (2016)
7. Gaulke, M.: Praxiswissen COBIT – Grundlagen und praktische Anwendung in der Unternehmens-IT. dpunkt.verlag, Heidelberg (2014)
8. Johannsen, W., Goeken, M.: Referenzmodelle für IT-Governance: Strategische Effektivität und Effizienz mit COBIT, ITIL &Co. dpunkt.verlag, Heidelberg (2007)
9. Häfner, C., Felden, C.: Building a Framework for an Efficient IT Governance. Freiberger Forschungshefte 231, Freiberg (2009)
10. ISACA: COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT (2012)
11. AXELOS: ITIL Service Design. The Stationery Office, London (2013)
12. ISO - International Organization for Standardization: International Standard ISO/IEC 27005:2011(E) – Information technology; Security techniques; Information security risk management (2011)
13. Bienert, P., Wildhaber, B.: IT-Governance: Strategische Führung und Kontrolle von Informationssystemen als Teil der New Corporate Governance. Forte Advisors, Glattzentrum (2007)

14. Rüter, A., Schröder, J., Göldner, A., Niebuhr, J. (Hrsg.): IT-Governance in der Praxis. Springer-Verlag, Berlin, Heidelberg (2010)
15. De Haes, S., Van Grembergen, W., Debreceny, R.S.: COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems 27, 307-324 (2013)
16. Sahibudin, S., Sharifi, M., Ayat, M.: Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. In: Proceedings – 2nd Asia International Conference on Modelling and Simulation, pp. 749-753. IEEE Press, New York (2008)
17. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. Information Management & Computer Security, 22, 410-430 (2014)
18. Cagliano, A.C., Grimaldi, S., Rafele, C.: A systemic methodology for risk management in healthcare sector. Safety Science 49, 695-708 (2011)
19. Ferstl, O.K., Sinz, E.J.: Grundlagen der Wirtschaftsinformatik, Oldenbourg Verlag, München (2013)
20. Bistarelli, S., Fioravanti, F., Peretti, P., Santini, F.: Evaluation of complex security scenarios using defense trees and economic indexes. In: Journal of Experimental & Theoretical Artificial Intelligence 24, 161-192 (2012)
21. Smith, D.L., Bryant, J.H.: Building the Infrastructure for Primary Health Care: An Overview of Vertical and Integrated Approaches. Social Science & Medicine 26, 909-917 (1988)
22. Cash, J.I., Konsynski, B.R.: IS Redraws Competititve Boundaries. Harvard Business Review 2, 134-142 (1985)
23. Johnston, R.H.; Vitale, M.R.: Creating Competitive Advantage With Interorganizational Information Systems. MIS Quarterly 12, 153-165 (1988)
24. Schüppler, D.: Informationsmodelle für überbetriebliche Prozess: Ein Ansatz zur Gestaltung von Interorganisationssystemen. Lang, Frankfurt am Main; Berlin [u.a.] (1998)
25. Bogenstahl, C.: Management von Netzwerken: Eine Analyse der Gestaltung interorganisationaler Leistungsaustauschbeziehungen. Gabler, Wiesbaden (2012)
26. Hildebrandt, H., Stunder, B.H., Wetzel, M., Gröne, O.: Erfolgsfaktoren für Netze und regionale Gesundheitsorganisationen: Organisationsformen, Führung, Patientenorientierung. In: Eble, S., Kurscheid, C. (Hrsg.): Gesundheitsnetzwerke: Strategien, Konzepte, Methoden. MWV, Berlin (2013)
27. Sydow, J.: Strategische Netzwerke: Evolution und Organisation. Gabler, Wiesbaden (1992)
28. Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 4 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214) geändert worden ist
29. Raupp, M.: Informationsmanagement und strategische Unternehmensführung. Lang, Frankfurt am Main; Berlin [u.a.] (2002)
30. Suomi, R.: On the Concept of Inter-organizational Information Systems. Journal of Strategic Information Systems, 2, 93-100 (1992)
31. Vilarinho, S., da Silva, M.M.: Risk Management Model in ITIL. In: Cruz-Cunha, M.M., Varajão, J., Powell, P., Martinho, R. (Hrsg.) ENTERprise Information Systems. CENTERIS 2011. Communications in Computer and Information Science 220, 306-314. Springer, Berlin, Heidelberg (2011)
32. European Commission: ANNEX to the European Interoperability Framework – Implementation Strategy COM(2017) 134 final. Brüssel (2017)