IT-Governance in Integrated Care: A Risk-centred Examination in Germany

Lena Otto[a]
Chair of Wirtschaftsinformatik, esp. Systems Development, Technische Universität Dresden, Dresden, Germany

Keywords: IT Risk Management, Integrated Care Networks, IT Governance Frameworks, Evaluation, Information Security.

Abstract: Health care systems face several challenges regarding costs and effectiveness. Integrated care networks and usage of application systems (as automated part of information systems) are two approaches to overcome these challenges. To fully reach their potential, a seamless process is mandatory. IT governance frameworks help health care organisations to implement an integrative risk management. Nevertheless, a network-centred approach, e.g. necessary for integrated care networks, is not in focus of existing frameworks, such as COBIT or ITIL. Therefore, the following article evaluates how selected frameworks can be used for risk management. A literature analysis and a case study of the German health care system are conducted focussing on confidentiality, integrity, and availability in integrated care networks' application systems. Findings suggest that inter-organisational risk management is especially influenced by the increased need for coordination and the autonomy of network partners. Finally, the main aspects necessary for using the evaluated frameworks within an integrated care context are shown.

1 INTRODUCTION

The German health care system is one of the most expensive worldwide while at the same time being one with very high-quality standards. However, the increasing effects of demographic change together with comorbidities enforce a focus on integrated care, where different actors are combined along the care continuum (Gröne et al., 2001). To transfer and use the highly sensitive data in the health care sector for ensuring the cooperation of actors requires the development of safe and secure application systems (Henriksen et al., 2013) as well as high compatibility of these systems to ensure available and sound data (Zambon et al., 2011), i.e. to guarantee information security. Information security as well as other business objectives, e.g. integrated care cooperation, rely on successful information technology (IT) provision (Bannerman, 2008), which can be disturbed by different risks. These risks include technical or human failures as well as external events, e. g. fire. To prevent and handle these risks (Agrawal, 2009), risk management measures can be applied (Silva et al., 2014). A clear guidance on how to implement and execute risk management is, among others, provided by IT governance frameworks (Alreemy et al., 2016). However, they mainly address the internal governance (Gaulke, 2014) and have rarely been analysed in the context of networks, especially integrated care networks. This leads to the following research question:

How can existing IT governance frameworks be adapted for the management of IT risks in integrated care networks and what are possible weaknesses?

The aim of this paper is to improve the understanding and use of IT governance frameworks to implement an adequate risk management in network organisations. Based on a literature study, the feasibility for using existing frameworks in the context of network organisations is examined for the three frameworks COBIT, ITIL and ISO 27005. As integrated care networks (especially in Germany) involve a high degree of autonomy for participants, a network's risk management needs be seen within the context of the risk management in each participating individual organisation. To demonstrate this inter-

[a] https://orcid.org/0000-0003-3814-4088

Otto, L.
IT-Governance in Integrated Care: A Risk-centred Examination in Germany.
DOI: 10.5220/0009376708080817
In *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2020) - Volume 5: HEALTHINF*, pages 808-817
ISBN: 978-989-758-398-8; ISSN: 2184-4305

dependence, a case study is conducted, illustrating the general measures incorporated in risk management strategies. Furthermore, the transfer of results from the exemplary case study to an integrated care setting is explained. Based on the findings, requirements for using IT governance frameworks for risk management in integrated care settings will be derived. Thereby, the paper contributes to the topic of IT governance in integrated care.

2 METHOD

First, consistent criteria were defined against which each framework could be evaluated. They were derived from a narrative literature review covering the topics integrated care and inter-organisation application systems. After all criteria were defined, the frameworks (AXELOS, 2013; ISACA, 2012; ISO, 2011) were evaluated and compared, using qualitative content analysis according to Mayring (2000). Each framework was checked for covering the criteria defined, which represent deductive categories.

A case study was used to further illustrate the process of risk management implementation. An integrated care network with two participants is displayed, showing hospital A as a maximum care provider and hospital B as a smaller rural hospital. In hospital A, risk management steps were conducted, identify, analyse and assess existing risks. For the initial risk identification and analysis, a focus group was conducted to evaluate the BSI catalogue of possible risks (BSI, 2011). Afterwards, the risk assessment was performed by means of a risk matrix. It was chosen as an evaluation tool as it shows very clearly which risks need to be covered and which risks can be neglected. Furthermore, the presentation of risks is differentiated with concurrent manageable complexity. The risk assessment was conducted within the focus groups, i.e. as part of a Delphi study (S. M. Smith et al., 2018). Different roles of the IT management and hospital management participated in these focus groups, e. g. the chief information officer, leading IT project managers, administrators, as well as representatives of the chief execution officer. For hospital B, no risk management was conducted but instead, the procedure of transferring the results to an integrated care setting was described.

Based on the results from literature analysis, qualitative content analysis and case study, recommendations were derived for future research on the topic of IT governance frameworks for risk management in application systems of integrated care networks.

3 FOUNDATIONS

3.1 IT Governance and IT Risk Management

The goal of IT governance is to achieve business objectives supported by IT processes while generating value and minimising risks (Alreemy et al., 2016). Nevertheless, different IT governance frameworks exist. The three most widely used ones in the context of risk management, i.e. COBIT, ITIL and ISO 27005:2011 (Häfner & Felden, 2009), will be analysed in detail in the following. While COBIT presents a universal governance concept (Gaulke, 2014), ITIL focusses on IT service lifecycle management with best practices (Sahibudin et al., 2008). On the other hand, ISO 27005 provides a generic frame for IT risk management and directly addresses information security (Fenz et al., 2014).

Risk management supports the handling of potential risks and includes the steps “definition of risk strategy”, “identification and analysis”, “assessment”, “control” and “monitoring” of risks (Agrawal, 2009). Furthermore, information and their security, including confidentiality, integrity and availability (Zambon et al., 2011), are an important aspect in application systems. Different events in daily business can be a direct risk to these security goals: Fire can harm availability and malware can threaten integrity or confidentiality of data, followed by economic and legal risks. When speaking of IT risks the automated part of an information system, the application system (Ferstl & Sinz, 2013), is addressed. This is also true for inter-organisational application systems which are the automated part of an inter-organisational information system. Main risk categories on this operational perspective are risks which are related to involved persons, processes and systems as well as external risks that consider the surrounding (Bistarelli et al., 2012). The BSI catalogue of possible risks provides a good starting point for identifying possible risks, especially for critical infrastructures. BSI (Bundesamt für Sicherheit in der Informationstechnik) is the German Federal Office for Information Security. The BSI catalogues provide a wide range of possible risks related to information technology and were developed by different experts in that field, which makes them reliable.

3.2 Characteristics of Integrated Care and Related Information Systems

Similar to most of the western health care systems, the health care system in Germany is separated into different sectors, with own budgets and planning structures (Koch, 2005). Connections within and between these sectors are insufficient and lacking (Amelung et al., 2012). A possible solution to overcome the related problems is seen in integrated care as it supports the patient-centred treatment across all sectors. However, integrated care is a widely used term that arose from a tendency towards cooperative care years ago (D. L. Smith & Bryant, 1988). Nevertheless, the focus in this research paper is on integrated care in Germany as its special characteristics are important for the later evaluation of frameworks. Digital tools are important to improve existing health services and integrated care solutions (Seventy-first World Health Assembly, 2018), e.g. information systems to share existing data. Information systems which are commonly used by different organisations are called inter-organisational information system. In inter-organisational information systems, information is processed beyond organisation's borders (Johnston & Vitale, 1988). Data retention is thereby possible in a centralised as well as decentralised manner.

In the following, characteristics of network structures generally and in integrated care settings and of application systems within these structures are introduced.

Organisational Structures. Challenges regarding the organisational structure occur due to the collaboration of different organisations in one network. Such networks have complex, relatively stable temporary relations with contractual commitment between legally independent but economically dependent participants for a specific purpose (Schüppler, 1998). The management has no direct authority, which is why all attendees get involved in leadership (Bogenstahl, 2012). Further challenges arise from the beneficiary involvement of every organisation and the following organisational structure of a network. Networks can range in multiple dimensions between market and hierarchy, competition and cooperation, autonomy and dependency, flexibility and specificity, variability and unity, trust and control, stability and fragility, formality and informality as well as economical action and safeguarding of power (Sydow, 2006). Every network has its own position within the different areas of tension. For integrated care networks in Germany, this position is as follows: In accordance with §140a SGB V special care contracts are possible between health insurance companies and different service providers. Integrated care is therefore market-related and service providers are cooperating even though they can compete when being on the same service level. Every service provider acts autonomously, specifically and variable as the network is built to separate tasks depending on specification. A supervisory authority does not exist in a narrower sense and therefore enormous trust between all participants is necessary. Furthermore, contractual commitment with a health insurance company guarantees a stable cooperation, high formality between service providers and economical action.

Inter-organisational Application Systems. Information processing beyond organisation's borders results in differences between inter-organisational application systems and such within a single organisation. These differences are displayed in table 1. Systems and processes in integrated care are developed differently in comparison to systems and processes in a single institution. Characteristics of inter-organisational application systems in an integrated care setting in Germany are also depicted in table 1, column 3.

Table 1: Characteristics of inter-organisational application systems and typical characteristics in Germany.

	General characteristics	Typical integrated care characteristics in Germany
I	Exchange/corporate usage of data and applications (Raupp, 2002; Schüppler, 1998)	Loosely coupled application systems
II	Risk of heterogeneous security concepts (Raupp, 2002)	Focus on internal security concepts
III	Centralised/decentralised data retention (Raupp, 2002; Schüppler, 1998)	Decentralised data retention
IV	Supervision by multiple participants (Suomi, 1992)	Supervision by respective network partners
V	Interface management necessary (can lead to system/media disruption and data inconsistencies) (Raupp, 2002; Schüppler, 1998)	No standardised interfaces
VI	(unilateral) interdependencies possible (Raupp, 2002)	Low dependencies

Table 2: Characteristics of inter-organisational application systems and typical characteristics in Germany (cont.).

	General characteristics	Typical integrated care characteristics in Germany
VII	Mostly standardised systems (Raupp, 2002)	Low standardisation
VIII	Centralised/decentralised rights of disposal (Raupp, 2002)	Centralised or decentralised
IX	High system security for data and transaction (Raupp, 2002)	System security is highly important
X	Flexible number of participants possible (Raupp, 2002)	Flexible number of participants
XI	Spatial distribution of network participants (Raupp, 2002)	Regional distribution
XII	Level of intensity in collaboration (Schüppler, 1998)	Low intensity

Another aspect, which is specific in inter-organisational application systems are the larger numbers of components (hard- and software) and involved persons (users and administrators) as well as the necessary secure connections between several application systems (Johnston & Vitale, 1988).

3.3 Evaluation of IT Governance Frameworks

To evaluate and compare the three chosen frameworks (COBIT, ITIL and ISO 27005) consistent comparison criteria are necessary. Important for risk management is its integration into business processes (see section *foundations).* Therefore, IT governance frameworks should provide recommendations for conducting the whole IT risk management process. In general, this involves the following steps: *definition of risk strategy* (1), *identification and analysis* (2), *assessment* (3), *control* (4) and *monitoring* (5) of risks (Agrawal, 2009). Furthermore, the goals of information security, i.e. *confidentiality, integrity and availability* (6), need to be considered (Zambon et al., 2011). Focussing on application systems, the components involved, i.e. *hard-* (7) and *software* (8), as well as involved *individuals* (9) need to be addressed within the frameworks (Johnston & Vitale, 1988). Further evaluation criteria are the risk categories *person-* (10), *process-* (11) and *system-related* (12) as well as *external risks* (13) (Bistarelli et al., 2012) and the appropriateness due to the *general characteristics* of the frameworks analysed (14).

Based on the selected criteria the three frameworks can be evaluated and compared regarding the suitability for risk management of (general) intra-organisational application systems, i.e. application systems within a single institution. Afterwards, the transfer of results to inter-organisational application systems in integrated care can be examined, considering the specific characteristics of integrated care.

3.3.1 Intra-Organisational Context

The results of analysing the three models are displayed in Table 2. As can be seen, COBIT is one of the most extensive IT governance frameworks, addressing all criteria and providing detailed explanation for risk management steps and system components (Gaulke, 2014). However, its complexity (14) threatens its applicability (De Haes et al., 2013). ITIL's focus on IT service lifecycle management leads to a lack in considering risk management as a continuous cyclical process (1, 5, 14)

Table 3: Evaluation criteria fulfilled per framework.

Category	COBIT	ITIL	ISO 27005
Covering of risk management process:			
(1) Definition of risk strategy	●	○	●
(2) Identification and analysis	●	●	●
(3) Assessment	●	●	●
(4) Control	●	●	●
(5) Monitoring	●	○	●
(6) Focus on confidentiality, integrity and availability	●	●	●
Consideration of components:			
(7) Hardware	●	●	●
(8) Software	●	●	●
(9) Individuals	●	●	●
Considered risk categories:			
(10) Person-related risks	●	●	●
(11) Process-related risks	●	○	●
(12) System-related risks	●	○	●
(13) External risks	●	○	●
(14) General characteristics	–	–	●

Legend:

Fully complies with criteria	Partly complies with criteria	Does not comply with criteria
●	○	–

(Vilarinho & da Silva, 2011). Furthermore, most of the specific risk categories (11-13) are not in focus. In contrast, ISO 27005 fully complies with the evaluation criteria.

As it can be seen from the comparison, the examined frameworks mostly support the implementation of risk management for application systems within a single organisation. ITIL is the framework which fits least as the definition of risk strategy as well as process-, system-related and external risks are only partly considered.

3.3.2 Inter-Organisational Application Systems in Integrated Care

To check the transfer of results to risk management in integrated care networks, the identified characteristics of inter-organisational application systems (I-XII) will be considered additionally. In addition to the presented evaluation categories (fully, partly, not complying), another one will be used in table 3, for differentiating the results. If a criterion is evaluated with "**○**", the framework addresses the criteria abstractly, but does not specify its prospective usage for inter-organisational networks.

The frameworks still consider the risk management process steps (see table 2), but do not take specific characteristics (see section *foundations*) of integrated care networks into account. For every step, finding a consensus between all network participants is at least partly necessary as they are, despite legally independent, economically dependent from each other. The risk strategy needs to be uniform for the whole network and risks evolving through a connection between participants have to be identified and analysed generally. A consistent assessment, control and monitoring also needs to be based on joint agreements, especially as integrated care networks are characterised by low dependencies (VI) and intensity in collaboration (XII) as well as high regional distribution of participants (XI). Additionally, risk assessment, in particular probability of occurrence, can change. For example, mistrust between the network participants can increase person-related risks, while the loosely coupled application systems (I) with non-standardised interfaces (VII) constitute a high risk of inconsistent data within process-related risks in integrated care networks.

None of the frameworks selected considers the specific characteristics explicitly. COBIT takes requirements of status groups into account (ISACA, 2012), but does not particularly address corporate networks. ITIL was not fully appropriate for intra-organisational application systems already. In ISO 27005, its usage for all kinds of organisations is mentioned (ISO, 2011), although characteristics of corporate networks are also not considered. Implementation guidance supported through examples for risk management steps is still provided, esp. in COBIT and ISO. Nevertheless, required integrated management processes and consultations are not yet included. Furthermore, solutions are lacking for problems of missing management authority and supervision (IV), low dependencies between participants (also regarding security concepts – VI/II), flexible number of participants (X) and additional interface management (V). These problems would require an adjusted risk management which leads to a reduced validation (1-5).

The criteria confidentiality, integrity and availability (6) are addressed for inter-organisational as well as for intra-organisational application systems. Integrated care networks do not require any additional aspects for these criteria. Therefore, the validation remains. Nevertheless, challenges can arise due to the operational assurance of these criteria.

Additionally, securing interoperability on all layers (legal, organisational, semantical, technical) without creating further risks is important (European Commission, 2017). Also, the components of inter-organisational application systems (hard- and software systems) are the same as for intra-organisational ones. However, the number of involved hard- and software systems is increasing in inter-organisational settings, which results in the need for appropriate interfaces (V). This is especially important due to the prevalence of loosely coupled application systems (I) and lack of standardised interfaces and systems (V/VII). Furthermore, the number of involved individuals (users and administrators) increases as well compared with an intra-organisational application system. All additional individuals need to be included in the risk management, especially when engaged on interfaces. Nevertheless, none of the selected frameworks takes one of these requirements into account. On the contrary, individual organisations and their holistic view are especially focussed on (Gaulke, 2014). Despite a high independence of network participants (VI), the network perspective and thus the "gaps" between single institutions are important to be considered. As this is not the case in all of the frameworks analysed, the assessment needs to be reduced (7-9).

The consideration of the four risk categories in the frameworks was already positively evaluated for intra-organisational application systems.

Table 4: Applicability of strategic fit for integrated care.

Category	COBIT	ITIL	ISO 27005
Covering of risk management process:			
(1) Definition of risk strategy	⭘	○	⭘
(2) Identification and analysis	⭘	⭘	⭘
(3) Assessment	⭘	⭘	⭘
(4) Control	⭘	⭘	⭘
(5) Monitoring	⭘	○	⭘
(6) Focus on confidentiality, integrity and availability	●	●	●
Consideration of components:			
(7) Hardware	⭘	⭘	⭘
(8) Software	⭘	⭘	⭘
(9) Individuals	⭘	⭘	⭘
Considered risk categories:			
(10) Person-related risks	⭘	⭘	⭘
(11) Process-related risks	⭘	○	⭘
(12) System-related risks	⭘	○	⭘
(13) External risks	⭘	○	⭘
(14) General characteristics	–	–	●

Legend:

Fully complies with criteria	Partly complies with criteria	Complies with criteria (no focus on networks)	Does not comply with criteria
●	○	⭘	–

Still, required consultations may be harmed due to complex relationships, regional distribution (XI) of partners collaborating with low intensity (XII) and the resulting low dependency (VI). None of these characteristics is included in the frameworks, what leads to a reduction in the assessment of corresponding criteria (10-13) as well.

Irrespective of the aforementioned lack of consideration of company network specifics, the evaluation of the fundamental characteristics (14) does not change. The overall assessment is shown in Table 3.

All in all, none of the three evaluated frameworks fully complies with all criteria. ITIL and COBIT did not or only partly fit for intra-organisational application system's risk management and the rating is further reduced due to special characteristics of integrated care. Also, ISO 27005 can only partly meet the adapted requirements.

2.3.3 Exemplary Demonstration: Risk Management in a Hospital Network

To illustrate the procedure of implementing risk management within a single institution and show how integrated care scenarios change this process, a case study was conducted. As case scenario, a real-world case of two hospitals (hospital A and B) is used, where the risk management process is exemplary executed for hospital A. Both hospitals are in a strategic partnership to organise the patient transfer in an integrated care network (see Figure 1). This means defined processes in integrated care pathways, shared electronic health records as well as shared management processes and responsibilities. Hospital

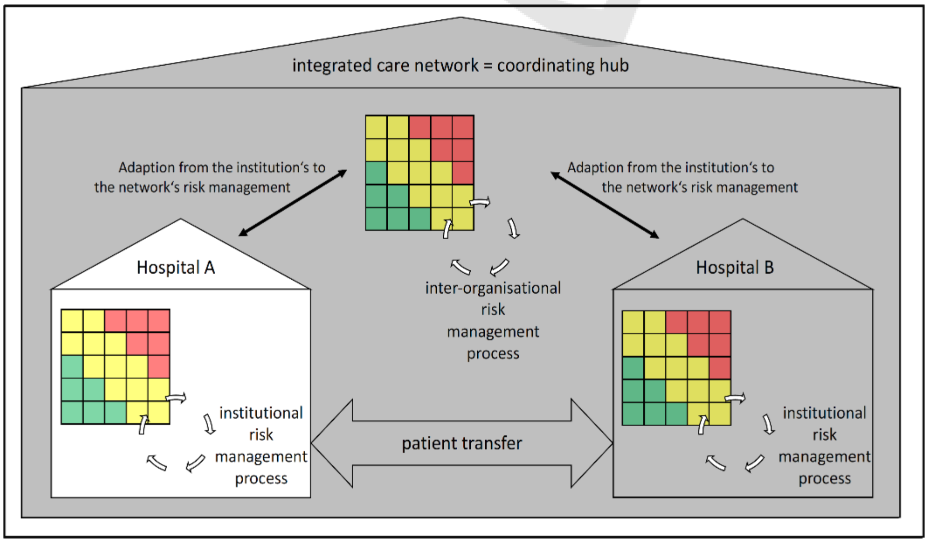
integrated care network = coordinating hub
Adaption from the institution's to the network's risk management
Adaption from the institution's to the network's risk management
inter-organisational risk management process
Hospital A
institutional risk management process
Hospital B
institutional risk management process
patient transfer

Figure 1: Integrated care network scenario.

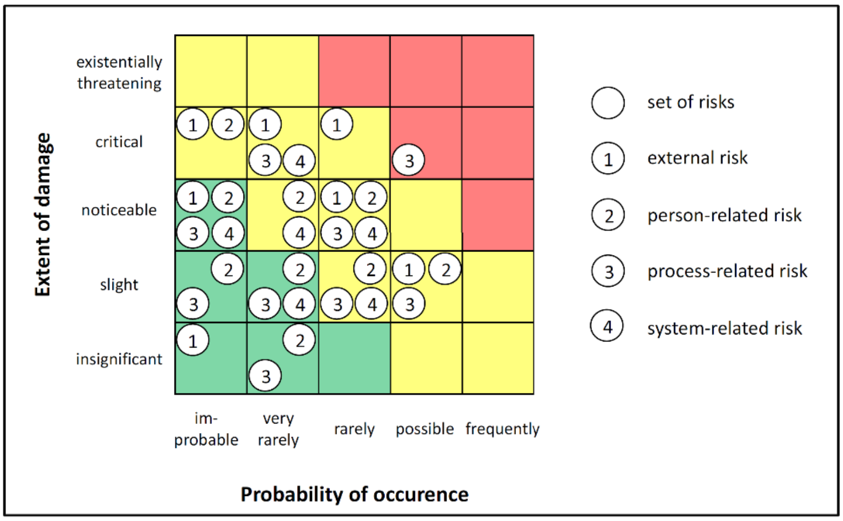

Figure 2: Accumulated risk matrix for assessing risks related to the application system of hospital A.

A is a maximum care provider with over 1,200 beds capacity. Contrary, hospital B is a hospital in a rural area focussing on basic care with 160 beds. The network and the inter-organisational application system are characterised by the typical features described above.

As first step, the risk assessment (identification and evaluation) was done on institutional level for hospital A. As initial set of relevant risks, the 660 risks in the six categories elementary threats, force majeure, organisational deficiencies, human errors, technical failures and intentional acts from BSI (BSI, 2011) were used.

Out of the 660 risks, 182 risks were defined as relevant by the focus group for hospital A. They were categorized into four groups: external (50), person- (75), process- (23), and system-related (34) risks. In the next step, all risks were evaluated with a 5x5 risk matrix regarding their probability of occurrence and the extent of damage they might have. Each risk was assessed by all experts, disagreement was solved through discussion until consensus was reached. Depending on this classification, the risks vary widely in criticality. Some are intolerable (red area), some undesirable (yellow area) and some negligible (green area) (see Figure 2). Depending on the rating, the following risk control is defined (the more a risk is placed in the upper right corner of the matrix, the more is a control action required). Each circle in Figure 2 represents a set of risks. Since the matrix does not reflect the number of risks in each section, table 4 summarizes this information additionally.

Table 5: Summary of criticality per category.

	Person-related risks	Process-related risks	System-related risks	External risks
In-tolerable	-	1	-	-
Un-desirable	24	17	13	46
Negligible	51	5	21	4

The results of the risk assessment show that the biggest proportion of the risks are assessed as undesirable (yellow area – 100 risks). Since the hospital A has a big IT department, only one system-related risk could be identified as intolerable (red area) and must be considered for further countermeasures. The other 81 negligible risks (green area) are existent but do not necessarily need further consideration. However, the reason for this result is not a missing importance of most risks. It is rather the low expected probability of occurrence that lead to an undesirable or negligible risk assessment. The focus group assessed the probability relatively low for most of the risks as the information system is already highly mature. However, some risks to be controlled further remain.

Conclusively, all four risk categories (person-, process-, system-related and external) are relevant for risk control and monitoring in hospital A. The usage of frameworks in this internal context would be helpful and can be realised e. g. with ISO 27005 which serves as a good framework for intra-organisational risk management as shown above (see Table 2). Furthermore, the BSI catalogues and their approaches are compliant with ISO 27001 (to which

ISO 27005 belongs) what supports the applicability of this framework for hospital A even more.

Outlining the transition to a common risk management within the integrated care setting described, the risk assessment of hospital B needs to be carried out as well, covering the individual application systems' risks of this second hospital. However, to fully cover the whole network within the risk management strategy, the network itself and its application system need to be considered. This is due to the fact that inter-organisational risk management is more than the sum of risk managements within each individual institution.

Some implications can be inferred from the maximum care provider's results. Following the results of framework evaluation, the assessment of risks, especially probability of occurrence, is likely to increase when considering the perspective of integrated care networks. The focus group workshop already came to the same conclusion by acknowledging that a modified assessment for some risks would be required within a network scenario. This applies to all risk categories and can lead to a higher criticality and more necessary control. Furthermore, an overall guideline or framework is needed for coordination in an integrated care network, especially as participants in integrated care networks act highly independent from each other and no common supervision exists.

Due to the lacking applicability of the frameworks included, the need for a new domain-specific framework could be identified. Summarising the identified deficits, the following requirements need to be considered for such a framework:

Req. 1 - **Cross-company Management Processes:** An explicit reference to the increased need for consultation in most risk management steps is necessary.

Req. 2 – **Assignment of Responsibility:** Instructions for defining responsibilities regarding a holistic control of all shared processes needs to be included in such a framework.

Req. 3 – **Rules in the Event of Changing Participants:** Responsibilities need to be ensured, also in case of changing participants. This can be ensured by means of a sufficient number of defined deputies or the implementation of process steps that come into effect when responsible persons leave the network.

Req. 4 – **Interoperability:** An explicit reference to the different levels of interoperability and the need to ensure it is needed.

Req. 5 – **Holistic Management Processes:** An explicit reference to the necessity of a holistic interface management (possibly by defining responsible persons) is necessary.

4 DISCUSSION & CONCLUSION

The three most widely used IT governance frameworks considering risk management (COBIT, ITIL and ISO 27005) were evaluated. Focus of evaluation was their use for application systems in integrated care networks. The results show that the selected IT governance frameworks are not applicable for risk management in integrated care networks, especially in Germany. Furthermore, a stronger analysis of institutionalisation for integrated care networks is necessary to enable a more powerful legitimation of the network itself and to subordinate the independence of participants under the processes of the network. Additionally, coordination of individual services or risk management could be a joint task. The organisation-centred approach, which is currently applied, possibly needs a shift to a network perspective, especially in Germany.

To gain further insights on understanding the coordination process for management, additional research is needed to transfer intra-organisational results to an integrated care network. However, the case example is limited to German and integrated care characteristics. Additional case studies need to be conducted to understand the transferability of results to other countries and to other kinds of networks. Nevertheless, the literature study has shown that the problems regarding the framework usage for networks are fundamental.

All in all, it has been shown that an application of the frameworks considered is always accompanied by a large number of restrictions, especially since an explicit consideration of networks as an organisational form is not intended. Missing aspects in this area are, in particular, consideration of additional consultations, lack of authority and control (management), incorporation of a flexible number of participants as well as necessary interoperability and interface management, resulting from the network characteristics itself. Nevertheless, risk management steps, a focus on confidentiality, integrity and availability as well as operational risks (person-, process-, system-related and external) are considered in all of the frameworks. On the one hand, it can be said that the evaluated frameworks cannot support the risk management of application systems in integrated care networks. However, on the other hand, a transfer to a network view would be worthwhile due to the high autonomy of participants in these networks, for which e. g. ISO 27005 is an adequate guideline.

Further research needs to focus on two aspects: Firstly, the scenario presented should be completed by investigating the risk management of the second hospital and the network itself as well as matching this with the presented results. Secondly, the findings of this paper could improve the design process to develop a risk management framework focussing on (integrated care) networks. Therefore, strengths of established frameworks need to be combined and extended by the requirements provided. A combination of ISO's clear structure supplemented by detailed explanations from COBIT and ITIL's best practices could be a good basis.

As a fully integrated IT enables integrated care concepts, a helpful framework for inter-organisational care networks can lead to improved care supply, not only in Germany.

ACKNOWLEDGEMENTS

I thank Hannes Schlieter for his feedback on the topic and Jeannette Stark for helping me improving the paper.

REFERENCES

Agrawal, R. C. (2009). *Risk Management*. ABD Publishers.

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, *36*(6), 907–916.

Amelung, V., Hildebrandt, H., & Wolf, S. (2012). Integrated care in Germany—A stony but necessary road! *International Journal of Integrated Care*, *12*(1), 1–5.

AXELOS. (2013). *ITIL Service Design*. The Stationery Office, London.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, *81*(12), 2118–2133. https://doi.org/10.1016/j.jss.2008.03.059

Bistarelli, S., Fioravanti, F., Peretti, P., & Santini, F. (2012). Evaluation of complex security scenatios using defence trees and economic indexes. *Journal of Experimental & Theroretical Artificial Intelligence*, *24*(2), 161–192.

Bogenstahl, C. (2012). *Management von Netzwerken: Eine Analyse der Gestaltung interorganisationaler Leistungsaustauschbeziehungen*. Gabler.

BSI. (2011). *IT-Grundschutz: Gefährdungskataloge*. Bundesamt Für Sicherheit in Der Informationstechnik. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00.html

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, *27*(1), 307–324. https://doi.org/10.2308/isys-50422

European Commission. (2017). *ANNEX to the European Interoperability Framework—Implementation Strategy COM (2017) 134 final*.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410–430.

Ferstl, O. K., & Sinz, E. J. (2013). *Grundlagen der Wirtschaftsinformatik*. Oldenbourg Verlag.

Gaulke, M. (2014). *Praxiswissen COBIT - Grundlagen und praktische Anwendung in der Unternehmens-IT*. dpunkt. Verlag.

Gröne, O., Garcia-Barbero, M., & WHO European Office for Integrated Health Care Services. (2001). Integrated care: A position paper of the WHO European Office for Integrated Health Care Services. *International Journal of Integrated Care*, *1*, e21–e21. PubMed.

Häfner, C., & Felden, C. (2009). *Building a framework for an efficient IT governance* (Vol. 231). Techn. Univ. Berakademie.

Henriksen, E., Burkow, T., Johnsen, E., & Vognild, L. (2013). Privacy and information security risks in a technology platform for home-based chronic desease rehabilitation and education. *BMC Medical Informatics and Decision Making*, *13*(85), 1–13.

ISACA. (2012). *COBIT 5—A Business Framework for the Governance and Management of Enterprise IT*.

ISO. (2011). *International Standard ISO/IEC 27005:2011(E)—Information technology; Security techniques; Information security risk management.*

Johnston, R. H., & Vitale, M. R. (1988). Creating Competitive Advantage With Interorganizational Information Systems. *MIS Quarterly*, *12*(2), 153–165.

Koch, O. (2005). Unterstützung von einrichtungsübergreifenden Kommunikationsprozessen in der integrierten Gesundheitsversorgung. In *Telemedizinführer Deutschland* (pp. 106–109).

Mayring, P. (2000). Qualitative Content Analysis. *Forum: Qualitative Social Research*, *2*(1), 1–10.

Raupp, M. (2002). *Informationsmanagement und strategische Unternehmensführung*. Lang.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations*. 749–753.

Schüppler, D. (1998). *Informationsmodelle für überbetriebliche Prozesse: Ein Ansatz zur Gestaltung von Interorganisationssystemen* (Vol. 2357). Lang.

Seventy-first World Health Assembly. (2018). *Agenda item 12.4—Digital health* (WHA71.7; pp. 1–4). World Health Organization. http://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf

Silva, M. M., Gusmão, A. P. H. de, Poleto, T., Silva, L. C. e, & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, *34*(6), 733–740. https://doi.org/10.1016/j.ijinfomgt.2014.07.005

Smith, D. L., & Bryant, J. H. (1988). Building the Infrastructure for Primary Health Care: An Overview of Vertical and Integrated Approaches. *Social Science & Medicine*, *26*, 909–917.

Smith, S. M., Wallace, E., Salisbury, C., Sasseville, M., Bayliss, E., & Fortin, M. (2018). A Core Outcome Set for Multimorbidity Research (COSmm). *Annals of Family Medicine*, *16*(2), 132–138. Embase. https://doi.org/10.1370/afm.2178

Suomi, R. (1992). On the Concept of Inter-organizational Information Systems. *Journal of Strategic Information Systems*, *2*, 93–100.

Sydow, J. (2006). Netzwerkberatung—Aufgaben, Ansätze, Instrumente. In J. Sydow & S. Manning (Eds.), *Netzwerke beraten*. Gabler.

Vilarinho, S., & da Silva, M. M. (2011). Risk Management Model in ITIL. In M. M. Cruz-Cunha, J. Varajão, P. Powell, & R. Martinho (Eds.), *ENTERprise Information Systems* (pp. 306–314). Springer Berlin Heidelberg.

Zambon, E., Etalle, S., Wieringa, R. J., & Hartel, P. (2011). Model-based qualitative risk assessment for availability of IT infrastructures. *Software Systems Modeling*, *10*(4), 553–580.