ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 3, pp. 271-285
DOI:10.33168/JSMS.2022.0314

Deriving Suitable Characterization Model for Information Governance from Case Study Analysis Perspective

Evan Asfoura

Arab open university, Riyadh, Saudi Arabia

e.asfoura@arabou.edu.sa

Abstract. The two fields of Information governance and information security are becoming more and more important for the corporates, due to the huge amount of data which is collected day by day through relaying on a variety of information systems for the aim of supporting the business processes. This paper describes a new model for characterization of information governance aspects through reviewing and crossing the related works. The model presented help the enterprises to analyze here cases in terms of applying the information governance aspects for improvement. For achieving the proposed model and ensure its validity, exploratory methods with empirical case study for accompany works in Mobile Telecommunications industries were used. Results are be presented as information governance life-cycle model with parallel and sequential stages, to successfully lead the enterprises to apply in practice their information governance, to manage and use data to obtain information.

Keywords: information governance, information security, information quality, information governance life cycle.

1. Introduction

"Governance" as a term is well-known and used in business, referring to monitoring and controlling the role and behavior of the management. It has focused on the role of boards of directors in representing and protecting the interests of shareholders. A critical role for governance is to monitor and to control the behavior of managers, who are hired for managing and controlling the day-to-day activities of running the organization (Fama & Jensen 1983). Generally, "corporate governance", is a set of laws, policies, customs, and processes that affect the managerial activities, including the decision making, planning, coordinating, and controlling, in addition to considering the relationships among the stockholders and the goals of the organization that the governance targeted (OECD 1999).

Reaching the goals of governance on a corporate level depends strongly on governing the use of the required resources, with a focus on the data and the information resources which are important inputs for supporting successful managerial activities. Therefore, recently, many researches focused on studying and exploring the aspects of information governance especially after growing the term, "Big Data", and "Business Intelligence" (Mikalef et al 2020; Prescott 2016; Coyne et al 2018).

On the other hand, successful Information governance relies on the consideration of the information security measures and the frameworks that are applied for reducing the risk which is related to damaging the quality of information, which will negatively impact the efficiency and effectiveness of information as management resource (Lomas 2010, Khatri & Brown 2010). Accordingly, it is assumed that bad resources (information) with good management will lead to insignificant outcomes. Similarly, good information without suitable management will lead also to insignificant outcomes; in other words, information security cannot be separated from information governance.

Therefore, in the next section, we will separately explore the approaches and concepts related to "information governance", then in line to each other. Moreover, information to extract significant characteristics of information governance and information security will be summarized as a basis for discussing and analyzing case study, related to improving the information governance and security.

2. Literature Review

Many researchers provide various approaches showing how the enterprises can manage their IT infrastructure to increase the security and the value of generated information, which will improve the quality of the managerial activity, including the decision making, planning, coordinating, and controlling. This section will review research articles that handle with information governance and information security. The review will focus on discussing the definitions, concepts, frameworks as well as

the limitations for each article, to derive mature characteristics that serve well-defined Information governance (IG) and information security (IS) as a basis for analyzing case studies in this context.

The study of Merkus and others reviewed the literature to explore widely and deeply set of definitions about terms such as data, information, data governance and information governance. Their approach was focusing on collecting and analyzing the elements of definitions about data information as underlaying for data governance and information governance within and cross the organization. Additionally, the study focused on investigating the similarities and differences between data governance and information governance (Merkus et al 2019, see also Liaw et al 2014, Morabito 2015, de Abreu Faria 2013).

The main finding of this article is to explain and to formulate the definition and description concepts of data, information, data governance and information governance, in information system domain as well as taking into accounts what the authors suggested about using data governance and information governance as similar terms based on their review and analysis.

The provided approach in this study is based on reviewing and analyzing existing research and previously accepted methods and concepts without finding out new methods related to how to improve the concepts and methods for applying information governance within and cross the organization.

The authors define information governance as: "… establishing management of information in an organization, assuring quality and access during its life-cycle to be accountable for information assets". Accordingly, this definition focused on managing information quality and information security.

Additionally, the authors defined the information security as an important aspect for reaching the information governance so as to manage and control the data and information access.

Differently, Nicho and Muamaar, developed a taxonomic model which comprehensively presented the challenges faced during the implementation and integration of IT governance (ITG) fireworks in the organization. This research has also compared the challenges faced with the implementation and integration of governance as well as security standards and frameworks in UAE with the other organizations from the extant literature. Not only this, but the research investigates the challenges for applying ITG in integrated environments, which led to adapting a framework, including new challenges that were not discovered earlier (Nicho & Muamaar 2016).

The content of this work focused only on exploring and adapting the previous models with some consideration of the different environmental and organizational contexts.

The authors in this work did not give a clear definition of information governance and security. However, they focused on comparing and reviewing the IT governance frameworks to figure out the challenges faced during applying IT governance and referred to information security issues as main part of these challenges.

Another integrated framework for information governance on country level has been emerged from Mullon and Ngoepe. The authors focused in their framework on the required instruments (policy and legislation), key success factors, principles and a proposed list of elements or disciplines, which should be managed in a successfully integrated manner (Mullon & Ngoepe 2019).

The outcomes of this research can be summarized as establishing some domains at different levels of maturity, where different stakeholder groups are responsible for each domain. These domains are records' management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, information risk, information security and e-discovery. This work focused on explaining the negative effects of unmodeled and regulated information governance at country level on the governance at organizational level. The presented framework focuses on how the information governance can successfully be implemented with consideration of possible difficulties, while the previous framework by Nicho & Muamaar (see also Silic & Back 2013). summarizes the challenges faced during the IG implementation.

The authors of this work defined information governance as a set of management aspects including the information security and records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance as well as information risk.

Daneshmandnia in his research, discussed the impact of the organizational culture on the effectiveness of information governance. The provided approach in this research relay on (Cameron and Quinn 2011) competing value framework, including four types of organizational structure profiles which have been quantitatively and qualitatively evaluated **(**Daneshmandnia 2019)**.**

This research reveals the possible positive impacts of the organizational structure on information governance effectiveness, as well as the emergence of that competition/result-oriented and control characteristics of organizational culture as they were perceived by IG professionals to produce more accurate information. This research was conducted on specific type of institutions and the result cannot be generalized on all the other institutions.

Information governance has been defined in this work as set of activities (processes), including information security, the function of an IG council, the presence of a Record Information Management department, the role of a compliance officer and information stewards and the use of an automated system or software to identify and maintain information life-cycle management.

Rasouli and others listed through their case study-based research a comprehensive number of information governance issues related to dynamic networked business processes, using structured steps for the identification of these issues, which can be applied on many industries, to explore domain-specific information governance issues. The identification of such issues will be helpful for business governors to have a better view on causing risks by information exchanging and/or sharing through dynamic networked interactions among independent and globally distributed parties (Rasouli, et al 2016) .

The main limitation of this research is that being conducted within case study, which is not an extremely dynamic business network, therefore, more research should be done about the more dynamic business networks, in order to improve the confidence of the findings. In addition, more research can be conducted for developing organizational, architectural, or computational solutions that address the identified IG issues in the context of dynamic business networks.

The information governance in business networks has been defined in context of this article as a holistic approach to different mechanisms that support high quality and secure information exchange.

In terms of security and Governance, Al-Fatlawi with others have published an article about applying IT governance with using COBITb 5 framework and its processes for reducing data processing risks and improving the security of accounting information system. The study has been conducted within a bank as a case study and its outcomes refer to the fact that the applying IT governance under the COBIT Internal Control Framework, improves the efficiency of the internal control system in electronic accounting systems (Al-Fatlawi et al 2021).

The contribution of this research was limited only on applying widely IT governance framework on specific organization to summarize the strengths and weaknesses related to risk and information security by managing accounting information system.

This work did not give clear definition for information governance. However, in the context of this work, it was referred to ITG as mechanisms for ensuring IT security and managing information system to reduce the risk and to increase the information quality which helps the organization to achieve its objectives.

One of the important studies which focused clearly on the information security and information governance is the study of (Lomas, 2010) which explained that the application of international security standard (ISO 27001) framework, simultaneously with the records management standard (ISO 15489), will lead to holistic information governance.

This study defines the information governance as a planned information management and security programs to ensure that information is controlled and “appropriately” available.

Continuously, With the consideration of security aspects, some researchers like Lemieux, Rowell, Seidel and Woo provided a framework for centralized–decentralized information governance. This framework includes three distinct dimensions: custody, ownership and the right to access data. It has been applied on two illustrative blockchain case studies, namely a pilot Brazilian land transfer recording solution and a Canadian health data consent sharing project.

This research provides mechanisms for strategic information governance decentralized business environment where the organizations are part of decentralized ecosystems with new business opportunities and challenges. (Lemieux et al, 2020).

The authors presented an analytic framework for strategic information governance challenges faced during the transformation to new decentralized word, through case study analysis, for the transitions and their impact on strategic information governance along three trajectories: custody, ownership and right to access records and data.

Related to the previous study, (Franks 2020) explored many articles about blockchain technology in distributed ledger technology for record management and information governance, in addition to formulated cybersecurity base framework for increasing the efficiency, by securing and managing information. Other research in security field can be reviewed through (Jiyoung & Suna, 2022. Sang, 2021. Wong et al 2020; Singh, 2020: Masilela & Nel 2021) and many other articles.

After this literature review, we can conclude that there are huge numbers of research articles that discussed innovative definitions, approaches and frameworks related to information security and governance from different perspectives. Despite the high consideration of this field in research, there are still many open areas for further exploration and analysis of the issue, as well as many opportunities related to identifying the responsibilities of executives and their role for improving the information governance and information security across the organization.

3. Methodology

This research has used exploratory methods to investigate definitions, aspects and frameworks of information governance handled in literature, joined with the use of practical case study for evaluating the usefulness of the derived model with its characteristics.

3.1. Deriving the characterization model for information governance cases

Based on the literature reviewed in section 2, we will take the opportunity to cross the reviewed articles to derive the following definition of information governance, so as to use it to analyze the next case studies. In a nutshell, “Information governance

means managing process of information systems and information security to ensure the quality of information as input, for planning, decision making and risk management across the organizational levels, to accomplish the organization goals, including the increase of the benefits and the reduction of the costs (see fig. 1 which has been validated in table 1).

This definition has been formulated based on the consideration of frequently repeated key words from the authors who published their research about information governance and some of them, presented in our literature review (see table 1).

Table 1: cross referencing the main keywords used by selected group of works related to information governance

	Merkus et al 2019), Liaw et al 2014, Morabito 2015, de Abreu Faria, 2013	Nicho & Muamaar, 2016; Silic, & Back, 2013.	Mullon &Ngoepe,2019	Daneshmandnia 2019	Rasouli, et al, 2016	Al-Fatlawi et al 2021
Managing process	√			√		√
Information system		√		√		√
Information security	v	√	√	√	√	√
Information quality	√	√	√	√	√	
Decision making			√			
Planning			√			
Risk management			√			
Organizationn's gools/objectives						√

Regarding information security, all the reviewed research articles confirmed that information security means managing the use of tools, polices, programs and strategies for the protection of the data and information against the unauthorized access and its use to ensure the data and information quality.

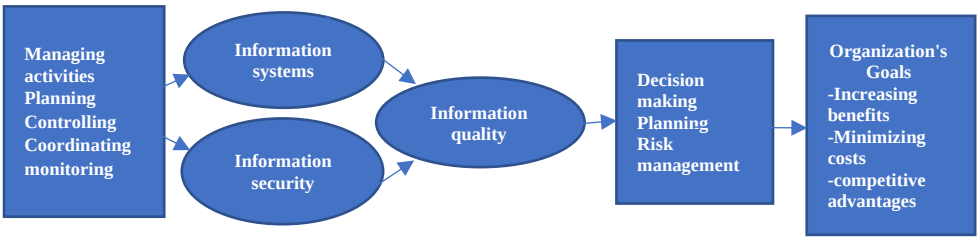

Fig. 1: The concept of information governance life-cycle including information security

The previous figure shows that the starting point of information governance with the management activities (processes) carried out from the executives like planning, coordinating and controlling the information security (see Vacca, 2013; Whitman & Mattord, 2013; Soomroet al 2016). and information systems(see Khani, 2011; Bharati, and Berg, 2003; Xu and Quaddus, 2013) to ensure the information quality (see Miller 1996; Gorla et al,2010; Stvilia et al 2007) to be used for the support of the managers and employees' activities along the organization, which will increase the benefits and will reduce the cost.

For evaluating the valid previous approach, the next section will use it to present a case study analysis for one of the companies that wok in Mobile Telecommunications industry to show the strengths, weaknesses and the possibilities for improvement related to applying the information governance successfully (the name of company will be hidden because of privacy issues.

3.2. Case study about ZN (Mobile Telecommunications Company)

ZN is a Kuwaiti mobile telecommunications company founded in 1983 in Kuwait as MTC (Mobile Telecommunications Company), and later rebranded as Zain in 2007. Zain has a commercial presence in seven countries across the Middle East with 49.5 million active customers, more than 7000 employees and about 1.66 billion generated revenues.

The management decided to integrate technology for more supporting to the managerial activities (processes), aimed at increasing the efficiency and productivity, especially because of the growing number of subscribers and the services that are provided by this company. Based on this decision, many information systems have been installed to support different departments, through creating the wide area network (WAN), which allows the sharing of information and applications between the branches over the countries where it operates. The used information systems in ZN now can be summarized as the following:

- CRM Coheris: This information system is able to collect and store huge amounts of data, collected through recording data about the subscribers, their suggestions and complaints and the line status, in addition to saving data about

the bills with their due date. For the benefits and the infractions, this system allows the employee to retrieve the subscribers who are recorded via using their telephone number. The retrieved records include details about the personal information, bills, benefits, contract, recorded calls, the sponsor, the archive of operations, in addition to many another details.

- Also, the company uses purchasing information system, which integrates, supports and automates all the activities related to the purchasing process for all the department in the company to increase the flexibility, via ordering and without contacting the high management, especially for cases that do not require many approvals and/or should be completed faster.
- Semak system has been introduced as an information system for the recording of the daily financial transactions. This system was adopted to create some schooled standard reports to the head of accounting and finance department, to give an overview about the performance of financial issues.
- Additionally, there are some web applications that have been activated to support activities related to different departments such as "telecopti", which is used for monitoring the attendance of the employees within the various branches, and this application provides reports about the attendance and about the work performance.
- ZN uses also social media like (Facebook, twitter and Instagram) for marketing objectives. The marketing team accomplished many effective campaigns, including attractive offers, especially during occasions.

The IT department in this company has been formulated as decentralized, including many IT groups, who are specialized to support specific department in ZN Company. These groups are directed from the head of IT department.

Recommendations for improvement

The starting point for the improvement is reorganizing that the IT department in this company has CIO who can stay in contact with the strategic management and can activate a direct line between the organizational strategic goals as well as building suitable IT infrastructure. This executive IT manager will be able to participate in decision making, planning and allocating the required resources for improvement.

Furthermore, the company needs to replace new integrated information system (ERP system) instead of the legacy systems, used to separately support the different business processes across the company, to improve the quality of data. This integrated system will help to increase the efficiency of business process across the departments on one integrated database which allows the managers and the employees from different levels in the company to retrieve high quality reports. This recommended transformation needs to be managed successfully through preparing the users (Managers and employees) in ZN to be able to use such complicated systems,

reengineering the business processes based on the workflow of this standard system and building the suitable IT infrastructure, where this software solution will work.

Additionally, ZN has big amounts of data because of the huge number of customers (subscribers) and the daily recorded transactions. Therefore, the company can take great competitive advantage through creating data warehouse, which includes data collected from different resources (internal and external), especially from the used CRM software which was mentioned in section 3. This data warehouse can be used as a base for applying business intelligence tools (like OLAP and datamining) for understanding the costumer problems, preferences and the costumer behavior, to improve the provided products. The access to this data warehouse should be managed successfully to allow the managers and the employees from all the organizational levels across the company to have access. That will increase the flexibility of work and will reduce the time for reacting to the costumers. Also, applying business analytics on the gathered data in the proposed data warehouse, will reduce the risk related to the reduction of the market share and will support well informed decisions about the marketing mix.

The previous analysis will be explained and summarized in fig2. with consideration to Figure1 .

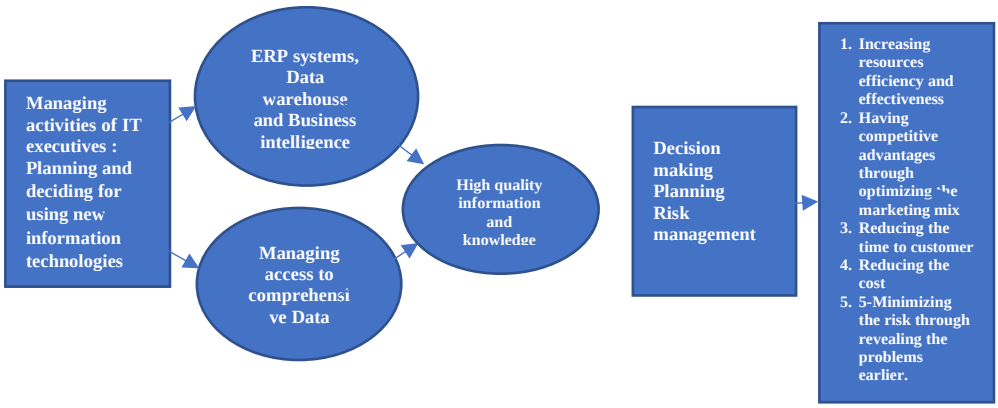

Fig. 2: The concept of information governance life-cycle by ZN company

Managing the information security as important phase for applying the information governance:

Information security is an important aspect of information management as shown in figure 1, in section 2 and all the studies in this section confirmed that no complete information governance can exist without protecting the information, so as to ensure the quality aspects of information.

Despite the used security measures by ZN company to protect its data and information system against the unauthorized access and use, it still needs to apply international security framework like (ISO 27001) which was presented by Lamas in

the literature review section to adjust comprehensively security issues. Thus, as I experienced during my career time with this company, there are sets of security polices, activities and technologies, using the different information systems and applications described in section 4, such as antiviruses, firewalls, intrusions detection system, access polices, awareness programs and disaster response teams, however, there is no clear framework to control the lack and weakness comprehensively. Therefore, applying (ISO 27001) standards will ensure the security from different aspects, namely:

- Policy, objectives and activities that reflect business objectives;
- Asset classification and control;
- Physical and environmental security;
- HR security;
- Approach and framework to implement, maintain, monitor, and improve;
- Systems consistent with the organizational culture;
- Incident reporting systems;
- Systems' development and maintenance protocols;
- Business continuity management;
- Legal compliance frameworks;
- Visible support and commitment within all the levels of management, including the provision of appropriate funding;
- Provision of appropriate awareness, training and education to all the managers, employees and other parties to achieve awareness.

ZN company can assign the responsibility to an auditing team, organized by the IT department, with some employees from other departments to check the availability and the maturity of the previous standards related to information assets, across the organization to be certified. That will reveal the weaknesses and the strengths in terms of information security (represented in three dimensions: confidentiality, integrity and availability) and information assets quality assurance.

Accordingly, the response team will be able to plan for upgrading the security dimensions for the information assets, across the company, which will improve the information quality as a critical aspect for achieving the information governance.

Fore example, applying the previous standards of (ISO 27001) on the CRM system as the core system used by ZN company; will ensure the following:

- The data and information provided from this system are accessible and useable upon demand by an authorized entity;
- The completeness and accuracy of information provided from this system;
- The Authenticity requirements are built into the system development.

Ensuring the compliance of the previous properties will help for a successful management of this information system and security aspects, which consequently will improve the quality and value of information being produced by the system, and will increase the performance of the decisions and managerial activities, which relay on this information for accomplishing the organizational goals.

4. Results and discussion

This paper presents new theoretical model to be used by the companies to characterize and analyze the aspects of applying the information governance to identify their weaknesses and strengths, for continues improvement.

The presented model in this work has been derived through crossing several main references that handled the issues related to information governance and information security as main aspects. The model includes several different phases called as information governance life cycle because they should be considered sequentially for sustainable information governance of the company that was applying the model.

Additionally, this paper provides a case study analysis on base of the given model to show and evaluate the practicability and usefulness of this model for characterizing the current situation of information governance to be improved in future.

In consequence, this work adds theoretical and practical values through providing new theoretical model for analyzing the cases of applying information governance successfully in practice. That will help the companies to increase the value from using its information systems and the collected information as important resource for decision making and as well as the other managerial activities.

Then this paper used new derived model which represent the information governance life cycle instead exist frameworks and models for use cases analysis. This model nobles the company to characterize their current situation regarding the governance of their information resources and to plan for improving in future in continuous process.

5. Conclusion

In this work, we reviewed different articles that discussed the topics of information governance aspects. The aim was to find out through crossing the reviewed works a new model for information governance, including the key aspects to be formulated and considered, as a basis for analyzing case studies, by the companies in general, with a focus on for improvement.

Acknowledgement

The researchers extend their thanks and gratitude to he Arab Open University for the support and funding this research.

References

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. Webology, 18 (Special Issue on Information Retrieval and Web Search), 294-310.

Bharati, P. & Berg, D. (2003). Managing information systems for service quality: A study from the other side. *Information Technology & People*, 16(2), 183-202.

Chun, Y. H., & Cho, M. K. (2022). An empirical study of intelligent security analysis methods utilizing big data. *Webology*, 19(1), 4672-4681.

Cameron, K. S., & Quinn, R. E. (2011). Diagnosing and changing organizational culture: Based on the competing values framework. John Wiley & Sons.

Coyne, E. M., Coyne, J. G., & Walker, K. B. (2018). Big data information governance by accountants. *International Journal of Accounting & Information Management.*

Daneshmandnia, A. (2019). The influence of organizational culture on information governance effectiveness. *Records Management Journal.*

De Abreu Faria, F., Maçada, A. C. G., & Kumar, K. (2013, January). Information governance in the banking industry. In *2013 46th hawaii international conference on system sciences*, 4436-4445). IEEE.

Fama, E. F. & Jensen, M. C. (1983). Separation of ownership and control. Journal of Law and Economics, 26, 301–325.

Franks, P. C. (2020). Implications of blockchain distributed ledger technology for records management and information governance programs. *Records Management Journal.*

Gorla, N., Somers, T. M., & Wong, B. (2010). Organizational impact of system quality, information quality, and service quality. *The Journal of Strategic Information Systems*, 19(3), 207-228.

Jiyoung, J. & Suna, k,, (2022). An innovative career management platform empowered by AI, big data, and blockchain technologies: Focusing on female engineers. *Journal of Logistics, Informatics and Service Science*, 9(1), 214-230.

Khani, N., Nor, K. M., Hakimpoor, H., Bahrami, M., & Salavati, S. (2011). IS/IT capability and strategic information system planning (SISP) success. *International Journal of Managing Information Technology (IJMIT)*, 3.

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, 53(1), 148-152.

Lemieux, V. L., Rowell, C., Seidel, M. D. L., & Woo, C. C. (2020). Caught in the middle? Strategic information governance disruptions in the era of blockchain and distributed trust. *Records Management Journal*.

Liaw, S. T., Pearce, C., Liyanage, H., Cheah-Liaw, G. S., & De Lusignan, S. (2014). An integrated organisation-wide data quality management and information governance framework: theoretical underpinnings. *Journal of Innovation in Health Informatics*, 21(4), 199-206.

Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journal*.

Masilela, L., & Nel, D. (2021). The role of data and information security governance in protecting public sector data and information assets in national government in South Africa. *Africa's Public Service Delivery and Performance Review*, 9(1), 385.

Merkus, J., Helms, R., & Kusters, R. J. (2019, May). Data governance and information governance: Set of definitions in relation to data and information as part of DIKW. In ICEIS, (2), 143-154).

Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2020). The role of information governance in big data analytics driven innovation. *Information & Management*, 57(7), 103361.

Miller, H. (1996). The multiple dimensions of information quality. *Information Systems Management*, 13(2), 79-82.

Morabito, V. (2015). Big data governance. *Big data and analytics*, 83-104.

Mullon, P. A., & Ngoepe, M. (2019). An integrated framework to elevate information governance to a national level in South Africa. *Records Management Journal*.

Nicho, M., & Muamaar, S. (2016). Towards a taxonomy of challenges in an integrated IT governance framework implementation. *Journal of International Technology and Information Management*, 25(2), 2.

OECD (Organization for Economic Cooperation and Development). (1999). OECD principles of corporate governance, SG/CG (99).

Prescott, M. E. (2016). Big data: Innovation and competitive advantage in an information media analytics company. Journal of Innovation Management, 4(1), 92-113.

Rasouli, M. R., Eshuis, R., Grefen, P. W., Trienekens, J. J., & Kusters, R. J. (2016). Information governance in dynamic networked business process management. *International Journal of Cooperative Information Systems*, 25(04), 1740004.

Sang, Y. L. (2021). Blockchain technology-based medical information system for personalized medical services. *Journal of System and Management Science*, 11(2), 121-133.

Singh, D. (2020). Towards data privacy and security framework in big data governance. *International Journal of Software Engineering and Computer Systems*, 6(1), 41-51.

Silic, M., & Back, A. (2013). Factors impacting information governance in the mobile device dual-use context. *Records Management Journal.*

Stvilia, B., Gasser, L., Twidale, M. B., & Smith, L. C. (2007). A framework for information quality assessment. *Journal of the American society for information science and technology*, 58(12), 1720-1733.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.

Wong, C. K., Maynard, S. B., Ahmad, A., & Naseer, H. (2020). Information security governance: a process model and pilot case study.

Vacca, J. R. (Ed.). (2013). Managing information security. *Elsevier.*

Whitman, M. E., & Mattord, H. J. (2013). Management of information security. *Cengage Learning.*

Xu, J., & Quaddus, M. (2013). Managing information systems: Ten essential topics. *Springer Science & Business Media.*