|  |
| --- |
| Information Security & IT Governance Framework |
| *Literature Review* |
| **Submitted to****Submitted by****Course Code****Dated** |



Table of Contents

[**Introduction 2**](#_Toc52206101)

[**Critical Literature Review 3**](#_Toc52206102)

[**Conclusion 7**](#_Toc52206103)

[**References 8**](#_Toc52206104)

# Introduction

With explosion of the internet based applications, the ways of conducting businesses has been changed dramatically. In today’s digital world, organizations are diverging into digitalization by moving from manual to electronic media as means of communication, storage and dissemination of data to stakeholders (Schinagl & Shahim, 2020). High dependency on IT has exposed the organizations towards threat of information security. IT has long been seen as the cornerstone for gaining competitive advantage in today’s competitive world. Although the new technologies are making things swift and easier for organizations, yet these are also making companies vulnerable to unexpected cyber-attacks and information security breach (Fazlida & Said, 2015).

Information security landscape has been reshaped as it has taken place as a key agenda in the boardrooms of big companies. Organizations have to compete in forever expanding dynamic environments while dealing with disruptive world through embracing the digital technology. As the organizations are adopting digital business strategies including internet of things, block-chain, artificial intelligence and cloud computing, the face of information security has changed from being an isolated issue to the key strategic business challenge. Information security management is a key aspect of IT governance as it forms the basis of privacy, risk management and IT governance (see figure below).



*Source: (Deane, Goldberg, Rakes, & Rees, 2019)*

Information security, IT security and IT governance all make a common part of Information Security Governance. Information security encompasses the collaborative efforts put in forth by the firms to protect the data and the information systems from the inappropriate access, modification, destruction and manipulation in order to ensure integrity and confidentiality of the data and systems (AlGhamidi, Win, & Vlahu-Gjorgievska, 2020). Information security governance includes the set of responsibilities and the practices that are exercised by the upper and lower management alike with a common goal of providing the strategic direction. It includes the ways through which organizations proceed towards achieving objectives while minimizing the risks of information breach.

Information security governance includes all the tools and processes that ensure that the organization has carried security for meeting the organizational needs. It requires the organization to set roles & responsibilities, defined tasks and performance measurements (Deane, Goldberg, Rakes, & Rees, 2019). There are several challenges that the companies are facing today in name of organizational information security. Information security holds a prime importance in organizations because the IS incidents and the breaches of security can directly impact the businesses and can halt the operations. The grave challenges facing the organization include security breaches and cyber-attacks. In order to analyze the problems, challenges and solutions related to cyber-attacks and information security in organizations, the role of information governance will be discussed critically using previous studies.

# Critical Literature Review

The threats of information breach and cyber-attacks are increasing as the organizations are diverging towards digital business strategies that require high level of technological deployment (Karanja, 2017). By diverting the business operations towards digitalization, the organizations have to fully embed and embrace the IT into business operations (Wu & Saunder, 2016). The major leading organizations including Airbnb and Uber are the dominant examples of how the distance between the physical world and IT digitalized world has been minimized (Schinagl & Shahim, 2020). Due to these advancements, the gap between security and the business operations have somewhat narrowed down. According to Wu & Saunders (2016), due to the shift towards digital technology, the firms are now required to embed information security into the whole IT governance structure so that the business challenges can be met with successfully.

Fazilda & Said (2015) reviewed the growing emergence of the information security threats that are required to be integrated by the organizational corporate governance and IT governance structure. According to the authors, the proper management of information security can aid IT governance by providing assistance and assurance in terms of integrity, confidentiality and availability of information. The firms who fail to formulate the IT security systems are prone to cyber-attacks that can lead to financial, reputational, client and partner losses and might result in litigation and government sanctions (Berkman et al., 2018). According to Hasbini et al. (2018), the cyber-attacks can also limit the firm’s innovation capability and might make it lose its competitive edge. For instance, the information security breaches might lead to negative market reaction and can cause the value, goodwill and materiality of the firm to fall (Higgs et al., 2016).

According to Georg (2017), many firms have been seen to experience deteriorating market value by 1 to 2.1% following the announcement of information security breach. Scholars have been finding evidences regarding strong negative correlation between firm’s overall value and the number of information security incidents (Berkman et al., 2018; Higgs et al, 2016). Deane et al. (2019) calculated the impact of the announcement about information security breach on the market value of the small and large firms. The study concluded that the IT investments in governance structure to oversee the security breaches can have a positive impact on the market value of the smaller firms. It was identified that the market tends to react positively to the information security certification and IT governance strategy (Deane, Goldberg, Rakes, & Rees, 2019).

Damenu & Beaumont (2017) argued that the recent outbreaks of cyber-attacks and security concerns have pushed the corporate boards to form sound IT governance strategies that include information security protocols and guidelines. The authors also stated that the senior executives play an important role in implementing sound and strong IT governance structure for limiting the cyber-attacks. Kemp (2018) also performed the study for analyzing the customers’ expectations regarding cyber security and information leakages. It was concluded by the authors that with ongoing information security breaches, the expectations of customers have increased towards corporations to take steps for protecting their security and privacy. As a result of the rising needs, several laws and regulations including General Data Protection Regulation have been emerged for strengthening the rights of the customers towards data protection (Romansky, 2017).

Tan et al. (2017) conducted a study for analyzing the information security as a part of IT governance structure in organizations. The study revealed information security strategy to be the cornerstone of the overall IT governance strategy in which the information security could be seen as a way for mitigating IT risks. Tan et al. (2017) also argued that the information security has a fluid and dynamic meaning because of the ever change socio-technical environment. Schinagl & Shahim (2020) viewed information security governance as a subset of the IT governance in the organizations today. According to the authors, information security controls, when implemented in the organizations, play a pivotal and vital role in ensuring that the controls are being implemented while the potential risks of breaches and threats are being minimized.

Rebollo et al. (2015) viewed information security governance as a leading path through which the companies can gain control of the security processes. By forming the information security governance strategy, the firms can ensure that the security processes are in alignment with the overall business strategy. Schinagl & Shahim (2020) also argued that although the information security is a subset of IT governance structure, little attention has been paid to it.

Damenu & Beaumont (2017) discussed the role of supportive security culture in combination with corporate governance structures for resolving the issues concerning information security threats. According to Fazilda & Said (2015), the firms must seek for developing sound IT governance system with subsets of information security protocols in order to achieve competitive edge, client satisfaction and trust creation. Ghamidi et al. (2020) carried on with the systematic literature review for establishing a sound information security governance framework in order to align the IT governance strategies, Corporate Governance strategies and information security policies. The review by Ghamidi et al. (2020) pointed towards developing a holistic framework of IT governance that connects the organizational objectives, communication strategies and information protection while ensuring compliance with procedures and guidelines.

Kauspadiene et al. (2017) reviewed the possibility of forming cyber-oriented IT governance models in which the concerns must be made towards increasing threats that are created due to digital communication and data dissemination. The model by the authors was based on the establishment of security systems that must consider the collaborative systems, multiple partners, third party applications and outsourcing. The authors proposed the businesses to form an integrated holistic framework that should be self-sustaining so that it could prevent cyber-attacks and information thefts. Moghadam & Colomo-Palacios (2018) also pointed towards formation of information security governance systems that entails risk management, security management and process management in order to uphold the business value of the firm.

In order to reduce the risks of information breach and cyber-attacks, several codes of practices including ISO 27002 has been formed at global level. According to Fazilda & Said (2015), various associations and the regulatory bodies have taken measures to inculcate the IT governance framework that entails the specific objectives to be achieved including control of IT, information protection from losses, quality software and information security. Thus the study signified that the information security falls under the large domain of IT governance. The leading IT governance structures include the COBIT, ISO 27001 and COSO that assists the senior management in having the information security management aligned with the overall business strategic goals.

Alghamdi et al. (2020) also highlighted the role of IT governance structure in maintaining minimum information security breaches. According to the authors, the optimal approach towards implementation of the IT governance varies from firm to firm. The key success factors for successfully integrating information security governance with IT governance includes effective communication, tailored good practices, availability of top executives’ support & direction on an ongoing basis and establishment of trust across all the management levels. IT governance implementation along with information security management must be properly managed. A security program using the top-down approach should be used for dealing with information security threats. The top-down approach points out towards the management’s involvement in initiating, supporting and directing the lower management for technology use and its management. A top-down approach ensures that the upper management is responsible for maintaining the integrity and security of the information systems implemented in the organization.

Georg (2017) provided an overview of the information security governance within the set of IT governance systems. According to the study, leadership commitment is a key to apply security systems across the organization. Requirements of security systems must be identified by the management and adequate resources must be put forth for dealing with the potential security risks. According to Georg (2017), it is with the help of leadership commitment, adequate resources and proper assignment of key roles & responsibilities that ensures implementation of IT governance structure in firms with a subset of information security governance.

# Conclusion

In a nutshell, sound information systems governance as a subset of IT governance within an organization can signal the overall attitude of company and its leadership towards information security risk. With growing dependency on digital technology, the information security threats call for integration of security measures within the IT governance framework. The literature review above clearly indicates how the narrow-focused isolated issue of information security has emerged out to be a strategic business issue as it can directly improve or reduce the goodwill and value of the company in the stock market. Although, security systems are considered to be a part of IT governance framework, still there is massive requirement of improvement in order to ensure that the security threats get covered under IT governance. By incorporating the information security systems within the large corporate governance framework of organizations, it is likely that it will complement IT governance in terms of confidentiality, integrity and information availability. By using frameworks like COBIT and following ISO 27001, the firms can manage to put extra attention on information security measures and maintain full communication with the low leel staff members so that it is ensured that the policy of information confidentiality is remained intact throughout the line of authority.

# References

AlGhamidi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*, 102030.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy , 37*(6), 508-526.

Damenu, T. K., & Beaumont, C. (2017). Analysing information security in a bank using soft systems methodology. *Information & Computer Security, 25*(3), 240-258.

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management , 20*(3), 107-121.

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance, 28*, 243-248.

Georg, L. (2017). Information security governance: pending legal responsibilities of non-executive boards. *Journal of Management & Governance , 21*(4), 793-814.

Hasbini, M. A., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development, 14*(1), 86-98.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems , 30*(3), 79-98.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security , 25*(3), 300-329.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. (2017). High-level self-sustaining information security management framework. *Baltic Journal of Modern Computing, 5*(1), 107.

Kemp, R. (2018). Legal aspects of cloud security. *Computer Law & Security Review, 34*(4), 928-932.

Moghadam, R., & Colomo-Palacios, R. (2018). Information security governance in big data environments: A systematic mapping. *Procedia Computer Science, 138*, 401-408.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology , 58*, 44-57.

Romansky, R. (2017). A survey of digital world opportunities and challenges for user’s privacy. *International Journal on Information Technologies and Security, 9*(4), 97-112.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? “From the basement to the boardroom”: towards digital security governance. *Information & Computer Security, 48*(2), 2056-4961.

Tan, T. H., Maynard, S. B., Ahmad, A., & Ruighaver, T. (2017). Information Security Governance: A Case Study of the Strategic Context of Information Security. *PACIS*, 43.

Wu, A., & Saunders, C. S. (2016). Governing the fiduciary relationship in information security services. *Decision Support Systems, 92*, 57-67.