International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

# Governance, risk and compliance frameworks applicability in the organizations

Aida Makaš *

*Department oF Economics, University of Buckingham, UK and Sarajevo School of Science and Technology, Bosnia and Herzegovina.*

International Journal of Science and Research Archive, 2023, 10(02), 716–724

Publication history: Received on 30 October 2023; revised on 05 December 2023; accepted on 08 December 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.10.2.1024

## Abstract

Governance, Risk and Compliance (GRC) is an emerging study embedding the importance of each element of the GRC and its strength in managing the organization and its sustainability. It becomes almost unavoidable to not have such a system in place. However, having it, can be costly and not efficient if the organizational system is not mature enough or financially stable enough to sustain the implementation and continuity of the GRC. The research investigates GRC systems in depth by (a) reviewing the literature on existing GRC frameworks, and (b) presenting a field study on GRC framework application in industries and organizations. The aim of this exploratory study is to understand the aspects and the nature of the GRC system following an enterprise systems approach. The result of this study is a framework of GRC characteristics that need to be taken into consideration when these systems are put in place. Structurally, this research was done based on the analysis, it is highlighted

- Overview of the GRC framework;
- Industry was GRC framework is most applicable;
- Organization size, they mostly fit in.

The result of this study is a guideline of GRC characteristics that need to be taken into consideration when these systems are put in place. By it, meaning, when deciding which governance system to put in place it is good to evaluate how it can help you in business continuity of the organization, and ability to mature and be cost effective for the organization. Further discussion about the issues, the concerns, and the diverse views on GRC would assist in developing an agenda for the future research on the GRC field.

**Keywords:** GRC; Corporate governance; Risk; Organization; Business continuity; Cost effectiveness

## 1. Introduction

The Sarbanes-Oxley Act (SOX), Basel II and the other international and regional regulatory mandates resulted in the expansive adoption of GRC software systems. (Anastasia Papazafeiropoulou & and Konstantina Spanaki, 2016)

With increasing impact of climate change, pandemics, financial distresses, technological changes, blockchain, cyberattacks, human capital movements and new age generations, and other risks which organizations are facing to their continuity and sustainability, implementation and maintenance of strong governance, risk and compliance system become one of the most important topics. However, there are challenges when it comes to its implementation and maintenance, ranging from not having internal team strong enough to sustain the system, having the complex core infrastructure or not having resources for implementation or for the maturity of such system that can in long-term benefit the organization structure and serve as preventive, protective and governing model. GRC acronym stands for Governance, Risk and Compliance as an integrated concept and describes different organizational activities, from

* Corresponding author: Aida Makaš; Email: aida.makas.am@gmail.com

arranging an annual audit to the establishment of internal continuous control monitoring procedures, to setting up roles and responsibilities in business processes and the system users, to data analytics procedures. The term GRC was initially introduced in 2004 by PricewaterhouseCoopers and since then is becoming a widely spread and important emerging solution for the business requirements of an organization (Gill and Purushottam, 2008).

Governance, risk management, and compliance (GRC) is an integrated framework that aims to align business operations with regulatory requirements, mitigate risks and ensure that the organization is managed effectively, efficiently, and ethically. The GRC framework includes structures, processes, and tools to manage governance, risk management, and compliance requirements in a coordinated and streamlined manner. (Kolkowska and Heimann, 2018)

While the literature refers to the GRC topic including different views regarding the different methodologies, which is analyzed (financial GRC, enterprise GRC, GRC IS etc.). This study focuses on the need to provide an overview of different GRC models from the organizational type by industry and size. Given the diversity of the opinions about GRC, the study will follow two sources of evidence. Initially a literature review will explore the academic research on GRC frameworks and implementations in different organizations.

## 2. GRC frameworks in the different organization literature overview

In this research have been analyzed overviews of each governance, risk and compliance frameworks and its implementation in different organizations depending on size and industries. The following fifteen most used GRC frameworks are analyzed: ISO Standards, COSO Framework, OCEG GRC Capability Model, ITIL Framework, NIST Cybersecurity Framework, Agile GRC, COBIT Framework, Privacy by Design, Social Responsibility and Sustainability (ESG), PCI DSS, HIPAA Security Rule, GDPR, FedRAMP, SOC Framework, GRI Sustainability Reporting Standards.

### 2.1. ISO Standards

According to ISO (2018), ISO standards provide a framework for implementing GRC practices in a systematic and consistent manner. Examples of relevant ISO standards include ISO 31000 (Risk Management), ISO 31203 (Business continuity management system), ISO 19600 (Compliance Management), and ISO 37001 (Anti-Bribery Management).(ISO Standards, 2018)

In the systematic literature review "The Use of ISO Standards as a Governance, Risk, and Compliance Framework" by (Santos and Santos, 2019) various types of organizations are referred to as those that have implemented ISO standards as a GRC framework. The review analyzed studies that reported the use of ISO standards in organizations of different industries, such as healthcare, finance, manufacturing, and information technology, among others. The review also considered studies from different organization sizes, including small and medium-sized enterprises (SMEs) and large multinational corporations. Overall, the review found that the use of ISO standards as a GRC framework is applicable to a wide range of organizations regardless of their industry or size.

However, on in another research by (.Kemper and Gasho, 2019) ISO standards are designed to be scalable and can be used by organizations of all types and sizes. Therefore, there is no specific size of organization that ISO standards are mainly recommended for. However, the implementation and maintenance of ISO standards may require more resources and expertise for larger organizations. Small and medium-sized enterprises may face fewer challenges in implementing ISO standards due to their simpler organizational structures.

(Compliance week, 2018) in its one of the weekly articles provides an overview of various ISO standards related to GRC, including ISO 19600 for compliance management, ISO 22301 for business continuity management, and ISO 27001 for information security management. The article discusses the benefits of using ISO standards for GRC, as well as some of the challenges and considerations for implementing them effectively. The article mentions various ISO standards related to GRC and how they can benefit organizations across different industries, not mentioning the specific type or size of the industry, indicating that can be used in various types. While in the study of internal auditors on role of the ISO standards in GRC, it has been mentions several examples of organizations across various industries that have successfully implemented ISO standards for GRC purposes, including: manufacturing industry (Fujitsu General America, Inc.), financial services industry (KeyBank), non-profit organization (World Wildlife Fund), healthcare industry (HealthTrust Purchasing Group). (The Institute of Internal Auditors (IIA), 2019)

### 2.2. COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework is a widely used GRC framework that provides guidance on internal control, enterprise risk management (ERM), and fraud deterrence. The

framework consists of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring. (Benjamin S. Neuhausen, 2019) The framework is widely used in industries such as finance, healthcare, and technology, among others. However, it is particularly relevant for larger, more complex organizations with multiple business units, subsidiaries, and international operations. (Vafeas, 2017)

The COSO Framework, a comprehensive study by Satori consulting, provides an overview of the COSO framework and its five components (control environment, risk assessment, control activities, information and communication, and monitoring activities). The guide also discusses how organizations across various industries can use the COSO framework as a GRC model to strengthen their internal controls and risk management processes. (Satori Consulting, 2021).

Some of the specific studies like in its study Evaluating the effectiveness of the COSO internal control framework providing the evidence from the Australian public sector (P. L. Boon, 2018) finds that the COSO framework is applicable and effective in improving internal controls and risk management processes in the public sector.

However even thought, the most studies, were analyzed large organizations, (M. F. Ali and et al., 2020) provided evidence from Malaysia SME sector on the impact of the COSO framework where study examined the impact of the COSO framework on small and medium-sized enterprises (SMEs) in Malaysia. The study finds that the implementation of the COSO framework is positively associated with improved internal controls and risk management processes in SMEs.

On another side one of the most used sectors of COSO framework is financial industry. (C. O. Nwanyanwu and and I. N. Ezeoha, 2021) finds that the implementation of the COSO framework is positively associated with improved financial performance in the banking industry.

### 2.3. OCEG GRC Capability Model

The Open Compliance and Ethics Group (OCEG) has developed a comprehensive framework for implementing GRC practices called the GRC Capability Model. This framework includes elements such as Governance, Risk Management, Compliance Management, Information Management, Performance Management, and Assurance.

The OCEG GRC Capability Model is designed to be used by organizations of all sizes and across all industries. It is a flexible framework that can be customized to meet the specific needs of each organization. However, it is particularly relevant for organizations with complex risk environments, high levels of regulatory oversight, and a need for integrated GRC practices. According to a survey conducted by OCEG, the majority of respondents were from large organizations with more than 1,000 employees, and the most represented industries were financial services, healthcare, and manufacturing. However, the model can be used by organizations of all sizes and across all industries. (OCEG, 2021)

### 2.4. ITIL Framework

The Information Technology Infrastructure Library (ITIL) provides a framework for managing IT services and ensuring that they align with business objectives and comply with applicable laws and regulations. The ITIL framework is mainly used in the information technology (IT) industry, and it can be applied to organizations of various sizes, from small to large. According to (Axelos, 2021) the organization that manages the ITIL framework, ITIL is used by "thousands of organizations worldwide, across industries, sectors, and public and private businesses." It is particularly relevant for organizations that rely heavily on IT systems and services.

Specifically, the ITIL framework was examined in SME and hospitality sector by (T. Chan and et al., 2020). The study found that ITIL is not widely adopted in the hospitality industry and SME sector. According to the study, the reasons for non-adoption were primarily due to the perceived high costs of implementing the framework, a lack of IT expertise and understanding, and a lack of awareness about the benefits of ITIL among stakeholders. The study also highlighted the need for more tailored and flexible IT service management frameworks for SMEs and the hospitality industry. (K. Trkman et al., 2016) analyzes implementation of ITIL framework in Slovenian Ministry of Public Administration, and also found challenges during the implementation. Some of the challenges mentioned include resistance to change, lack of understanding of ITIL, inadequate resources and budget, lack of leadership support, and difficulty in measuring the benefits of the implementation.

(ISACA, 2014) in study about ITIL frameworks for IT governance, focus on how organizations, in various industries like healtcare, finance, government and retail can use them to align IT with business objectives and manage IT-related risks, and how to overcome the challenges implementing ITIL framework. By understanding these reasons, organizations can make informed decisions about whether to adopt these frameworks and how to overcome any potential obstacles

during implementation. Additionally, understanding the reasons for not being adopted can help identify areas for improvement in the frameworks themselves to make them more applicable and accessible to a wider range of organizations.

### 2.5. COBIT Framework

The Control Objectives for Information and Related Technology (COBIT) framework provides a comprehensive approach to IT governance and risk management that is widely used in the technology industry some of most cited industry that uses the COBIT is financial industry, particularly banking sector. Like (R. Abbas and et al., 2015), also (J. A. Botha and et al., 2011) studied the COBIT as a GRC framework in banking sector that adopted the COBIT. It discusses the benefits and challenges of using COBIT, and how the bank customized COBIT to meet its specific needs.

### 2.6. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has developed a framework for managing cybersecurity risks that is used by many organizations in the United States.

The NIST Cybersecurity Framework is mainly used by organizations that manage critical infrastructure, such as energy, finance, healthcare, and government agencies. It can be used by organizations of all sizes, but it is particularly relevant for medium to large organizations that have complex IT environments and are subject to regulatory compliance requirements.(Md Rakibul Islam and Kamal Hossain, 2020).

The NIST Cybersecurity Framework has been adopted by organizations in various sectors including critical infrastructure, financial services, healthcare, and higher education.(Congressional Research Service, 2018)

### 2.7. Agile GRC

Agile GRC is an approach to GRC that emphasizes collaboration, flexibility, and rapid adaptation to changing risk and compliance requirements. According to (Haase and Endres, 2021) agile GRC is designed to be flexible and adaptable to different contexts, including small and medium-sized businesses, as well as larger enterprises. The framework emphasizes collaboration, communication, and continuous improvement in managing governance, risk, and compliance, they note that the Agile approach is increasingly being adopted by organizations of all sizes and across various sectors due to its flexibility, speed, and adaptability to changing business needs. They also highlight that the Agile GRC Framework can be particularly useful for organizations that operate in highly regulated industries, such as finance and healthcare, where compliance requirements are complex and constantly evolving.

The term "Agile GRC" is a relatively new concept that has not yet been widely adopted or defined within the GRC community.

### 2.8. GRI Framework

The GRI Sustainability Reporting Standards are a set of guidelines for companies to report on their sustainability performance. They provide a framework for organizations to disclose information on a range of sustainability topics, including environmental impact, labor practices, human rights, and anti-corruption measures. The GRI Standards are widely recognized as a leading framework for sustainability reporting. Implementation of sustainability reporting standards are widely used across various sectors, including consumer goods, financial services, and energy.(Van der Waal and & Schouten, 2019)

GRI Standards are widely in the sustainability reporting of educational institutions, according to (Lozano *et al.*, 2015). The KPMG Survey of Corporate Responsibility Reporting 2020, this survey covers sustainability reporting trends among companies around the world and finds that the GRI Standards are the most widely used sustainability reporting framework. The report notes that the GRI Standards are used across all industry sectors and by organizations of various sizes, from small to large. (KPMG International., 2020)

### 2.9. Privacy by Design

Privacy by Design is an approach to building privacy protections into products and services from the ground up, rather than as an afterthought. This can help organizations to comply with privacy regulations and mitigate privacy-related risks. It is mainly related to companies in tech industry.(Shu He and Aleksandra Korolova, 2019) and big data analytics organizations.(Khaled El Emam and Luk Arbuckle, 2014). These sources suggest that the Privacy by Design framework

is applicable to a wide range of industries and organizations, particularly those that handle sensitive personal information.

They highlight the benefits of embedding privacy considerations into the design of products and services, and provide examples of organizations that have successfully implemented the framework in practice. However, they also recognize the challenges of implementing the framework, particularly in the context of emerging technologies such as big data analytics.

### 2.10. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that are designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. The standard was created by the major credit card brands (Visa, Mastercard, American Express, Discover and JCB) in order to establish a common set of guidelines for protecting sensitive data.(Mukherjee and Sen, 2018)

Payment Card Industry Data Security Standard (PCI DSS) is primarily used by organizations in the financial industry, including banks, credit card companies, and payment processors. It also notes that smaller organizations, such as merchants and service providers, may also need to comply with PCI DSS if they handle payment card data. (Mukherjee and Sen, 2018)and (Ruchita Bansal, Rupali Bagga and Deepika Ahuja, 2019) similarly notes that PCI DSS is primarily relevant to organizations in the financial industry, including banks, payment processors, and merchants. It also discusses the challenges that organizations may face in achieving PCI DSS compliance, including the high costs and complexity of implementing the necessary controls.

Payment Card Industry Data Security Standard (PCI DSS) Compliance is applicable for Security Controls in Small and Medium Enterprises (SMEs handling payment card data, however it is challenging implementation due to limited resources and lack of awareness of the standard. (M. Asif Naeem, Andrew Woodward and Ali Al-Badi, 2017)

### 2.11. HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule applying governance, risk, and compliance principles to healthcare organizations. HIPAA regulations have many similarities with GRC frameworks, and that GRC can help organizations establish a comprehensive and proactive approach to HIPAA compliance.(Allison M. Callahan, 2018)

### 2.12. GDPR

General Data Protection Regulation (GDPR) is a comprehensive data privacy law enacted by the European Union (EU) in 2016 and became enforceable in May 2018. The GDPR provides a set of rules and principles to govern the processing and protection of personal data of individuals within the EU, as well as the transfer of personal data outside the EU. The GDPR applies to any organization that processes personal data of individuals within the EU, regardless of where the organization is based. The GDPR aims to strengthen data protection rights for individuals and harmonize data protection laws across the EU member states.

The industries that are most affected by the GDPR, including those that process large amounts of personal data such as healthcare, finance, and e-commerce (Allison M. Callahan, 2018). By (Aniko Hannak and David Lazer, 2018) the industries that are most affected by it, including healthcare, finance, and technology.

### 2.13. FedRAMP

Federal Risk and Authorization Management Program (FedRAMP) is a framework for assessing and authorizing cloud service providers (CSPs) that wish to offer services to the U.S. federal government.

The FEDRAMP is mainly used in government, including federal agencies, state and local governments, and private sector organizations.(Joshua J. Pauli, 2018) and (Kathryn K. Schiller, Jennifer L. Bayuk and Shadi A. Nashwan, 2018) mentioning the industries including federal agencies, state and local governments, and private sector organizations.

### 2.14. SOC Framework

SOC stands for System and Organization Controls. It is a framework developed by the American Institute of Certified Public Accountants (AICPA) that provides a set of standards and guidelines for service organizations to demonstrate that they have effective controls in place for their customers' data and systems. SOC reports are often requested by

customers of service organizations, such as cloud service providers, to assess the effectiveness of the controls implemented by the service provider in protecting their data and systems. Compliance Frameworks for Cloud Service Providers" by the Cloud Security Alliance (2017): This paper provides an overview of the SOC framework and its relevance for cloud service providers. The paper also explains the differences between SOC 1, SOC 2, and SOC 3 reports, and provides guidance on how organizations can use SOC reports to meet their compliance and risk management needs. SOC 1 and SOC 2 are both.

## 3. Discussion

The purpose of this paper is to draw a clearer picture of GRC frameworks based on organizational size, type and industry in order to contribute to a clearer understanding of GRC frameworks and help in the implementation in real sector. Through the literature overview of GRC frameworks, it was overviewed industries, size and types of different organizations who implemented the GRC framework.

The following are some of the main conclusions from the overview:

**Table 1** GRC framework comparison by industry and type

| GRC Frameworks | Industry | Organization size or type |
|---|---|---|
| ISO Standards | All industries | Mainly Large size of the organizations due to cost of ISO standard maintenance |
| COSO Framework | All industries | Mainly Large size of the organizations due to cost of cost of implementation |
| OCEG GRC Capability Model | Implemented is in the financial services, healthcare, and manufacturing.<br><br>However, the model can be used by organizations in all industries. | It is particularly relevant for organizations with complex risk environments, high levels of regulatory oversight and a need for integrated GRC practice. |
| ITIL Framework: | IT model- based GRC framework,<br><br>Applicable to any industry, however specific industries based on the studies that use ITIL are: hospitality industry, public admin, healthcare, finance, government, and retail. | It is particularly relevant for organizations that rely heavily on IT systems and services.<br><br>Large size and SMEs (however it can be challenging for SME due to cost of implementation, understanding, resources availability, and maintenance) |
| NIST Cybersecurity Framework | Mainly used by organizations that manage critical infrastructure, such as energy, finance, healthcare, and government agencies, higher education. | It can be used by organizations of all sizes, but it is particularly relevant for medium to large organizations that have complex IT environments and are subject to regulatory compliance requirements. |
| Agile GRC: | The framework is flexible and adaptable to different context, however due to its newly introduction, there is lack of scientific articles analyzing the implementation in various industries. | It is designed to be flexible and adaptable to different contexts, including small and medium-sized businesses, as well as larger enterprises. |
| COBIT Framework | various sectors, including consumer goods, financial services, educational institutions, and energy. | Large organizations and SME (however it can be challenging for SME due to cost of implementation, understanding, resources availability, and maintenance) |
| Privacy by Design | The framework is applicable to a wide range of industries and organizations, particularly those that handle sensitive personal information. | Sensitive personal information handing organizations large or small. However, they also recognize the challenges of implementing the |

| | | |
|---|---|---|
| | | framework, particularly in the context of emerging technologies such as big data analytics. |
| PCI DSS | Mainly in the financial industry, including banks, payment processors, and merchants. | large organizations due to the high costs and complexity of implementing the necessary controls |
| HIPAA Security Rule | Healthcare industry mainly | healthcare all size |
| GDPR | The industries that are most affected by the GDPR, including healthcare, finance, and technology | Large organization mainly due to cost of implementation, complexity of understanding the framework, resources available to maintain. |
| FedRAMP | Mainly applicable to industries, including government agencies, healthcare organizations, and financial institutions. | Large organizations transit to cloud computing and driven by cost reduction. |
| SOC Framework | Organizations: companies that process, store, or transmit sensitive information, such as healthcare providers, financial institutions, and technology companies. | Medium to Large organizations |
| GRI Sustainability Reporting Standards | specific organizations across various industries, including banking, energy, healthcare, and telecommunications. | The size of the organizations mentioned ranges from small businesses to large multinational corporations. |

Source: Author summary of literature review

Some limitations of the study are typical of the ones met in qualitative studies such as the number of participants as well as the geographical context of the research. These limitations were alleviated to a certain degree by the participants' vast experience in GRC projects in various organizational and geographical settings. These can be addressed in future studies by including views from other organizations/experts. Additionally, future research in the field can use this analysis of the GRC characteristics and investigate further the ways of improving and enhancing the GRC practice.

## 4. Conclusion

The purpose of this paper is to draw a clearer picture of GRC frameworks based on organizational size type and industry in order to contribute to a clearer understanding of GRC frameworks and help in the implementation in real sector.

From the studies conducted earlier, we can understand that implementation of proper governance, risk and compliance models are necessary for the organization and context where the organization exist, however, due to its costly implementation it was mainly implemented by larger organizations. Furthermore, such gap could be assessed on larger government level, where governance, risk and compliance could be modified and regulatory implemented for all sizes, industries which will impact performance, and regulate the risks organizations operate in.

Some limitations of the study are typical of the ones met in qualitative studies such as the number of participants as well as the geographical context of the research. These limitations were alleviated to a certain degree by the participants' vast experience in GRC projects in various organizational and geographical settings. These can be addressed in future studies by including views from other organizations/experts. Additionally, future research in the field can use this analysis of the GRC characteristics and investigate further the ways of improving and enhancing the GRC practice.

## References

[1] Allison M. Callahan (2018) 'Security Rule applying governance, risk, and compliance principles to HIPAA compliance', Journal of Health Information Management. [Preprint].

[2] Anastasia Papazafeiropoulou & and Konstantina Spanaki (2016) 'Understanding governance, risk and compliance information systems (GRC IS): The experts view', Inf Syst Front , 18:1251–1263.

[3] Aniko Hannak and David Lazer (2018) 'The EU General Data Protection Regulation (GDPR) and Its Implications for Big Data Research', Big Data & Society, , 5(2).

[4] Axelos (2021) 'ITIL: The Basics'.

[5] Benjamin S. Neuhausen (2019) 'COSO Framework: Benefits and Limitations ', Journal of Accountancy. [Preprint].

[6] C. O. Nwanyanwu and and I. N. Ezeoha (2021) 'The impact of the COSO internal control framework on financial performance: Evidence from the Nigerian banking industry'.

[7] Compliance week (2018) 'ISO Standards for Governance, Risk and Compliance', Compliance week [Preprint].

[8] Congressional Research Service (2018) 'NIST Cybersecurity Framework: Analysis, Implementation, and Implications'.

[9] Gill, S., & and Purushottam, U. (2008) 'Integrated GRC-is your organization ready to move. Governance, risk and compliance', SETLabs Briefings [Preprint].

[10] Haase, A.C. and Endres, T. (2021) 'Integrating Agile and Governance, Risk Management, and Compliance (GRC) Frameworks. ', In Agile Methods for Safety-Critical Systems (pp. 307-328). Springer. [Preprint].

[11] ISACA (2014) 'IT Governance Using COBIT and ITIL: A Strategic Approach'.

[12] ISO Standards (2018) ' ISO 31000:2018 Risk management – Guidelines. International Organization for Standardization.', ISO Standards [Preprint].

[13] J. A. Botha and et al. (2011) 'COBIT as a Framework for IT Governance and Management: A Case Study of a South African Bank'. Available at: https://www.scielo.br/scielo.php?pid=S1807-17752011000200002&script=sci_arttext&tlng=en (Accessed: 15 April 2023).

[14] Joshua J. Pauli (2018) 'Federal Risk and Authorization Management Program (FedRAMP): A Framework for Secure Cloud Computing in Government', Journal of Cybersecurity and Privacy, 7(2).

[15] K. Trkman et al. (2016) 'Implementing ITIL Service Management Practices in the Public Sector'.

[16] Kathryn K. Schiller, Jennifer L. Bayuk and Shadi A. Nashwan (2018) 'The Benefits and Challenges of the Federal Risk and Authorization Management Program (FedRAMP) '.

[17] .Kemper, H.G. and Gasho, V. (2019) 'Governance, risk management, and compliance: It's time for convergence', Business Horizons, , 62(1),(109-117. doi: 10.1016/j.bushor.2018.08.004).

[18] Khaled El Emam and Luk Arbuckle (2014) 'Privacy by Design in the Age of Big Data ', The Journal of Technology Science [Preprint].

[19] Kolkowska, E., & and Heimann, R. (2018) 'Governance, risk management, and compliance in organizations: A literature review', Journal of Accounting & Organizational Change, 14(3),(394-423. doi: 10.1108/JAOC-01-2018–0016).

[20] KPMG International. (2020) ' The KPMG Survey of Corporate Responsibility Reporting 2020.'

[21] Lozano, R., C.K., et al. (2015) 'A review of commitment and implementation of sustainable development in higher education: results from a worldwide survey. ', Journal of Cleaner Production, , 108, .(1–18).

[22] M. Asif Naeem, Andrew Woodward and Ali Al-Badi (2017) 'Payment Card Industry Data Security Standard (PCI DSS) Compliance and the Challenges of Implementing Security Controls in Small and Medium Enterprises (SMEs) ', International Journal of Information Security and Privacy. , 11(2).

[23] M. F. Ali and et al. (2020) 'The impact of the COSO framework on small and medium-sized enterprises: Evidence from Malaysia'.

[24] Md Rakibul Islam and Kamal Hossain (2020) 'Cybersecurity and the NIST Framework: A Content Analysis of Literature'.

[25] Mukherjee, A. and Sen, A. (2018) 'Evaluating the effectiveness of the Payment Card Industry Data Security Standard (PCI DSS) in mitigating payment card fraud.', Information Systems Frontiers, , 20(6)(1279-1294. https://doi.org/10.1007/s10796-017-9814-2).

[26] OCEG (2021) 'GRC Capability Model Overview. '.

[27] P. L. Boon, et al. (2018) 'Evaluating the effectiveness of the COSO internal control framework: Evidence from the Australian public sector', Australasian Accounting, Business and Finance Journal, 12(1).

[28] R. Abbas and et al. (2015) Enterprise Information Systems for Business Integration in SMEs. 9781466681836th edn. IGI Global.

[29] Ruchita Bansal, Rupali Bagga and Deepika Ahuja (2019) 'Payment Card Industry Data Security Standard (PCI DSS) Compliance: Challenges and Solutions', International Conference on Computing, Communication and Signal Processing (ICCCSP) [Preprint].

[30] Santos, E. and Santos, E. (2019) 'The Use of ISO Standards as a Governance, Risk, and Compliance Framework'.

[31] Satori Consulting (2021) 'The COSO Framework: A Comprehensive Guide'.

[32] Shu He and Aleksandra Korolova (2019) 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents', Proceedings of the ACM on Human-Computer Interaction (PACM HCI) [Preprint]. Available at: https://dl.acm.org/doi/abs/10.1145/3359203 (Accessed: 15 April 2023).

[33] T. Chan and et al. (2020) 'Adoption of IT Service Management Frameworks: A Qualitative Study'.

[34] The Institute of Internal Auditors (IIA) (2019) 'The Role of ISO Standards in GRC', The Institute of Internal Auditors (IIA) [Preprint].

[35] Vafeas, N. (2017) ' COSO: An ongoing evolution', Journal of Accounting and Public Policy, 36(1)(1-6. doi: 10.1016/j.jaccpubpol.2016.11.001).

[36] Van der Waal, J., and & Schouten, G. (2019) ' The development and implementation of sustainability reporting guidelines: A study of the Global Reporting Initiative. J', ournal of Cleaner Production, 222,(236-243.).