

Conceptual Review: Compatibility of regulatory requirements of FSA to Insurance industry in Indonesia for Integrated GRC

Stefiany Norimarna¹

¹Center for Risk Management and Sustainability, Indonesia

Abstract

This study aims to obtain understanding and assurance whether the regulatory requirements of FSA for integrated GRC to the insurance industry are compatible with the requirements and suggested practices of ISO 37000 on Governance, ISO 31000 on risk management, and ISO 37301 on Compliance. The qualitative approach in which literature review and comparative study are conducted to find the degree of fitness of POJK with these ISO standards (ISO 37000, ISO 31000, and ISO 37301). This study found out that the regulatory requirements set forth by FSA (Financial Services Authority) to Insurance Industry for integrated GRC have all been compatible with all the elements of ISO 37000, ISO 31000, and ISO 37301. It means Insurance companies could use those ISO as standards. Therefore, it would be some efforts needed by the industry to carry out their learning curves in assuring the implementation of integrated GRC is continuously calibrated to their respective context either as an insurance company in general or as a particular organization that has its own respective and unique characteristic. The result of this paper could be used as generic inputs and considerations for insurance companies that have initiated their integrated GRC practices and/or just recently commenced and/or improved their practices more effectively.

Keywords: Integrated GRC, ISO 37000 Governance, ISO 31000 Risk Management, ISO 37301 Compliance, Insurance industry



This is an open access article under the CC-BY-NC license.

INTRODUCTION

GRC Implementation goes far beyond the critical roles of corporate Governance, Risk, and Compliance. The reason is that the GRC also covers other vital areas, namely Internal audit; Compliance and risk; The field of law; Finance; Information Technology (IT); Human Resources (HR), and Line of business, executive chain, and Board of directors.

GRC refers to human resources, processes, technology, and information that help companies achieve principled performance conditions. In other words, GRC is the path to realizing principled performance. GRC refers to capabilities that help organizations achieve goals, deal with uncertainty, and act in the name of integrity.

In Indonesia, many organizations are doing GRC activities with a silo mentality; therefore, it creates redundancies and gaps between the interrelated risks in various business processes within an enterprise. Consequently, organizations often deal with processes with a high level of inefficiency, ineffectiveness, and lack of agility.

However, based on the GRC Survey 2019, the survey result shows that 25.7% of respondents have not made any efforts to integrate GRC in their organization, including the Financial Services industry and

Corresponding author

Stefinay_norimarna@yahoo.com

DOI: <https://doi.org/10.31098/bmss.v1i5.456>

Research Synergy Foundation

Insurance as the TOP 1 industry in Integrated GRC. It could be encouraged because the FSA regulates the implementation of Governance, risk management, and Compliance for Insurance Companies.

Organizations in Indonesia understand the importance of integrating GRC; however, they remain unsure how to reach there. In that regard, we would like to confirm whether regulatory requirements as set forth by FSA (Financial Services Authority) to Insurance Industry for integrated GRC have all been compatible with all the elements of ISO 37000, ISO 31000, and ISO 37301.

ISO 37000, ISO 31000, and ISO 37301 are guidelines for organizations' Governance, risk management, and Compliance. ISO 37000 provides key principles, relevant practices, and a framework as guidelines for the Governance of organizations in meeting their responsibilities to fulfil their purpose. ISO 31000 provides principles, a framework, and a process for managing risk that can help organizations increase the likelihood of achieving objectives by identifying opportunities and threats and effectively allocating and using resources for risk treatment. While ISO 37301 specifies requirements and guidelines for establishing, developing, implementing, evaluating, maintaining, and improving an effective compliance management system within an organization.

LITERATURE REVIEW

Governance

Governance is simply 'the culture, values, mission, structure, and layers of policies, processes, and measures by which organizations are directed and controlled' (OECD, 2004). The Institute of Internal Auditors (IIA) defines Governance as structures and processes in an organization to attain its objectives by Board's advising, directing, managing, and monitoring an organization's activities (IIA, 2010).

IFC defines corporate Governance as "the structures and processes for the direction and control of companies. However, the concept of corporate Governance has now evolved from the ownership structure through to the processes and procedures of the firm. Thus corporate governance should be seen to involve the relationship among the firm and its stakeholders. Corporate Governance focuses on a company's structure and processes to ensure fair, responsible, transparent, and accountable corporate behavior.

Numerous codes of best practices and corporate governance principles have been developed over the last ten years. The OECD Principles have gained worldwide acceptance, addressing policymakers and businesses and focusing on the entire governance framework (shareholder rights, stakeholders, disclosure, and board practices). The OECD corporate governance framework is built on four core values: Fairness, Responsibility, Transparency, and Accountability.

In 2021, the new standard ISO 37000 was developed by experts and trusted voices from many worldwide organizations. ISO 37000 provides a globally accepted reference for all organizations, regardless of size, type, or location. Governing bodies need to ensure that their organizations act with purpose, sustainability, and society in mind. ISO 37000 also provides comprehensive guidance for the Board of Directors by distilling Governance into eleven principles, the foundation of successful organizations, ensuring that they are well-governed, well-managed, and socially responsible.

ISO 37000 can assist organizations in building robust governance systems to mitigate risks, improve transparency and hold them accountable in the face of heightened scrutiny from all levels of society. It provides a clear roadmap for organizations to achieve their purpose and value strategically and improve

their overall accountability at all levels. Governing bodies need to ensure that their organizations remain viable and perform over time as we strive to fulfil the UN Sustainable Development Goals and Vision 2030.

Risk Management

Due to the increasing demand and need for integrated ERM within the enterprise level, the International Organization for Standardization (ISO) has issued the ISO 31000 standard. The first edition was released in 2009 entitled "risk management – principles and guidelines" and is known as the ISO 31000:2009 (ISO, 2009). The ISO 31000:2009 standard aims to aid organizations in implementing integrated risk management within their activities, infusing the principles of ERM within its governance structure and mechanism, and enhancing its value through its decision-making process.

The second and current edition was released in 2018 (i.e., ISO 31000:2018) and renamed to "risk management – guideline" (ISO, 2018). Within the ISO 31000:2018 standard latest edition, the primary changes that have taken place to revolve around the emphasis on the continual nature of risk management and the revision of the risk management principles. It also concentrates on the open system model to accommodate the organization's numerous needs and context. It focuses on the leadership aspect and the integration of risk management that begins from the organization's Governance (ISO, 2018). Even though the respective standard is updated, its purpose remains unchanged: to enhance the organization's value creation and protection through the application of risk management, continual improvement, and risk-oriented decision making. Similar to its predecessor, within the latest ISO 31000:2018 standard, there are three fundamental components in building and implementing a practical, efficient, and integrated ERM, namely (1) the principles, (2) the framework, and (3) the process of risk management. Furthermore, these three components are interdependent. To have effective risk management, the organization must ensure that its activities and governance structure reflect the risk management principles.

The adoption of the ISO 31000 standard gains broad acceptance in many countries and large corporations as it is practical and business-oriented. Although some challenges still need to be addressed, the ISO 31000 standard tries to harmonize risk management practices and achieve a global benchmark for risk management (Almeida et al., 2019; Leitch, 2010; Purdy, 2010). The ISO 31000 standard has established the risk management principles, framework, and process in managing the enterprise risks, relevant and appropriate to any organization (Choo & Goh, 2015). Thus, the ISO 31000 standard captures ERM as an integrated way of managing risk rather than merely an ERM framework. Furthermore, its universal characteristics make them applicable for any organization.

Since the ISO 31000 standard has the universal trait, it applies to any organization. As the only G20 country in the SEA region, Indonesia adopted ISO 31000 as their national risk management standard, namely SNI ISO 31000 (*Standar Nasional Indonesia ISO 31000* in Indonesian) in 2011. However, implementing ISO 31000-based integrated risk management started in 2018 in the Indonesian Ministry of Finance and was followed by some other general government bodies in 2019, such as the Financial Services Authority, the Central Bank of Indonesia, and the Supreme Audit Board.

Compliance

During the global financial crisis and the COVID-19 pandemic, many companies focused their risk and compliance activities on protecting themselves from downside risks to meet evolving regulatory

requirements. The risk and compliance functions are expected to protect companies from downside risks and shift toward strategic advice to support growth and change. For others—companies that had significantly expanded the functions after the financial crisis to meet specific regulatory requirements—it is about right-sizing and developing a true value proposition beyond regulatory issues.

Open Compliance and Ethics Group (OCEG) (2019) states that to help an organization drive towards its objectives, they must put Compliance and ethics at the center. Organizations must act with integrity and stay within mandated boundaries (laws, rules, and regulations) and voluntary boundaries (organization values). The main goals of Compliance should include those related to legal and regulatory requirements, with internal policies, managing compliance risks, and establishing an ethical culture.

In 2014, ISO 19600 was first introduced and recognized as the international standard for best compliance management practices that provided a detailed guideline standard for effective compliance programs. This year, the ISO 37301 framework, published in April 2021, provides a certifiable global benchmark for compliance systems.

The ISO 37301 requirements are flexible. It recognizes that each organization is responsible for determining the needs of their compliance management system and how to implement the recommended practices ultimately. The standard applies to all types of organizations, irrespective of their size, industry, risk exposure, or global footprint, including private organizations, public organizations, and non-profit organizations. The ISO 37301 encourages organizations to focus on the systematic implementation of an organization-wide compliance system.

GRC Implementation in Insurance Company

Nowadays, it is becoming crucial for the company boards to understand better the evolving landscape of financial crimes, such as money laundering, terrorist financing, market abuse, fraud, bribery, and corruption, and what effective countermeasures should be in place for control and prevention.

The Open Compliance and Ethics Group's (OCEG) notion integrates governance, risk management, internal control, assurance, and compliance into one primary function: the GRC capability model (Mitchell & Stern Switzer, 2013). GRC integrates capabilities to enable an organization to reliably achieve objectives while addressing uncertainty and acting with integrity (OCEG).

Accelerated globalization, changing consumer preferences, volatilities in the cybersecurity environment, and the dynamic regulatory landscape combined made the modern business landscape a tricky place to navigate, especially for the insurance company. In that regard, insurance companies need to invest in GRC strategies to facilitate good Governance, better risk management, and regulatory compliance.

The literature mentions several possible reasons for risk governance failures in insurance companies. Eling and Marek's (2014) research and identify poor risk culture as the central problem and attributes it to executives' variable compensation on the UK and German insurance markets. Kleffner et al. (2003) find that organizational structure was a deterrent to adopting ERM in Canadian insurance companies, and there is a high resistance to change.

Conceptual Review: Compatibility of regulatory requirements of FSA to Insurance industry in Indonesia for Integrated GRC

Stefiany Norimarna

In Indonesia, many organizations are doing GRC activities with a silo mentality; therefore, it creates redundancies and gaps between the interrelated risks in various business processes within an enterprise. Consequently, organizations often deal with processes with a high level of inefficiency, ineffectiveness, and lack of agility.

Some benefits of GRC Implementation are a value-adding principle essential to organization competitiveness (PricewaterhouseCoopers, 2004); more efficient and effective performance capabilities (Grant Thornton International, 2009)

and an improved level of maturity in their Enterprise Risk Management (ERM) capabilities (Grant Thornton International, 2009; OCEG, 2008).

Integrated GRC Using ISO-based Series

ISO 37000:2021 - Governance of organizations — Guidance, ISO 31000:2018 Risk Management Guidelines, and ISO 37301: 2021 Compliance Management System are standards or guidelines with a similar structure based on four phases PDCA (Plan-Do-Check-Act) cycle. It consists of principles, framework, policy, plan, implement, evaluate, and improvement. Alijoyo (2020) said that although they could be used independently and separately, they are compatible and become a cohesive reference to implement integrated GRC.

The interconnection among those three ISO series to support the integration of GRC could be seen below:

Table1. Interconnection of ISO 37000 – ISO 31000 – ISO 37301

	MANAGEMENT SYSTEM STANDARD	PHASE I: PLAN			PHASE II: DO	MANAGEMENT SYSTEM STANDARD	PHASE III: CHECK			PHASE IV: ACT	MANAGEMENT SYSTEM STANDARD	PHASE V: IMPROVEMENT		
		ISO/DIS 37000	ISO 31000	ISO 37301			ISO/DIS 37000	ISO 31000	ISO 37301			ISO/DIS 37000	ISO 31000	ISO 37301
	1. INTEGRATED MANAGEMENT POLICY					3. SUPPORT & OPERATION					4. MONITORING & REVIEW			
	Management system, policy, and Management commitment & leadership	4.2 7.7	5 5.2 5.3 5.4.2	4.4 5.1 5.2 5.3		3.1. Resources (personnel, infrastructure, cost)	5 5.1	5.4.4 7.1 7.2	7.1 7.2		4.1. Performance monitoring and measurement of process and procedures.	7.4 5.6 6.6.	5.6 6.6.	9.1
	2. PLANNING					3.2. Competencies, awareness, training.	5.2	4 5.4.4	7.2 7.2.3 7.3		4.2. Audit of non-compliance, non-conformities, and investigation	7.4.3	5.6	8.3 8.4 9.2
	2.1. Organizational context, stakeholders needs & expectation	4.1 4.3	5.4.1 6.3 6.3.3	4.1 4.2 4.3 4.5		3.3. Communication, coordination, and cooperation.	7.5	5.4.5 6.2	7.4		4.3. Management review	7.4.3	5.4.2 5.6	9.3.2 9.3.3
	2.2. Objectives and targets setting	7.1 7.2	5.5 6.4	4.5 6.2		3.4. Documented information	7.8	6.7	7.5		4.4. Recording & reporting	7.5.3	6.7	9.1.5
	2.3. Risk assessment	7.3.3	6.4	4.6		3.5. Control of documents		6.7	7.5.3		5. IMPROVEMENT			
	2.4. Programs to address risk and opportunities that affect objectives/targets.	7.3	5.5 6.5	6.1		3.5. Operational planning, execution and control of operation risks.	7.9	6.5.2 6.5.3	8.1		5.1. Improvement Plan	7.3.3 7.11	5.7	10.1
	2.5. Internal control plan to address operation risk	7.3	6.5.2 6.5.3	8.1 8.2		3.6. Operationalization of contingency plan.	7.4 7.4.3	6.5.3	8.1 8.4		5.2. Corretive actions, adaptation, and improvement.	7.11.3	5.7.1 5.7.2	10.2
	2.6. Emergency/contingency plan	7.4 7.4.3	6.5.3	8.1 8.4										

Source: Alijoyo (2020)

The use of ISO-based integrated GRC will help the organization clarify work relations between Governance, risk management, and Compliance, which allow an organization to optimize its GRC practice more effectively and efficiently. Despite there are many more benefits that can be produced through the use of ISO series, Alijoyo (2020) pointed out that since there are many adopters of ISO-based series globally, it is more practical for an organization to do benchmarking either to obtain a faster learning curve or to enrich their continual improvement.

RESEARCH AND METHODOLOGY

In order to answer the research question posed in the Introduction, this study will focus on 2 (two) steps.

Firstly, a literature review is performed by selecting papers about using ISO 31000, ISO 37000, and ISO 37301 in Insurance and GRC integrated approach implementation in Insurance. The papers are selected by using the Google Scholar search engine, with the keywords "GRC" and "insurance" and also "ISO" and "insurance."

Secondly, a comparative study will be conducted between POJK as Indonesian insurance regulations, with ISO 37000, ISO 31000, and ISO 37301 as ISO standards for the GRC approach. The result will show the degree of fitness of POJK with these ISO standards.

RESULT AND FINDINGS

Comparative Study

A comparative study was conducted between POJK as Indonesian insurance regulations, with ISO 37000, ISO 31000, and ISO 37301 as ISO standards for the GRC approach. The result will show the degree of fitness of POJK with these ISO standards.

Some related POJK for Indonesian Insurance Regulations used for this comparative study are POJK NO. 73/POJK.05/2016 *Tentang Tata Kelola Perusahaan yang Baik bagi Perusahaan Perasuransian*, POJK NO.43/POJK.05/2019 *Tentang Perubahan Atas POJK NO.73/POJK.05/2016 Tentang Tata Kelola Perusahaan Yang Baik Bagi Perusahaan Perasuransian*, and POJK NO. 44/POJK.05/2020 *Tentang Penerapan Manajemen Risiko Bagi Lembaga Jasa Keuangan Nonbank*.

Related Indonesian Insurance Governance Regulation vs. ISO 37000: Governance of organizations - Guidance

POJK NO. 73/POJK.05/2016 is Indonesian Insurance Regulation related to ISO 37000: Governance of organizations. It regulates the structures and processes used and implemented by the organs of the Insurance Company. Insurance companies must apply the principles of Good Corporate Governance in every business activity at all levels or levels of the organization, as stated in this POJK. This study would compare whether it is in line with ISO 37000, which gives guidelines for the Governance of organizations.

Below is the result of the compatibility of POJK NO.73/POJK.05/2016 with ISO 37000.

	4. Context of this standard	5. The governing body	6. Framework	7. Principles of Governance
CHAPTER I Clause 1	0	0	0	0
CHAPTER II Clause 2-4	0	0	0	0
CHAPTER III Clause 5	0	0	0	0
CHAPTER IV Clause 6-18	0	0	0	0
Chapter V Clause 19-34	0	0	0	0
Chapter VI Clause 35-45	0	0	0	0
CHAPTER VII Clause 46-48	0	0	0	0
CHAPTER VIII Clause 49-54	0	0	0	0
CHAPTER IX Clause 55	-	-	-	0
CHAPTER X Clause 56-64	0	0	0	-
CHAPTER XI Clause 65	0	0	0	-
CHAPTER XII Clause 66-67	0	0	-	-
CHAPTER XIII Clause 68	0	-	-	-
CHAPTER XIV Clause 69-70	0	-	-	-
CHAPTER XV Clause 71-72	0	-	-	0
CHAPTER XVI Clause 73-75	-	-	-	0
CHAPTER XVII Clause 76-78	-	-	-	0

CHAPTER XVIII Clause 79	-	-	0	-
CHAPTER XIX Clause 80	-	-	-	-
CHAPTER XX Clause 81	-	-	-	-
CHAPTER XXI Clause 82	-	-	-	-
CHAPTER XXII Clause 83-86	-	-	-	-

Notes:

'0' refers to compatible

'-' refers to N/A

Based on the result above, we could conclude that almost all POJK clauses are in line with and can be mapped with clauses in ISO 37000. The clauses that are not mapped are clauses regarding violations or those relating to the provisions of other/previous POJK.

Related Indonesian Insurance Risk Management Regulation vs. ISO 31000: Risk Management - Guidelines

POJK NO. 44/POJK.05/2020 *Tentang Penerapan Manajemen Risiko Bagi Lembaga Jasa Keuangan Nonbank* relates to ISO 31000: Risk Management. The increasing business activities of non-bank financial services institutions with increasingly complex risks need to be balanced with the application of risk management, and the development of non-bank financial services institutions (including insurance companies) requires the application of adequate, effective, and measurable risk management.

Below is the result of the compatibility of POJK NO.73/POJK.05/2016 with ISO 37000.

	4. Principles	5. Framework	6. Process
CHAPTER I Clause 1-2	0	0	-
CHAPTER II Clause 3-5	0	0	0
CHAPTER III Clause 6-9	0	0	0
CHAPTER IV Clause 10-11	0	0	0
Chapter V Clause 12-14	0	0	0

Chapter VI Clause 15-17	0	0	0
CHAPTER VII Clause 18-21	0	0	0
CHAPTER VIII Clause 22-23	0	0	0
CHAPTER IX Clause 24-25	0	0	-
CHAPTER X Clause 26-27	-	-	-
CHAPTER XI Clause 27	-	-	-
CHAPTER XII Clause 29-30	-	-	-

Notes:

'0' refers to compatible

'-' refers to N/A

Based on the result above, we could conclude that almost all POJK clauses are in line with and can be mapped with clauses in ISO 31000:2018. The clauses that are not mapped are clauses regarding violations or those relating to the provisions of other/previous POJK.

Related Indonesian Insurance Compliance Regulation vs. ISO 37301: Compliance Management System- Guidelines

We could address no specific Indonesia Insurance Compliance Regulation to see the Compliance Management System in Insurance Company. In POJK NO.43/POJK.05/2019, we only find a regulation for Insurance companies to have their own Compliance Director. At the same time, we could find the process of managing compliance risk in POJK NO. 44/POJK.05/2020 *Tentang Penerapan Manajemen Risiko Bagi Lembaga Jasa Keuangan Nonbank*.

CONCLUSIONS

Since the organizations in Indonesia understand the importance of integrating GRC, this study confirms that regulatory requirements as set forth by FSA (Financial Services Authority) to Insurance Industry for integrated GRC have all been compatible with all the elements of ISO 37000, ISO 31000, and ISO 37301.

Limitations

For insurance companies who seemingly remain unsure regarding the method to integrate GRC in their organizations, the result of this paper could be used as generic inputs and considerations for insurance companies that have initiated their integrated GRC practices and/or just recently commenced and/or improving their practices more effectively.

Reccomendations

Whereas the study provides general understanding and assurance of the compatibility, it is not supported yet by empirical evidence of how insurance companies practically exercise the implementation of integrated GRC based on ISO series 37000, ISO 31000, and ISO 37301 and how do they conduct calibration efforts to its efficacy. Therefore, it is recommended to conduct such empirical case studies in several insurance companies in Indonesia as further study.

REFERENCES

- Alijoyo , F. Antonius & Fisabilillah, Al Fattaah M.S (2021). *Risk Management Implementation in Public Sector Organizations-Global Phenomena*. International Journal of Current Science Research and Review, Volume 04 Issue 03 March 2021.
- Almeida, R., Teixeira, J. M., Mira da Silva, M., & Faroleiro, P. (2019). A conceptual model for enterprise risk management. *Journal of Enterprise Information Management*, 32(5), 843–868. <https://doi.org/10.1108/JEIM-05-2018-0097>
- Choo, B. S.-Y., & Goh, J. C.-L. (2015). Pragmatic adaptation of the ISO 31000:2009 enterprise risk management framework in a high-tech organization using Six Sigma. *International Journal of Accounting & Information Management*, 23(4), 364–382. <https://doi.org/10.1108/IJAIM-12-2014-0079>
- Grant Thornton International (2009). Enterprise risk management: Creating value in a volatile economy. Retrieved from http://www.gtrus.ru/doc/public/gti/gti_erm_en.pdf
- International Organization for Standardization. (2018). *Risk management - Guidelines (ISO 31000:2018)*. International Organization for Standardization.
- International Organization for Standardization. (2021). Compliance Management System (ISO 37301:2021). International Organization for Standardization.
- International Organization for Standardization. (2021). Governance of organizations — Guidance (ISO 37300:2021). International Organization for Standardization.
- Kleffner, Anne & Lee, Ryan & McGannon, Bill. (2003). The Effect of Corporate Governance on the Use of Enterprise Risk Management: Evidence From Canada. *Risk Management and Insurance Review*. 6. 53 - 73. 10.1111/1098-1616.00020.
- Leitch, M. (2010). ISO 31000:2009 - The new international standard on risk management. *Risk Analysis*, 30(6), 887–892. <https://doi.org/10.1111/j.1539-6924.2010.01397>.
- Marek, Sebastian D. and Eling, Martin, Corporate Governance and Risk Taking: Evidence from the U.K. and German Insurance Markets (September 2014). *Journal of Risk and Insurance*, Vol. 81, Issue 3, pp. 653-682, 2014, Available at SSRN: <https://ssrn.com/abstract=2483539> or <http://dx.doi.org/10.1111/j.1539-6975.2012.01510.x>
- Mitchell, S.L. and Switzer, C.S. (2012). Measuring the Effectiveness and Performance of Your Governance, Operational Risk, and Compliance Programs. In *Governance, Risk, and Compliance Handbook*, A. Tarantino (Ed.).
- Open Compliance and Ethics Group (OCEG). (2008). OCEG Benchmarking Series Report: GRC measurement and metrics. Retrieved from www.oceg.org/.
- Pape, L., & Speklé, R. F. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review*, 23(11), 1–32. doi:10.1080/09638180.2012.661937

- Pernell, K., Jung, J., & Dobbin, F. (2017). The Hazards of Expert Control: Chief Risk Officers and Risky Derivatives. *American Sociological Review*, 82(3), 511-541. <https://doi.org/10.1177/0003122417701115>
- PricewaterhouseCoopers (PwC). (2004). 8th Annual Global CEO Survey. Retrieved from <http://www.globes.co.il/Serve/Researches/documents/8thAnnualGlobalCEOSurvey.pdf>.
- Purdy, G. (2010). ISO 31000:2009 - Setting a new standard for risk management. *Risk Analysis*, 30(6), 881-886. <https://doi.org/10.1111/j.1539-6924.2010.01442.x>
- POJK NO. 73/POJK.05/2016 Tentang Tata Kelola Perusahaan yang Baik bagi Perusahaan Perasuransian (Indonesia). Retrieved from <https://www.ojk.go.id/id/kanal/iknb/regulasi/asuransi/peraturan-ojk/Documents/Pages/POJK-tentang-Tata-Kelola-Perusahaan-yang-Baik-bagi-Perusahaan-Perasuransian/SAL%20-%20POJK%20Tata%20Kelola%20Asuransi%20-.pdf>
- POJK NO.43/POJK.05/2019 Tentang Perubahan Atas POJK NO.73/POJK.05/2016 Tentang Tata Kelola Perusahaan Yang Baik Bagi Perusahaan Perasuransian (Indonesia). Retrieved from <https://www.ojk.go.id/id/regulasi/Documents/Pages/Perubahan-Atas-Peraturan-Otoritas-Jasa-Kuangan-Nomor-73-tentang-Tata-Kelola-Perusahaan-yang-Baik-bagi-Perusah/pojk%2043-2019.pdf>
- POJK NO. 44/POJK.05/2020 Tentang Penerapan Manajemen Risiko Bagi Lembaga Jasa Keuangan Nonbank (Indonesia). Retrieved from <https://www.ojk.go.id/id/regulasi/Documents/Pages/Penerapan-Manajemen-Risiko-bagi-Lembaga-Jasa-Kuangan-Nonbank/pojk%2044-2020.pdf>
- Sheedy, Elizabeth A. and Griffin, Barbara, Risk Governance, Structures, Culture, and Behavior: A View from the Inside (January 2018). *Corporate Governance: An International Review*, Vol. 26, Issue 1, pp. 4-22, 2018, Available at SSRN: <https://ssrn.com/abstract=3100452> or <http://dx.doi.org/10.1111/corg.12200>
- The Institute of Internal Auditors (IIA). (2010). Governance, risk & control. Retrieved from <https://na.theiia.org/standards-guidance/topics/Pages/Governance-Risk-and-Control.aspx>.