Research Paper

Risk Control Self-Assessment: Identifying Risk at PT BRI Asuransi Indonesia

M. Agung Pramana*
BRI Asuransi Indonesia, Indonesia

Received: July 15, 2025	Revised : November 13, 2025	Accepted : march 25, 2026	Online : April 30, 2026

Abstract

Discussions on risk management have been extensive across various companies internationally. However, much of the existing research data is outdated, with most studies conducted several years ago. This article aims to update previous research on the implementation of risk management, focusing on PT BRI Asuransi Indonesia. The company has implemented Risk Control Self-Assessment (RCSA), a key tool for its risk management framework. This tool is utilized to identify and subsequently control risks within work units. This study updates previous scholarship that focused solely on operational risk, in contrast, this study emphasizes risk management tools that leverage digitalization to mitigate the risks faced by the Company. This paper primarily addresses how risk management, specifically the risk assessment process, is implemented at PT BRI Asuransi Indonesia. It also explores the broader development of risk management in an international context. This study employs a netnography method, sourcing data from online platforms combined with existing literature. The findings reveal that PT BRI Asuransi Indonesia has adapted its risk assessment process to modern times by digitalizing it. The entire process, from identifying and assessing risks to implementing controls, is conducted digitally. Furthermore, risk assessment reports are accessible through the BRINESIA RCSA website. The assessments are based on real-time data from Branch Offices, enhancing risk awareness at the local level. These findings support previous studies which suggest that a thorough implementation of RCSA leads to more effective operations and minimized risks within work units.

Keywords: *Company, Risk Identification, Risk Management Tools*

INTRODUCTION

The topic of risk management implementation is a compelling area of discussion as it directly pertains to a company's sustainability. At its core, risk is about uncertainty, which necessitates careful management. Risk Management is a systematic process of identifying, analyzing, evaluating, and mitigating specific risks that arise from business activities in the global market. The objective is not to eliminate all risks, which is impossible, but to manage them intelligently to protect assets, ensure profitability, and achieve strategic goals. Risk management is a systematic and integrated discipline crucial for the success of any organization. Its approach extends beyond mere loss prevention. With the appropriate framework, processes, and culture, risk management can assist an organization in not only protecting but also creating value (Hopkin, 2018). Ideally, business continuity will inherently involve risks. Therefore, a tool is needed to monitor and predict the risks a company might face. This is particularly vital for operational risk management, a critical component for any enterprise. The importance of this is underscored by numerous loss incidents involving public and private institutions in South Africa. The collapse of African Bank was attributed to operational risk factors, according to the Myburgh Commission's findings. The investigation revealed that the Chief Executive had disagreements with auditors and fellow directors over errors in reporting risks and impairments on non-performing loans, suggesting weaknesses in risk governance (Rensburg, 2016).

Corresponding author's email: agungpramana369@gmail.com

Another incident was the fall of VBS Mutual Bank in March 2018, where investigations showed that the chairman and others allegedly defrauded depositors by falsifying accounts, creating fictitious deposits, bribing officials, and transferring funds to themselves (Mkokeli & Bonorchis, 2018). Many such cases stem from a lack of adequate risk governance. A key aspect of effective risk governance and management is sufficient risk reporting. Risk management has evolved significantly as a discipline and a corporate function. However, its undisciplined application, coupled with regulatory weaknesses, was a major contributor to the 2007 financial crisis. A more diligent, transparent, and independent implementation of risk management is required.

Furthermore, Risk Control Self-Assessment is a significant application of risk management within a company. Literature on RCSA implementation is still relatively scarce; the author's search indicates that discussions on RCSA have been most active over the last decade. Therefore, this research serves to refresh the ideas on this phenomenon and to promote the implementation of risk management at PT BRI Asuransi Indonesia. RCSA is highly beneficial for minimizing fraud related to branch operations. If RCSA is genuinely implemented in the risk management process at the branch level, the operational effectiveness of the branch office will be enhanced (Akurugoda & Rajapaksha, 2021).

Regarding risk and its control, besides RCSA, there is also the Control Self-Assessment (CSA) method. This method is used for periodic analysis of risks and controls, followed by a series of action plans to improve risk management and internal controls. The emphasis of CSA is on decision-making through cooperation and participation between management and employees. CSA educates employees on analyzing and reporting risk controls, which helps to increase control awareness throughout the organization (Jacobus, 2015; Kincaid et al., 1999).

Turning to the subject of this research, PT. BRI Asuransi Indonesia, a subsidiary of Bank Rakyat Indonesia (BRI), operates in the general insurance sector. The company, hereinafter referred to as BRINS, has 23 branch offices across Indonesia and 23 divisions, each with its specific function. In terms of risk management implementation, BRINS has a Compliance and Risk Management division. This division is tasked with overseeing and managing existing risks in accordance with applicable regulations.

This research is compelling because, as various references have shown, risk management implementation is essential for any institution. Without a principle of prudence and vigilance towards risk, what happened to VBS Bank and other institutions that collapsed due to their inability to manage their own risks could occur. This study also aims to reinforce the findings of Akurugoda and Rajapaksha, who stated that risk management implementation is crucial, especially concerning RCSA, which can minimize fraud related to branch operations (Akurugoda & Rajapaksha, 2021).

Furthermore, this study addresses the scarcity of literature regarding the digitalization of risk management tools, particularly the risk assessment process. This discussion is presented as a novel contribution to this field, asserting the need to strengthen operational risk management tools to mitigate the challenges the Company will face moving forward.

This article focuses on the main question: How is risk management within the scope of academic literature, particularly the RCSA component, implemented at PT BRI Asuransi Indonesia? Additional questions explored by the author include the nature of RCSA in an international context and how PT BRI Asuransi Indonesia conducts digital RCSA assessments for its branch offices across Indonesia.

To answer these questions, the author has divided this article into four parts. The first part provides an introduction to the research topic. The second part describes RCSA within an international scope, which is then narrowed down to the context of PT BRI Asuransi Indonesia. Subsequently, the author will explore the implementation of digital RCSA at branch offices

throughout Indonesia. Finally, the article concludes with a summary of the findings.

LITERATURE REVIEW

Previous studies on risk management implementation in companies have been numerous, each with its own focus. In South Africa, for example, operational risk management has been critical since the early 1990s, with the practice growing rapidly due to increased regulatory requirements and risk-related incidents. The Municipal Finance Management Act 56 of 2003, for instance, mandates that institutions implement and maintain a transparent, efficient, and measurable risk management and control system. The fall of VBS Mutual Bank serves as a stark reminder of the consequences of inadequate operational risk management (Young, 2019). Operational risk is generally defined as the risk of loss resulting from operational failures, and it encompasses all other types of risks, including market, liquidity, and credit risks. In fact, if operational risks are effectively mitigated and failures are prevented, other risks are likely to be well-managed (Samad-Khan, 2008). Operational risk is defined as the risk of loss resulting from inadequate internal processes, people, and systems, or from external events. This definition includes legal risk (Pakhchanyan, 2016). In 2008, the financial crisis became an issue that caused the failure of a large number of banks and financial institutions. Hess (2011) observed that one of the main causes was the failure of financial institutions in 2008, and even now, is the lack of an operational risk management strategy (Hess, 2011). Cummins et al (2006) also cited the failure to manage operational risk in financial institutions with the example of the $1.3 billion loss suffered by Barings Bank. The loss was caused by one person, Nick Leeson, who assumed speculative positions until the bank was declared bankrupt in 1975 (Cummins et al., 2006).

Initially, the study of risk management began after 1955. At its inception, the discipline was closely linked to the use of insurance to protect individuals and companies from losses due to accidents. The primary focus was on pure risk, which is a risk that only has the potential for loss, not gain. In line with the research subject of an insurance company, risk management was also born with the establishment of insurance companies. When the insurance market was considered very expensive and incomplete in protecting against all pure risks, alternative forms of risk management began to emerge. These included self-insurance, where companies created liquid reserve funds to cover losses from accidents, and self-protection, which involved activities aimed at reducing the probability or impact of losses before they occurred, such as accident prevention. Additionally, captives and risk retention groups were formed, where companies established their own insurance subsidiaries (captives) or formed groups with similar companies to bear risks together.

The period of the Financial Revolution and Derivatives (1970s - 1980s) saw the use of derivatives (financial contracts whose value is derived from other assets) as risk management instruments, beginning in the 1970s and expanding rapidly in the 1980s. Initially limited to agricultural products, derivatives were then widely used to protect against financial risks such as fluctuations in interest rates, exchange rates, and commodity prices. During this period, financial risk management became an important complement to pure risk management for many companies. Financial institutions have intensively developed market risk and credit risk management.

The Modern Era of Governance and Regulation (1980s - early 2000s) marked the beginning of international risk regulation in the 1980s. Large investment banks started establishing risk management departments, and risk management became a concern for the board of directors. The concept of integrated risk management was introduced, and the position of Chief Risk Officer (CRO) began to be created to oversee all of the company's risks (Dionne, 2013). According to Berg, risk management is important because it involves integrated activities that include the recognition, assessment, strategy development, and mitigation of risks using managerial resources. The goal is to reduce various types of threats to an acceptable level (Berg, 2010).

As is known, the application of risk management is crucial for companies or institutions to achieve their objectives. This is reflected in the increase in financial scandals and corporate crises due to uncontrolled risks in the 1990s. To address this, COSO (Committee of Sponsoring Organizations of the Treadway Commission) was formed as a committee to deal with risk management, internal control, and good corporate governance. In this context, operational risk is an important part of the risk management framework that must be managed to minimize the causes of operational losses (Bajaj, 2021). Risk management is not just about compliance or control, but about improving the quality of decision-making under conditions of uncertainty. Effective risk management should be part of a focus on rationally balancing all risks and returns (East, 2022).

According to Padganech (2010), operational risk has long existed in financial institutions. However, the emergence of globalization and new regulations for financial institutions, along with technological advancements and the development of a global financial outlook, have forced financial institutions to pay more attention to operational risk. Operational risk arises from the people in charge, the prevailing financial systems, the implemented financial processes, or other external events that can affect the financial institution. Risks originating from responsible individuals can come from management failures and human resources. When examining how processes operate, breakdowns can result from violations of stable operations or a failure to strictly follow procedures. System risks can include technical failures and other internal issues. Finally, external events can include vandalism, theft, and market failures. Nystrom also revealed that a key component of operational risk management is identifying the risks that a financial institution will face in the future (Nyström & Skoglund, 2002). Therefore, a tool is needed to identify the risks within our financial institutions. In this regard, the author focuses the discussion on Risk Control Self-Assessment (RCSA) at PT BRI Asuransi Indonesia. The success of operational risk management does not depend on a single solution, but on an integrated system that includes eight factors: strong leadership, clear policies, thorough planning, relevant processes, proper implementation, continuous training, fair performance assessment, and most importantly, a risk-aware culture must be embedded throughout the organization (Gakpo, 2021).

There are several tools in risk management, such as Control Self-Assessment, which focuses on employee controls, and the Loss Event Database, which is a record of all losses faced by the company, whether from legal issues, fraud, fines, or IT disruptions. Furthermore, there is Risk Control Self-Assessment (RCSA), which is a step of risk identification accompanied by controls as an effort to minimize future risks. This is necessary for the implementation of risk management as it is a key component and requires effective risk management within the company with good corporate governance. RCSA is a structured process that allows an organization to proactively identify, analyze, and manage operational risks and evaluate the effectiveness of existing internal controls. When companies adopt sophisticated risk management practices and have an effective and sound management strategy, it increases their chances of long-term survival. It should be noted that the risk management process must be fully understood by the board of directors and all other employees for meaningful change to be realized (Aebi et al., 2012).

For example, Yang (2017) studied CREDIT Bank, one of Taiwan's largest commercial banks, noting that the bank established an operational risk management department and began implementing Risk Control Self-Assessment (RCSA) procedures. This tool is designed for companies to collect, identify, and assess operational risks embedded within their business processes (Yang et al., 2017).

This study is anchored in ISO 31000, which details the risk management framework and the collection of tools utilized to execute the assessment phase of the process. This standard provides the principles and guidelines for managing all forms of risk in a systematic, transparent, and reliable manner. It is generic in nature, meaning it can be applied across an entire organization or to specific

functions, activities, and projects. A core component within this framework is risk identification (De Oliveira et al., 2017). This, therefore, aligns with the present study, which explains the digitalization of risk management tools, especially concerning the risk assessment process.

RESEARCH METHOD

This study utilizes a qualitative method with a descriptive approach. The qualitative method is employed to explore the implementation of risk management, with a particular focus on RCSA as a tool to minimize risks that could impact the company, in this case, PT BRI Asuransi Indonesia. According to Creswell, the qualitative method is a research approach aimed at exploring and understanding social reality (Creswell et al., 2007). In the context of this study, social reality also encompasses the social reality in the digital space.

The data collection technique used is netnography. Netnography involves research that uses digital data to understand phenomena occurring in the digital realm (Kozinets, 2019). The digital data for this research is focused on the digitized BRINESIA web platform of PT BRI Asuransi Indonesia. Data selection was conducted using purposive sampling. To this end, data from 23 branch offices were analyzed to isolate the most specific risk assessment process data relevant to this research topic. The researcher identified this data by examining the inputs submitted by each branch office, which will be detailed subsequently in the results and discussion. The selection was guided by specific criteria, such as the most recent Risk Control Self-Assessment (RCSA) data from all branch offices. This method was chosen to observe the practical implementation of risk management, particularly RCSA, at PT BRI Asuransi Indonesia. In addition to obtaining digital data from the BRINESIA website, the author also documented research data using screenshots.

This serves as a form of applying online research ethics. Additional data for validation was also obtained from representatives of the Branch Offices regarding the implementation of risk management at their respective locations.

The collected data were then analyzed using content analysis. The stages of analysis adopted the concepts of Miles and Huberman as follows: First, data reduction. At this stage, the author collected and selected data relevant to the research. Second, data display. Here, the author presented the data in the form of statements, images, and other formats. Third, concluding. In this final stage, the author summarized the research findings that answered the research questions (Miles & Huberman, 1994).

FINDINGS AND DISCUSSION

Risk Control Self-Assessment: Risk Management and PT BRI Asuransi Indonesia

In a dynamic and uncertain global business landscape, companies are faced with increasingly complex risks, ranging from regulatory changes in various countries to cyber threats and more. To navigate these challenges, companies require a proactive risk management tool. This is where Risk Control Self-Assessment (RCSA) plays a crucial role as a strategic framework for identifying, evaluating, and managing risks across all business activities. Its main objective is to instill a risk-aware culture at all levels of the organization or institution, ensuring that every work unit understands its role in managing risks relevant to their work.

For instance, in Malaysia, Islamic banks use this tool to identify risks, which is useful for pinpointing potential breaches of Shariah parameters in the end-to-end processes of each function. Thus, the responsibility for identifying and assessing Shariah non-compliance risk is borne by each respective risk owner, in this case, the work unit (Ariffin, 2022). In other words, RCSA helps in risk identification and records all operational risks in the business, looking at inherent risks and what controls are in place so that residual risk can be reduced to a tolerable limit (Kumar, 2022). A well-designed and implemented RCSA can help embed operational risk management throughout the

organization, improve management's attitude towards operational risk management, and enhance the overall risk culture. An effective RCSA can also support an organization's governance and compliance activities. It can also support the work of internal and external auditors, helping them prioritize audit attention and structure audit reports (Ashby, 2022). RCSA is expected to be based on situational analysis to identify and assess current or future threats and vulnerabilities, and also to evaluate current controls and/or suggest modifications to effectively minimize risks (Butler & Brooks, 2024).

Turning to the company that is the subject of this research, PT BRI Asuransi Indonesia is a subsidiary of PT Bank Rakyat Indonesia engaged in the insurance sector. Currently, PT BRI Asuransi Indonesia has 21 branch offices spread across Indonesia. The company also has 23 divisions at its head office, each focusing on its respective area. Regarding the topic of discussion, the implementation of risk management has also been carried out in this company. The division that oversees and regulates the implementation of risk management at PT BRI Asuransi Indonesia is the Compliance and Risk Management division. The risk management in this company focuses on Risk Control Self-Assessment, Branch Office Risk Profiles, Loss Event Database, and others. However, the author focuses on Risk Control Self-Assessment. Risk assessment is conducted to predict the profile of the work unit in the future. The initial stage involves identifying the risks present in the work unit, after which controls are implemented for these risks so that the company's objectives can be achieved. It can also minimize fraud that occurs in the work unit (Akurugoda & Rajapaksha, 2021). RCSA is a key component of a robust operational risk management framework. This process provides a better understanding of business risks, helps identify high-risk areas, and provides an operational overview to management and the board of directors (Tattam, 2017).

In the international sphere, studies on Risk Assessment have been discussed by scholars. However, from the author's search, references to RCSA were only found from the 2010s. This is what makes this research present as an update on Risk Assessment risk management, and the author wants to explore more deeply the workings of PT BRI Asuransi Indonesia. RCSA has become more than just a best practice; it is used as a strategic necessity. Here are some of the reasons, First, the diversity of operational risks. Each country has a unique risk landscape, including cultural, legal, political, and economic differences. Risk Assessment allows branch offices in different countries to identify specific risks relevant to their environmental context, which may not be visible from the head office. Second, it increases accountability. By involving teams that understand their own work unit's environment directly in the risk identification and assessment process, RCSA fosters a sense of ownership and accountability. Branch leaders are no longer just implementers of policies from the central office but become active risk-aware individuals in their regions. Basically, the people who best understand a risk are those who do the work in that work unit (Mehra, 2010). Malaysian Islamic banks, for example, use RCSA as one of the processes where Shariah non-compliance events can be discovered through risk identification, in addition to through Shariah reviews or internal/external audits. Risk Assessment is used as a detection mechanism (Embi & Shafii, 2018). RCSA has become a powerful tool for management to manage its organization's risks proactively and systematically from within.

In the Indonesian context, the implementation of RCSA cannot be separated from the role of regulators. The main drivers include: First, the Financial Services Authority (OJK). For the financial services industry (banking, insurance, capital markets), the OJK explicitly requires the implementation of effective risk management. OJK Regulations (POJK), such as the POJK on the Implementation of Risk Management for Commercial Banks, mandate that banks have adequate risk identification, measurement, monitoring, and control processes. RCSA becomes a key implementation tool to meet the standards for operational risk. Second, the Ministry of State-Owned Enterprises (BUMN). The Ministry of BUMN consistently encourages the improvement of

Good Corporate Governance (GCG) quality within BUMNs. The application of risk management based on international frameworks such as ISO 31000 has become one of its main pillars, where RCSA is one of the most commonly used methods for assessing risks at the operational level. Lastly, GCG Principles. The demands for transparency and accountability from investors and other stakeholders encourage companies to adopt a strong internal control framework like COSO (Committee of Sponsoring Organizations of the Treadway Commission), which inherently supports the RCSA methodology.

Risk Control Self-Assessment: Digitization of Risk Management Tools at PT BRI Asuransi Indonesia

At PT BRI Asuransi Indonesia, the implementation of RCSA has been systemically designed. The workflow involves each work unit conducting its own assessment of the risks within its area. This is followed by a review from the Compliance and Risk Management division, and the results are then reported to management. The author focuses on the RCSA assessment at the 21 Branch Offices. The RCSA assessment is carried out by a "Risk Champion" (a term for an employee tasked with overseeing risk in a work unit) who is selected based on applicable provisions. First, the Risk Champion must log into their account on the Branch Office link on the BRINESIA website (https://cabang.web.brinesia.app/), a platform that supports the operational activities of PT BRI Asuransi Indonesia.

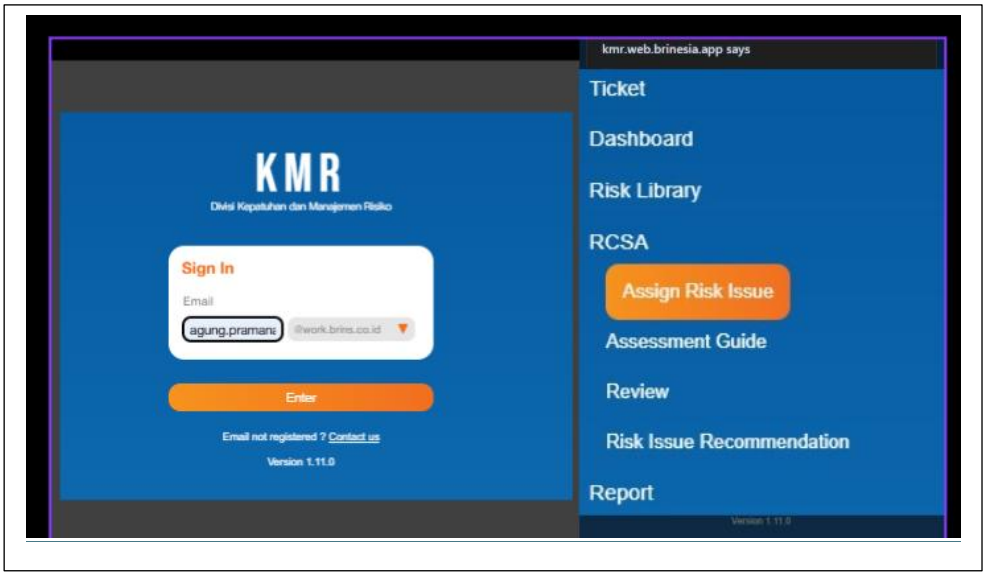

Figure 1. RCSA Work Unit Dashboard Display
Source: Author's Research

A sidebar menu is visible with options like Ticket, Dashboard, Risk Library, RCSA (with sub-options Assign Risk Issue, Assessment Guide, Review, Risk Issue Recommendation), and Report.] After logging in, a token code is sent to the Risk Champion's email, which they use to access the RCSA dashboard. The dashboard appears as shown below.

Next, by clicking the "assessment" menu, a list of "risk issues" will appear for each branch office to evaluate. The assessment consists of "inherent risk," "control," and "residual risk". Inherent risk includes "impact," "likelihood," and "severity". The residual risk score has similar components but differs in function. The Inherent Risk Score (IRS) assesses the inherent risk; the IRS impact measures the magnitude of the impact if the risk were to occur in the work unit, based on parameters mandated in the RCSA guidelines of PT BRI Asuransi Indonesia. "Likelihood" refers to

the frequency of the event, or how often the risk occurs in the work unit. This then calculates the "severity". Following this, a list of controls is presented for the Risk Champion to complete.

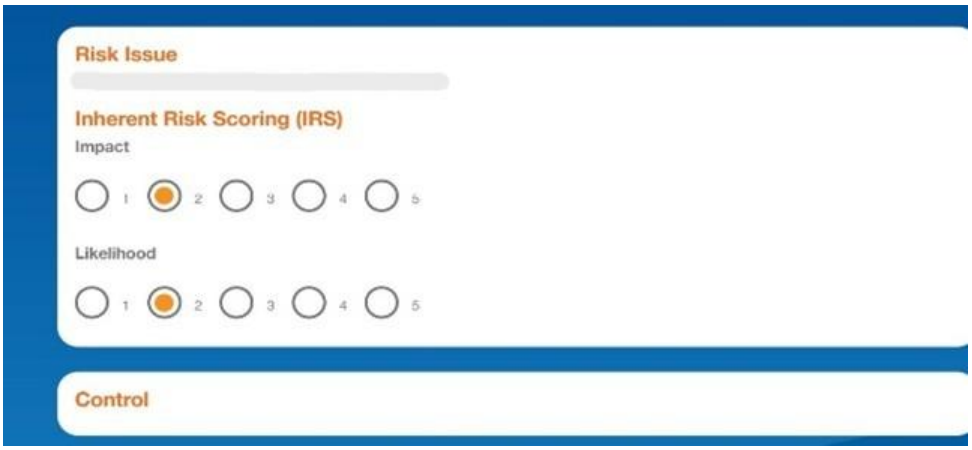

Figure 3. IRS and Control Assessment on the BRINESIA Web
Source: Author's Research

Once the controls for the issue have been filled in, a composite control score is calculated from the list of controls. This then generates the Residual Risk Score (RRS), which also includes RRS impact, likelihood, and severity. These are derived from the IRS impact and the composite control score, and the IRS likelihood and the composite control score, respectively. The assessment is based on a heatmap defined in the general risk policy guidelines.

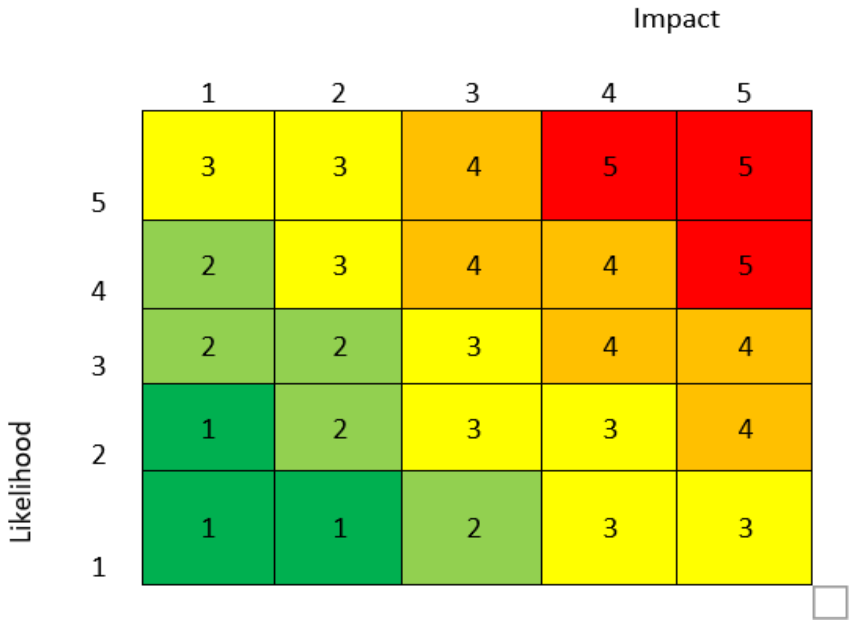

Figure 4. Risk Assessment Heatmap
Source: Author's Research

Figure 5. RRS RCSA Digital Calculation
Source: Author's Research

Continuing the process, after the Risk Champion (RC) completes the assessment, it moves to the approval stage by the head of the branch office work unit. Similar to the RC, the branch office head must also log in to the BRINESIA RCSA website to confirm their approval of the RCSA assessment conducted by the RC. In the system, the branch office head navigates to the approval menu and clicks the approval button located below the risk issue. Subsequently, the RCSA assessment results are sent to the RCSA dashboard of the Compliance and Risk Management division for review.

During the review process, the Compliance and Risk Management division of PT BRI Asuransi Indonesia examines data from previous assessment periods, checks whether the action plans from the previous period have been implemented, and also uses the branch office audit reports from the Internal Audit division as a reference. These two divisions coordinate on the RCSA assessment of the Branch Offices. If there is a discrepancy between the RC's assessment results and the audit findings, the Compliance and Risk Management division has the right to reject the branch office's RCSA assessment and request a revision. This aligns with Akurugoda and Rajapaksha, who stated that if RCSA assessment is properly implemented in the risk management process at branch offices, their operations will run effectively (Akurugoda & Rajapaksha, 2021). This also corresponds with Cristea's opinion, whose conceptual framework outlines four main stages in the operational risk management process: identification, analysis, mitigation, and monitoring of risks (Cristea, 2021). All these processes are implemented in the online RCSA system of PT BRI Asuransi Indonesia.

This study is fundamentally anchored in the ISO 31000 standard, which furnishes the principles and guidelines for managing all forms of risk in a systematic, transparent, and reliable manner. This standard is generic in nature, signifying its applicability across an entire organization or for specific functions, activities, and projects. In this context, the Company's risk identification and assessment process is predicated upon the ISO literature (De Oliveira et al., 2017). This research extends the existing body of literature, which has predominantly focused on conventional risk assessment processes within the Company's industry and has scarcely addressed the concept of risk assessment digitalization. It provides further analysis of the assessment process that has been digitalized by PT BRI Asuransi Indonesia. The objective is to minimize risk and observe how the Company identifies the challenges it confronts in the contemporary era, utilizing the aforementioned assessment methodologies.

CONCLUSIONS

Currently, risk management has become a significant topic of discussion for safeguarding and achieving corporate goals. The optimal implementation of risk management yields a positive impact on a company. Conversely, as seen with VBS Bank and Barings Bank in Africa, failure to manage risks can lead to corporate collapse. This study serves as an update to previous research on risk management implementation. Whereas previous research focused solely on the risk management process, this study contributes to the academic literature by incorporating ISO 31000 and examining the digitalization of risk management tools for risk identification, specifically the Risk Control Self-Assessment (RCSA). The author observes that PT BRI Asuransi Indonesia has implemented risk management in accordance with prevailing standards and regulations. Focusing on RCSA, one of the risk management tools utilized at PT BRI Asuransi Indonesia, the author aims to showcase its digitized implementation within the company's branch offices. This study also reinforces the findings of Akurugoda and Rajapaksha, who argued that the effective implementation of RCSA at the branch office level facilitates operational efficiency. Based on this conclusion, this research recommends that future studies on corporate risk management, particularly within the Indonesian context, be conducted more extensively. This will help generate and develop innovative and constructive ideas regarding the implementation of risk management within companies. Furthermore, it would allow for an examination of other perspectives on risk management implementation in different companies, including the specific tools they use and their methods of application. This would foster a more engaging discourse on corporate risk management implementation in Indonesia. The author's search indicates that most discussions on risk management are from several years ago, rendering them less relevant today, especially given the massive advancements in digitalization.

LIMITATION AND FURTHER RESEARCH

This study is limited by its single-case focus on PT BRI Asuransi Indonesia, restricting generalizability across industries and regions. The use of netnography and internal digital data may also limit data depth and objectivity. Future research should adopt comparative multi-company approaches, incorporate quantitative methods, and explore the effectiveness of digital RCSA across sectors. Further studies could also examine user behavior, system integration, and long-term impacts of digital risk management implementation.

REFERENCES

Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance, 36*(12), 3213–3226.

Akurugoda, N. S., & Rajapaksha, U. G. (2021). Studying the issues faced in commercial bank branch operational related fraud management. http://192.248.104.6/handle/345/5123

Ariffin, N. M. (2022). Shariah risk management practices in Malaysian Islamic banks. *International Journal of Economics, Management and Accounting, 30*(1), 101–123.

Ashby, S. (2022). *Fundamentals of operational risk management: Understanding and implementing effective tools, policies and frameworks*. Kogan Page.

Bajaj, R. V. (2021). Operational risk management. *India Banking and Finance Report*, 77.

Berg, H.-P. (2010). Risk management: Procedures, methods and experiences. *Reliability: Theory & Applications, 5*(2), 79–95.

Butler, T., & Brooks, R. (2024). Time for a paradigm change: Problems with the financial industry's approach to operational risk. *Risk Analysis, 44*(6), 1285–1304. https://doi.org/10.1111/risa.14240

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative research designs:

Selection and implementation. *The Counseling Psychologist, 35*(2), 236–264. https://doi.org/10.1177/0011000006287390

Cristea, M.-A. (2021). Operational risk management in banking activity. *Journal of Eastern Europe Research in Business and Economics*, 969612, 1–16.

Cummins, J. D., Lewis, C. M., & Wei, R. (2006). The market value impact of operational loss events for US banks and insurers. *Journal of Banking & Finance, 30*(10), 2605–2634.

De Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production, 151*, 616–633.

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review, 16*(2), 147–166. https://doi.org/10.1111/rmir.12016

East, T. (2022). Operational risk management. In *Routledge handbook of risk management and the law* (pp. 5–18). Routledge. https://doi.org/10.4324/9781351107242-3

Embi, S., & Shafii, Z. (2018). The impact of Shariah governance and corporate governance on risk management practices: Evidence from local and foreign Islamic banks in Malaysia. *Journal of Muamalat and Islamic Finance Research*, 1–20.

Gakpo, M. D. Y. (2021). Operational risk management systems implementation in Ghanaian banks: The critical success factors. *International Journal of Sciences: Basic and Applied Research (IJSBAR), 55*, 59–70.

Hess, C. (2011). The impact of the financial crisis on operational risk in the financial services industry: Empirical evidence. *The Journal of Operational Risk, 6*(1), 23–?.

Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. Kogan Page.

Jacobus, D. (2015). New paradigm of managing risks: Risk and control self-assessment. *Agriculture and Agricultural Science Procedia, 3*, 32–34.

Kincaid, J. K., Sampias, W. J., & Marcella, A. J. (1999). *Certification in control self-assessment*. Institute of Internal Auditors.

Kozinets, R. (2019). *Netnography: The essential guide to qualitative social media research*. Sage.

Kumar, S. (2022). Introduction to risk management. SSRN. https://doi.org/10.2139/ssrn.4123419

Mehra, Y. S. (2010). Operational risk management in Indian banks: Evaluation of applicability of the RCSA method under advanced measurement approach. *Indian Journal of Finance, 4*(11), 3–13.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Mkokeli, S., & Bonorchis, R. (2018, July 30). Ponzi scheme at small South African bank becomes biggest heist. *Bloomberg*. https://www.bloomberg.com/news/articles/2018-07-30/-ponzi-scheme-at-small-south-african-bank-becomes-biggest-heist

Nyström, K., & Skoglund, J. (2002). Quantitative operational risk management. Swedenbank, Group Financial Risk Control. https://www.ime.usp.br/~rvicente/risco/nystrom.pdf

Pakhchanyan, S. (2016). Operational risk management in financial institutions: A literature review. *International Journal of Financial Studies, 4*(4), 20.

Rensburg, R. (2016, May 13). Damning report strengthens the cases of those suing African Bank. *News24*. https://www.news24.com/citypress/business/damning-report-strengthens-the-cases-of-those-suing-african-bank-20160513

Samad-Khan, A. (2008). Modern operational risk management. *Emphasis, 2*, 26–29.

Tattam, D. (2017). *A short guide to operational risk*. Routledge.

Yang, S. O., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling effective operational risk management in a financial institution: An action research study. *Journal of Management Information Systems, 34*(3), 727–753. https://doi.org/10.1080/07421222.2017.1373006

Young, J. (2019). Value-adding activities of operational risk management methodologies.

Administratio Publica, 27(4), 110–133.