Analysis of GRC System Implementation in Supporting Application in IT Division

Achmad Hidayatno[1], Sukiswo[2], Karnoto[3]

[1,2,3] *Lecturer, Department of Electrical Engineering, Diponegoro University, Central Java, Indonesia*

ABSTRACT

PT. PLN is the largest electricity company in Indonesia, and they need hardware and software to manage their operations internally and externally. They have implemented a framework called the GRC system, which stands for Governance, Risk Management, and Compliance. This system ensures the company's business operations are practical and efficient by considering governance, risk, and compliance. The GRC system involves everyone, from top-level management to regular employees, by implementing the GRC system, PT. PLN aims to improve its operational performance, reduce potential risks, analyze the impact of these risks, and enhance its reputation among stakeholders. However, it is essential for the company to continually assess and improve the GRC system to achieve optimal results. In this report, the author specifically focuses on implementing the GRC system at PT. PLN, with a particular emphasis on the observation method used by the Information Technology Division's software development team. The author will provide an analysis to improve the existing GRC system in the company.

Keywords: *GRC, Governance, Risk, Compliance, Software, Business Development*

1. INTRODUCTION

The development of a company's work system is a necessary obligation to improve effectiveness and efficiency. The development of the company's work system is not only focused on efficiency and energy but also on enhancing data security and fostering trustworthy and honest employees. Implementing the GRC system in the company can overcome resource limitations and the complexity of the company's information system. The GRC system is often implemented to solve these constraints and enhance the company's data exchange quality. In the implementation of GRC, the company evaluates risk and compliance assessments, identifies company needs, and designs accordingly. The GRC system is crucial in ensuring the quality of the company's work system. Implementing the GRC system requires integrating two or more work systems to minimize expenses for application development and maintenance, leading to efficient utilization of company funds. After implementing the GRC system, the results include risk reduction in various company areas, improved employee compliance, and overall business performance enhancement.

In this research report, the author limits the scope to provide a general description of the implementation process of the GRC system in the development of information systems for supporting company applications, as well as the application of the GRC system in software development. The analysis includes the implementation of the GRC system in 9 supporting applications and the study of integrating these applications to enhance work efficiency in the company.

2. THEORETICAL FOUNDATION

2.1 Governance, Risk, and Compliance (GRC)

In Indonesian, governance, Risk, and Compliance (GRC) translates to Compliance, Risk, and Governance. This approach refers to an integrated approach to managing corporate governance, risk management, and compliance requirements that all company employees must adhere to. Implementing a GRC system is to strengthen the company's governance following applicable standards and regulations. Specific goals of implementing a GRC system include:

1. Enhancing compliance: The GRC system helps employees understand and comply with company policies and regulations.
2. Managing risks: The GRC system assists in identifying, measuring, and managing risks that can impact the company's operations, helping prevent losses and enhance security.
3. Strengthening governance: The GRC system reinforces the company's governance by implementing effective processes and controls to manage operations and maintain integrity.
4. Increasing transparency: The GRC system provides better visibility into company activities and processes, enhancing transparency and accountability.
5. Enhancing company reputation: By adhering to standards and regulations and effectively managing risks, the company can strengthen its reputation among stakeholders and the general public.
6. Optimizing operational performance: Implementing a GRC system helps improve the efficiency and effectiveness of the company's operations by identifying areas for improvement and optimizing workflow processes.
7. Ensuring business sustainability: The company can minimize potential operational disruptions and maintain business sustainability by effectively managing risks and ensuring compliance with regulations.

Governance pertains to how an organization is structured and operated. It encompasses policies, procedures, organizational structure, corporate governance, ethics, and organizational culture. Good governance can help an organization achieve its strategic goals, minimize risks, enhance compliance, and maintain its reputation. Critical aspects of government include leadership, policies and procedures, organizational structure, corporate management, ethics, and legal compliance.

Compliance or adherence refers to observing or fulfilling legal regulations, standards, and policies within organizational activities. The purpose of compliance in GRC (Governance, Risk, and Compliance) is to ensure that the organization complies with applicable rules and standards while maintaining its reputation. Critical compliance includes identifying legislation, policy establishment, employee training, supervision, and enforcement. Fig -1 shows the GRC work description form.

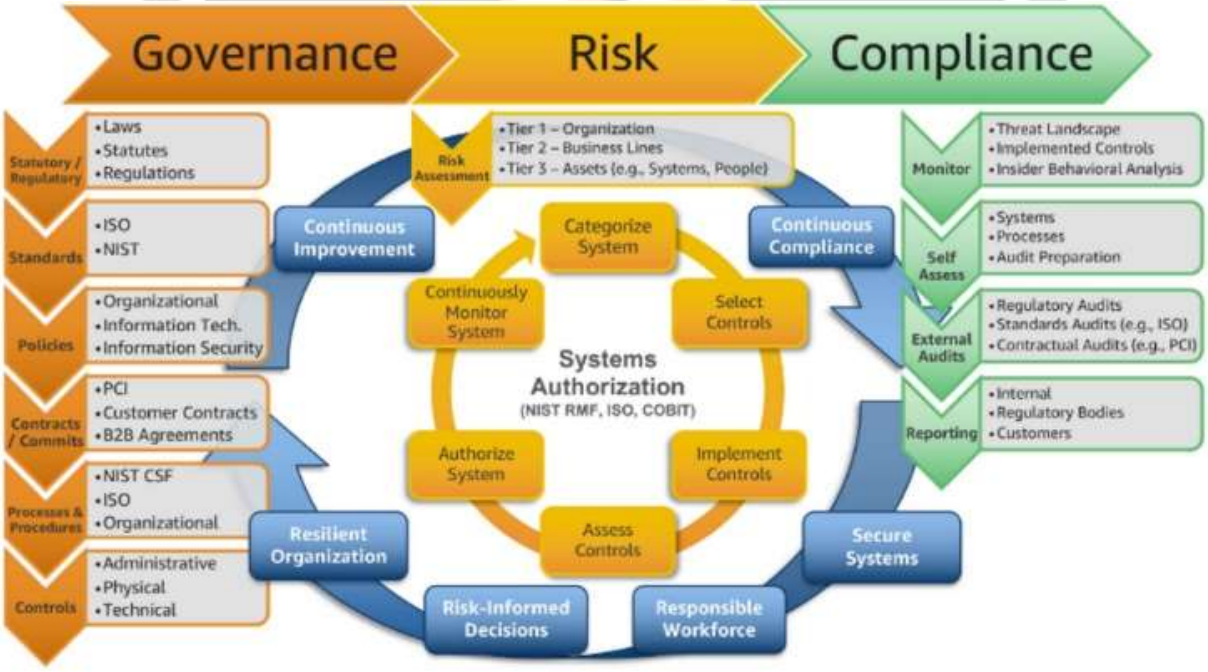

Fig -1 GRC Work Description Form

The GRC Capability Model is a framework used to assess an organization's ability to implement GRC systems. This model typically consists of stages and assessment criteria used to measure an organization's capability in understanding, managing, and controlling risks and complying with internal and external regulations and policies. There are two commonly used GRC Capability Models in a company.

The CMMI, or Capability Maturity Model Integration, is a capability model used to assess an organization's ability to understand and manage risks, comply with regulations and policies, and improve the quality of its GRC systems. This model consists of five levels of capability:

1. Initial: Organizations at this level have little or no control over their GRC processes. Processes are often undocumented, inconsistent, and based on individual experience and expertise.
2. Managed: Organizations at this level begin to manage their GRC processes systematically. GRC processes are documented, and relevant risks and policies are better understood.
3. Defined: Organizations at this level have well-defined and well-documented GRC processes. They follow standard procedures, and performance measurements are in place to ensure compliance with the standards.
4. Quantitatively Managed: Organizations at this level regularly measure and analyze the performance of their GRC processes. They understand the relationship between risks and business performance and use data to make better decisions.
5. Optimizing: Organizations can adapt and improve their processes according to changes in the business and technological environment.

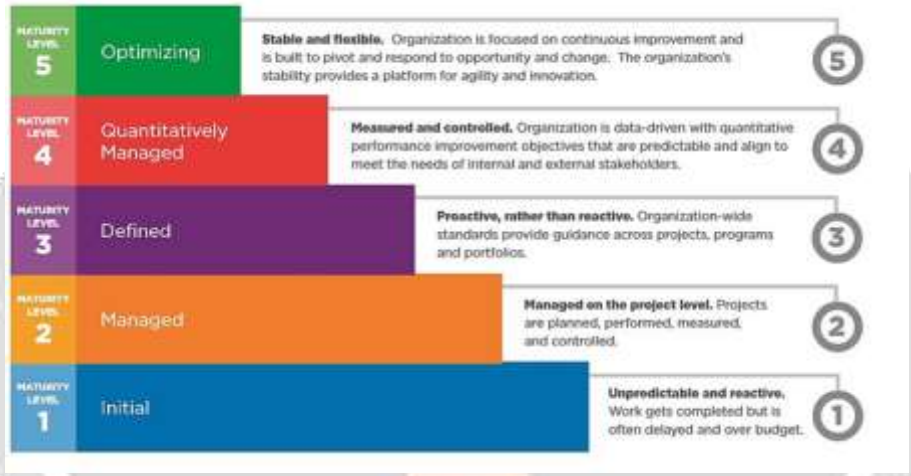

Fig -2 CMMI Capability Model

In the CMMI model in Fig -2, organizations are expected to progressively advance to higher levels and continuously enhance their GRC processes. This model offers explicit guidance on gradually improving the GRC process and assesses an organization's capability to manage risk and adhere to regulations effectively.

The OCEG, or Open Compliance and Ethics Group, is a global organization focused on best practices in corporate risk management, compliance, and ethics. OCEG also develops GRC capability models to assist organizations in enhancing their GRC programs' effectiveness.

Organizations must go through five primary stages to achieve better GRC capability. The four stages are as follows:

1. Learn The first stage, "Learn," involves understanding the organization's GRC needs and learning about best practices in the relevant industry. It entails comprehending applicable regulations and standards and learning from experiences in managing risk, ensuring compliance, and optimizing governance.

2. Align: The second stage is "Align," which entails ensuring that the organization's GRC practices align with its strategic objectives. This stage involves developing an integrated GRC strategy aligning with the organization's business strategy and GRC goals with business objectives.

3. Perform: The third stage is "Perform," which involves implementing effective GRC practices within the organization.

4. Review: The fourth stage is "Review," which involves periodically evaluating the organization's GRC performance and addressing identified issues.

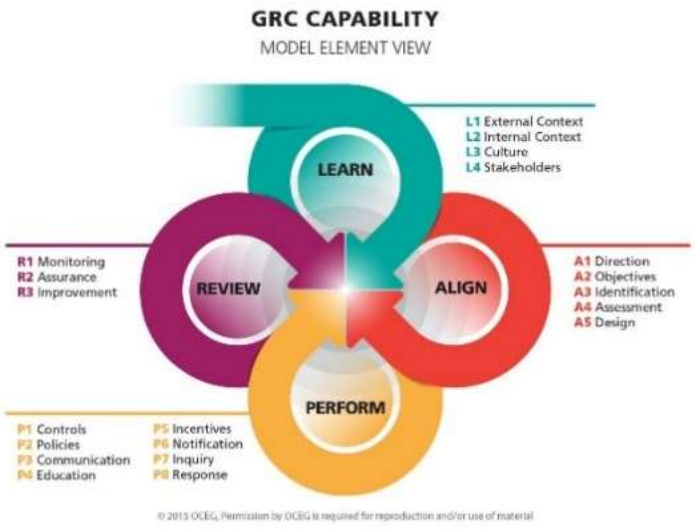

Fig -3 CMMI Capability Model

By continuously following the Learn-Align-Perform-Review cycle in Fig -3, organizations can improve their GRC capabilities incrementally and ensure that their GRC practices are always practical and in line with business and regulatory requirements.

Best Practices in GRC are proven practices aimed at helping organizations achieve their GRC goals more effectively and efficiently. These practices are typically based on industry best experiences and applicable regulatory standards. Best Practices have been proven effective in managing risks, ensuring compliance, and enhancing organizational governance. Best Practices in GRC systems are usually developed based on the experiences of relevant organizations, industry standards, and applicable regulations. Here are five Best Practices for successful GRC programs:

1. Engaging Stakeholders: Involving stakeholders such as the board of directors, senior management, and employees is critical to the success of a GRC program.
2. Establishing a Structured Framework: Creating a structured framework helps organizations effectively manage risks, ensure compliance, and enhance governance.
3. Setting Performance Measurement and Reporting: Establishing clear and measurable performance metrics and reporting is crucial in measuring the success of a GRC program.
4. Conducting Continuous Evaluation and Improvement: Ongoing and continuous improvement are essential in ensuring the success of a GRC program.
5. Using Appropriate Technology: GRC technologies such as risk management platforms, compliance management systems, and governance enhancement tools can assist organizations in improving the effectiveness and efficiency of managing risks, ensuring compliance, and enhancing governance.

The COSO Framework (Committee of Sponsoring Organizations of the Treadway Commission) is a widely recognized internal control and enterprise risk management framework. The COSO Framework provides a comprehensive approach that helps organizations effectively manage risks, achieve their objectives, and enhance overall governance. This framework consists of five interconnected components.

1. Control Environment: A robust control environment includes ethics, values, organizational culture, structure, responsibility, and commitment to compliance.
2. Risk Assessment: This component involves identifying, analyzing, and assessing risks. By understanding the existing threats, organizations can develop appropriate risk management strategies.
3. Control Activities: This component involves implementing appropriate control measures to manage identified risks.
4. Information and Communication: This component involves collecting, processing, and distributing relevant information for effective decision-making.

5. Monitoring: This component involves continuous monitoring of the effectiveness of the internal control system.

The COSO Framework is suitable for explaining a company's GRC (Governance, Risk Management, and Compliance) system because it comprehensively covers the essential aspects of risk management and internal control. This framework ensures that governance, risk management, and compliance are well-integrated into business operations. The COSO Framework helps companies build effective internal control systems, identify risks that may occur in their operations, manage those risks appropriately, and ensure compliance with regulations and policies for every employee.

The COSO Framework provides clear and structured guidance for companies implementing GRC systems. By following this framework, companies can identify relevant risks, develop effective control strategies, and ensure compliance with regulations and policies. Additionally, the COSO Framework helps companies build a robust control environment and create an organizational culture that prioritizes integrity and business ethics. With a robust control environment, companies can ensure that every individual in the organization understands the importance of internal control and is committed to implementing it.

The COSO Framework also guides effective monitoring of the internal control system. Ongoing monitoring and periodic evaluation help companies identify weaknesses in their GRC systems and make necessary improvements.

Companies can integrate governance, risk management, and compliance comprehensively into their business operations using the COSO Framework. This integration helps companies achieve strategic objectives, reduce potential risks, and build a strong reputation in the eyes of stakeholders. Continuous evaluation and improvement of the GRC system are also necessary for companies to continually enhance the effectiveness and efficiency of their internal controls. Fig -4 shows the dimension of the COSO Framework.

Fig -4 COSO Framework

3. METHODOLOGY

The PT. PLN Central Office already has several active supporting applications in place. With nine supporting applications running, it is expected to implement an application with a GRC system—these nine functional supporting applications at the PT. PLN Central Office is already part of the GRC system, with each application having its role in Governance, Risk, and Compliance.

Four applications operate in the Governance field: INSPEKTA, GA SERVICES, EPPID, and DAMS. Two applications are dedicated to the risk field: SMARTER and ERBASS. And there are three applications focused on Compliance: LIS MODUL, COS, and FRA.

1. The integration process of applications involves several stages, and to determine whether an application can be integrated or not, several factors need to be considered, including:
2. Technology Compatibility: The technologies and systems used in both applications must be compatible to integrate two applications. Different applications may sometimes use other programming languages, operating systems, or technologies, making integration challenging.
3. API Capability: Application Programming Interface (API) is an interface that allows two applications to communicate. The availability of APIs in each application needs to be considered to integrate two applications.

4. Data Structure: Application integration requires data exchange between applications. Therefore, the data structure of each application needs to be considered. If the data structures are incompatible or do not match, application integration may become more complex.
5. Security: Application integration can pose security risks, especially when integrating different applications other parties develop. Therefore, security should be a crucial factor in the integration process. Security evaluation and testing should be conducted to ensure that the integration does not introduce unwanted security risks.
6. Application Function and Purpose: Before integrating two applications, the goals and functions of each application need to be considered. If the objectives and procedures of the applications are significantly different, integration may become more challenging or impractical.
7. Cost and Resources: Application integration incurs costs and requires resources for developing and maintaining the integration. Therefore, cost and resource availability should be considered before integrating two applications.

By considering the factors, it is expected to identify which supporting applications can be integrated to enhance the level of GRC system implementation in the supporting applications of PT. PLN Central Office.

The applications that will be attempted to integrate are the SMARTER application with the ERBASS application and the consolidation of the COS and FRA applications. During the internship, the results of the analysis and interviews conducted will be submitted to the IT Planning and Strategy Department of PT PLN Central Office. The analysis findings will serve as a reference for determining whether the integration of the applications will be implemented to enhance the level of GRC system implementation in the company.

Both of these applications fall under the management umbrella of the Supporting Applications division of PT. PLN Central Office. SMARTER is an application that plays a role in risk within the GRC system. It features the ability to create risk profiles, identify risks, and map risks for the company. On the other hand, ERBASS or E-Risk Based Audit System, is an application designed to audit manually inputted risk assessments, which auditors then evaluate manually.

These applications are created to establish risk management determinations for every activity conducted at PT. PLN Central Office. The User results include the Human Capital Service Division, employees, evaluators, and officials involved in creating termination decrees at PT. PLN Central Office, the application will digitize the process of creating and issuing orders, making it easier, faster, and more accurate.

In the ERBASS or E-Risk Based Audit System application, it can be observed that the system used to assess risks is done manually by auditors. It is considering this working system, with the assistance of the SMARTER application, that generates work risk profiles at PT. PLN Central Office, reference values for risk assessment parameters can be established. The purpose of using this system is to make the parameter levels of activity consistent and reduce human errors that could result in different decisions in similar conditions.

By combining these two applications, several benefits can be achieved, impacting the risk management system within PT. PLN Central Office, such as:

1. Enhanced Risk Assessment: The integration allows for more accurate and consistent risk assessment, reducing discrepancies and improving the overall risk management process.
2. Efficiency and Accuracy: The digitization of processes and automation of risk assessment in ERBASS, coupled with SMARTER's risk profiling capabilities, streamline workflows, making the issuance of termination decrees easier, faster, and more accurate.
3. Standardized Parameters: The integration ensures standardized risk assessment parameters are used, minimizing variations and potential inconsistencies in decision-making.
4. Reduction of Human Errors: By leveraging technology and automation, the risk of human errors in the assessment and decision-making process is reduced, leading to more reliable outcomes.
5. Improved Risk Management: These applications enhance the overall risk management system by providing a comprehensive and integrated approach to risk assessment, identification, and mitigation.

Overall, integrating the SMARTER and ERBASS applications brings numerous advantages that positively impact the risk management system at PT. PLN Central Office, leading to more efficient, accurate, and standardized processes.

Fig -5 Output Result from SMARTER Application

The supporting applications at PT. The COS application and the FRA application are the PLN Central Office that plays a role in rejecting bribery actions within the company. The COS application is designed to detect bribery within the company and establishes a system where employees can acknowledge whether they reject or accept a bribe. On the other hand, the FRA or Fraud Risk Assessment application is focused on fraud management, aiming to detect fraudulent activities. It includes features for reporting and reporting fraud incidents at PT. PLN, as well as problem-solving and prevention measures for future occurrences. Additionally, both applications fall under the same Compliance field in implementing the GRC system. Fig -5 and Fig -6 show the output result from the SMARTER application.

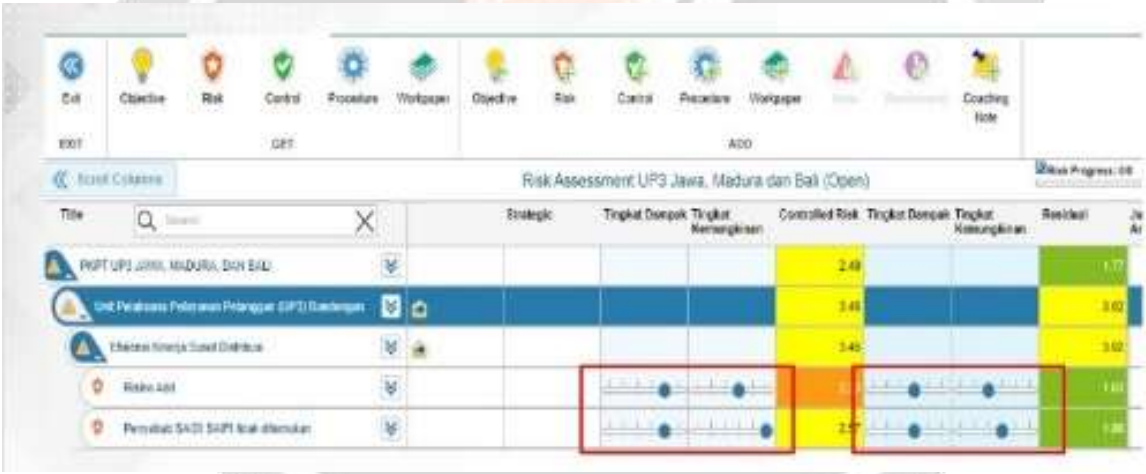

Fig -6 Output Result from SMARTER Application

These two applications can be integrated to generate a comprehensive main application that operates more efficiently within the company's workflow. Furthermore, both applications are under the same BPO (Business Process Outsourcing) division of the PKP Division at PT. PLN Central Office. FRA operates in the Risk field. Integrating the functions of both applications can lead to a more efficient application that supports the company's operations. Additionally, both applications are under the same BPO division at PT's PKP Division. PLN Central Office.

Figure 7 depicts the standardization of the FRA application, while Figure 8 shows the output of mapping the fraud risk levels within PT. PLN Central Office. The color-coded representation indicates the level of threat that can occur. With the same BPO division overseeing both applications, the integration of these two applications brings several benefits, including:

1. Improving Efficiency: By integrating applications, users can save time and effort in transferring data between applications and avoid data duplication.
2. Enhanced Functionality: Application integration allows additional functionality or enhancements to be integrated into a single application. This way, users don't need to switch between different applications to perform related tasks.

3. Cost Savings: Application integration can reduce development and maintenance costs as only one application needs to be developed instead of two separate applications.
4. User-Friendliness: By using integrated applications, users can avoid the complexity of switching between two different applications and quickly access related functionalities.

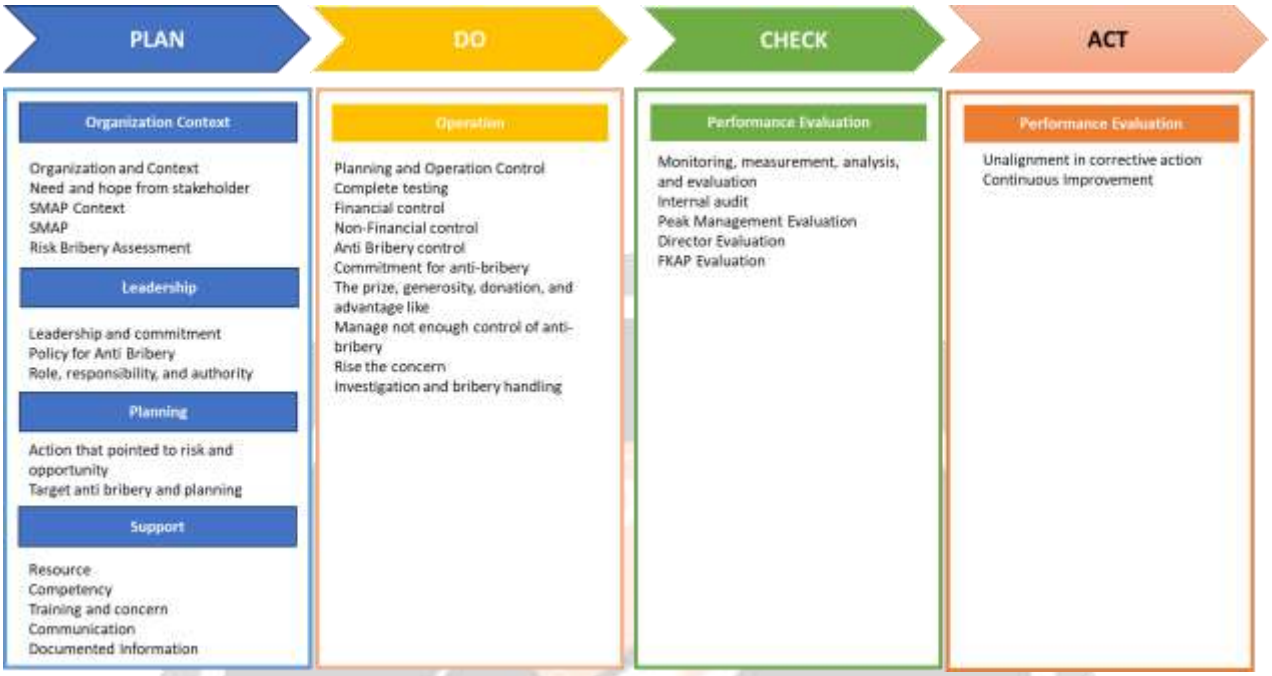

Fig -7 ISO 37001:2016 SMAP clause

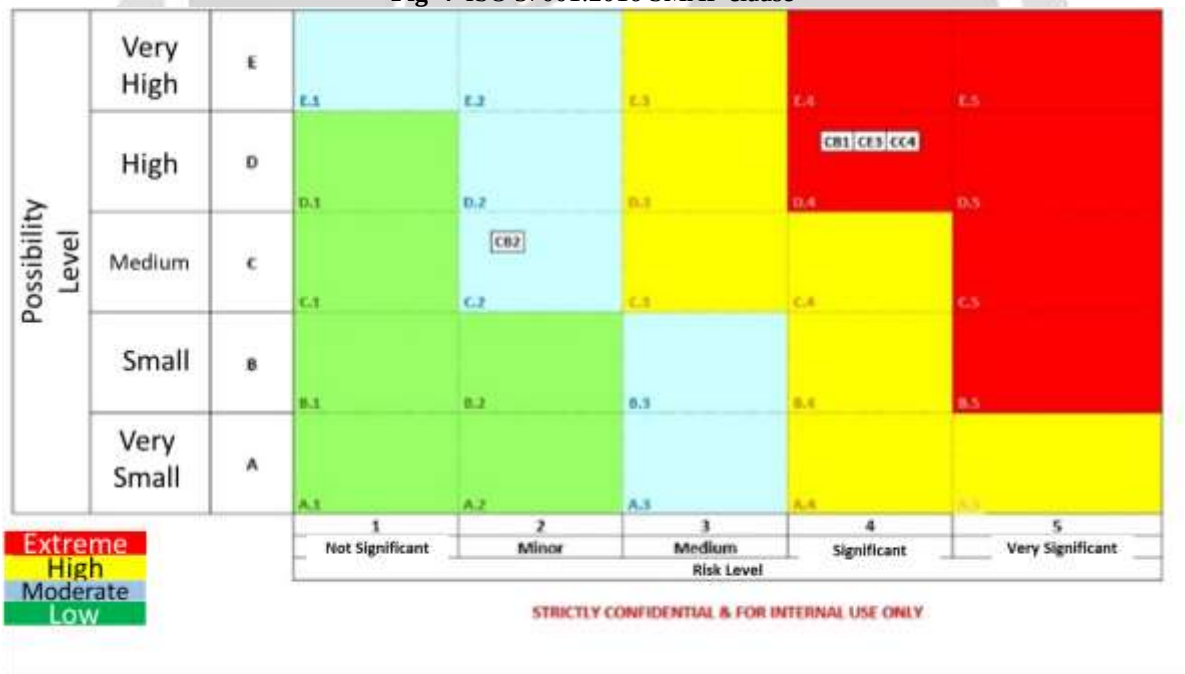

Fig -8 Output Result of FRA Application Risk Mapping

Fig -9 COS Application Explanation

Integrating these two applications will result in a primary compliance application for the company that can be used efficiently and effectively. This application's working system can detect acts of bribery within the company, and fraudulent actions committed by individuals can be processed and thoroughly exposed for each action taken. Additionally, this application can provide PT. PLN employees with a sense that the company will meticulously detect every step they take. It is a preventive measure to make employees hesitate when considering actions that deviate from the company's regulations.

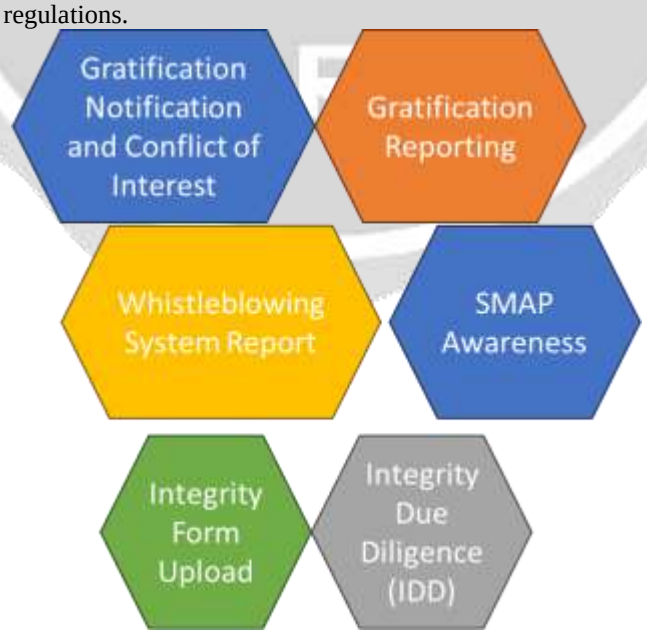

Fig -10 The features that exist in the COS application

Figure 10 illustrates the various features of the COS (Compliance Online System) application. This application includes the gratuity reporting feature, whistleblowing reporting, SMAP awareness, integrity pact uploads, and gratuity notifications. The gratuity notification system provides monthly training for all employees to undergo tests that educate them about gratuities. Moreover, this application can provide PT. PLN employees with a sense that the company will meticulously detect every action they take. It is a preventive measure to make employees hesitate when considering actions that deviate from the company's regulations.

Fig -11 Whistleblowing Reporting feature on the COS application

Figure 11 is one of the reporting features in the COS application. The Whistleblowing System feature is a type of confidential reporting in which the party designated as the perpetrator of the crime does not know the identity of the party reporting the crime to the company.
Using the COSO Framework, the author will describe the GRC system from integrating COS and FRA applications at PT PLN Headquarters. Table 1 shows the components and principles of GRC.

Table -1 Component and Principles of GRC

5 Components	**Principles**
Control Environment	PT PLN has an integrity culture, ethical values, and strong governance in all organizations. PT PLN has a clear organizational structure with responsibility and authority that has been well applied. Has a policy and written procedure for controlling company operation
Risk Assessment	Done the identification and risk evaluation faced by PT PLN in facing fraud and gratification like corruption and bribery Set the prevention with examination regularly.
Control Activities	Implement policies for reporting as well as anti-bribery study at the beginning of the month. Develop systematic procedures for reporting and making reports for any acts of fraud and gratification one.
Communication	Develop an effective reporting and communication system to ensure fraudulent information can be submitted to interested parties. Ensure open and clear communication in all levels of the PT PLN

	organization.
Monitoring Activities	Perform continuous monitoring of the GRC system available to identify weaknesses and errors and make the necessary repairs. Conduct internal audits and independent evaluations on an independent basis periodically to evaluate the effectiveness of the GRC system.

4. CONCLUSIONS

Based on the research conducted at PT PLN Persero regarding the implementation of a high-level design architecture for a centralized application system, the following conclusions can be drawn:

1. Implementing the GRC (Governance, Risk, and Compliance) working system enhances operational efficiency and effectiveness.
2. The selection of a GRC system for a company should consider the company's needs and goals, available resources, and applicable requirements and compliance.
3. The GRC system strengthens corporate governance, regulates and minimizes risks, and enhances employee compliance. The output from one application can serve as input for another application, allowing for the integration of their GRC systems.
4. We are integrating multiple applications into a comprehensive and unified application results from implementing a GRC system.
5. The successful implementation of integrated applications improves decision-making systems.

6. REFERENCES

[1] Gunawan, R. M. B. (2021). GRC (Good Governance, Risk Management, and Compliance). Jakarta: Rajawali Pers. Retrieved from https://books.google.co.id/books?hl=en&lr=&id=NNgaEAAAQBAJ&oi=fnd&pg=PA2&dq=pentingnya+sistem+grc+pada+perusahaan&ots=P6Hg-BYL6w&sig=OnPBoQWmRtJ9JdkpuuI-ehDAX5o&redir_esc=y#v=onepage&q=pentingnya%20sistem%20grc%20pada%20perusahaan&f=false

[2] Racz, N., Weippl, E., & Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In Enterprise Interoperability V (pp. 89-100). Springer, Berlin, Heidelberg. Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-13241-4_11

[3] Anastasya, D. N. (2019, October 1). The Influence of Governance, Risk, and Compliance (GRC) Implementation on Company Performance. Retrieved from https://ojs.umrah.ac.id/index.php/jiafi/article/view/1514/731

[4] Wiesche, M., Berwing, C., Schermann, M., & Krcmar, H. (2011). Patterns for Understanding Control Requirements for Information Systems for Governance, Risk Management, and Compliance (GRC IS). Journal/Conference Name, Volume(83). Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-22056-2_23#author-information

[5] Gibson, D. L., Goldenson, D. R., & Kost, K. (2006). Performance Results of CMMI-Based Process Improvement. Final report. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2006_005_001_14771.pdf

[6] Anders, S. B. (2016). Governance, Risk Management, and Compliance: OCEG and the Network. The CPA Journal, 86(3). Retrieved from https://www.proquest.com/openview/c61c97dbf1b363f7ddea6144e9557b5e/1?pq-origsite=gscholar&cbl=41798

[7] Atkinson, J., & Leandri, S. (2006). Best practices: an organizational structure that supports compliance; Traditional organizational structure is crumbling under the weight of ever-increasing regulations that drive greater accountability and transparency. Smart companies are at the forefront of building new and improved structures that support and enhance this new compliance environment, and best practices are emerging. Internal Auditor, 63(5), 65-70. Retrieved from https://go.gale.com/ps/i.do?id=GALE%7CA140306548&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=08954186&p=AONE&sw=w&userGroupName=anon%7Ef779fd17

[8] CROWE. (2019). COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK: An Implementation Guide for the Healthcare Provider Industry. In A. Schandl MSIB, CPA & P. L. Foster MBA, ARe, ARM, AIC, CPCU (Authors), January 2019. Retrieved from https://www.coso.org/Shared%20Documents/CROWE-COSO-Internal-Control-Integrated-Framework.pdf
[9] Title: "What is Governance, Risk, and Compliance (GRC)?" Author: Amazon AWS Website: aws.amazon.com URL: https://aws.amazon.com/id/what-is/grc/#:~:text=AWS%20membantu%20GRC%3F-,Apa%20itu%20GRC%3F,semua%20peraturan%20industri%20dan%20pemerintah. Accessed: February 11, 2023