SELINUS UNIVERSITY
OF SCIENCES AND LITERATURE

THE EVALUATION OF INTEGRATED GOVERNANCE, RISK, AND COMPLIANCE (GRC) IMPLEMENTATION TO ENHANCE ENTERPRISE RISK MANAGEMENT (ERM): A CASE STUDY

By Ahmed Sekti Adinata

A DISSERTATION

Presented to the Department of
Enterprise Risk Management
Program at Selinus University

Faculty of Business & Media
In fulfillment of the requirements
for the degree of Doctor of Philosophy
in Enterprise Risk Management

2024

DECLARATION

I do hereby attest that I am the sole author of this project/thesis and that its contents are only the result of the readings and research I have done. The dissertation titled “The Evaluation of Integrated Governance, Risk, and Compliance (GRC) Implementation to Enhance Enterprise Risk Management (ERM): A Case Study" submitted for the degree of Doctor of Philosophy (PhD) at Selinus University of Sciences and Literature, is my original work. To the best of my knowledge this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted as part of the requirements of any other academic degree or non-degree program, in English or in any other language. This is a true copy of the thesis, including final revisions.

Date : 16 October 2024

Name : Ahmed Sekti Adinata

Student ID : ID UNISE2571IT

Signature :

ABSTRACT

This PhD thesis presents a comprehensive case study on the implementation and optimization of an integrated Governance, Risk, and Compliance framework at Company X, a leading pharmaceutical company in Indonesia. The in-depth study examines the key drivers, challenges, and valuable lessons learned from Company X's experience in transitioning its previously siloed risk management, compliance, and governance functions into a cohesive, enterprise-wide GRC system.

The research findings suggest that the implementation of a well-designed and effectively executed GRC program can significantly enhance an organization's overall Enterprise Risk Management capabilities. By integrating these critical functions, Company X was able to better identify, assess, and proactively mitigate a wide range of strategic, operational, financial, and compliance-related risks.

The case study highlights the critical role of several key success factors, such as strong leadership commitment, a supportive organizational culture, effective change management practices, and the strategic alignment of the GRC initiative with the company's overall business objectives. The thesis provides a detailed analysis of the comprehensive GRC implementation journey at Company X, including the key design considerations, innovative process improvements, strategic technology enablement, and the evolution of the internal audit function to support the continuous maturity and optimization of the GRC framework.

The research findings offer a wealth of valuable insights and practical recommendations that can be applied by other organizations seeking to enhance their Enterprise Risk Management through the implementation of an integrated, enterprise-wide Governance, Risk, and Compliance framework.

Keywords: Enterprise Risk Management, Governance, Risk, Compliance, Organizational Culture, Change Management, Internal Audit, Digital Transformation

ACKNOWLEDGEMENT

Alhamdulillahi rabbil ‘alamin, It is a remarkable achievement, that I’ve arrived at this stage. I would like to express my heartfelt gratitude to the many individuals who have supported and encouraged me throughout the journey of completing my doctoral dissertation.

I am really grateful to my parents-in-law, **Drs. Yasun S.E., M.M. (Papa)** and **Petut Yulistria (Mama)** who have generously and unconditionally fully supported my PhD study. Their supports and contributions have been instrumental in allowing me to focus solely on my research and studies, and their unwavering belief in my abilities has been a constant source of motivation.

I am also immensely grateful to my beloved parents, **Drs. Ateng Suhaeni S.E., Ak., CA., M.M. (Ayah)** and **Dra. Rina Diana Surianata (Ibu),** whose unwavering love and support have been a constant source of comfort and strength throughout the challenges and triumphs of this endeavor. Their encouragement has provided me with the motivation to push forward, and I am forever thankful for their invaluable guidance and profound wisdom, which have been instrumental in shaping my personal growth.

My heartfelt appreciation also goes to my beloved wife, **Fitriani Puspitasari S.E.,** and my amazing two children, **Arkhanza Adinata** and **Rayyanza Adinata**. They always inspire me and drive me to be the best version of myself that I can be. They are the reason I strive more physically and spiritually, and I push myself to achieve my best.

To my supervisor, **Prof. Salvatore Fava Ph.D**., I extend my sincere gratitude for your invaluable guidance, mentorship, and unwavering support in shaping the successful completion of this dissertation. I would also like to express my appreciation to **Selinus University of Sciences and Literature** for providing the resources, infrastructure, and academic environment that have been essential to the successful completion of this research.

Finally, I would like to express my sincere gratitude to other individuals and organizations who have contributed to the successful completion of my doctoral dissertation, but whom I cannot mention explicitly due to space constraints. Their support, whether financial, intellectual, or emotional, has been instrumental in helping me achieve this milestone.

TABLE OF CONTENT

CHAPTER 1
INTRODUCTION

1.1. Background

Enterprise Risk Management has become a critical aspect of modern business operations, as organizations strive to navigate the increasingly complex and volatile business landscape (Marchetti, 2012). Effective risk management is crucial for organizations to mitigate potential risks, optimize performance, and ensure long-term sustainability (Bromiley et al., 2015). The integration of Governance, Risk, and Compliance processes has become increasingly important in organizations as it can enhance risk management practices and optimize performance. By adopting a holistic approach that combines governance, risk management, and compliance, organizations can better identify, assess, and manage risks while aligning with strategic objectives and regulatory requirements.

Governance, Risk, and Compliance (GRC) is defined as the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty, and act with integrity (OCEG, 2024). GRC assists a company in completely understanding the risks it confronts in the face of Volatility, Uncertainty, Complexity and Ambiguity (VUCA) condition. Understanding an organization's risks is crucial for making strategic decisions that lead to cost effective, excellent execution, and profitable growth. GRC connects strategic goals with the risk management process and enables an organization to integrate disparate systems and programs into a business-wide, risk-based internal control framework that is both efficient and effective.

One way to enhance Enterprise Risk Management is through the adoption of an integrated GRC approach. Company X, an Indonesian pharmaceutical firm that manufactures and markets Over-The-Counter (OTC) medical products throughout Asia and Africa, has recognized the potential benefits of implementing an integrated GRC framework to strengthen its risk management practices. Integrating Governance, Risk, and Compliance processes is a complex task that requires careful planning and execution. The integration of GRC processes has the potential to not only identify and assess risks, but also to provide a framework for managing these risks in a way that aligns with the overall goals of the organization.

Company X leveraged the GRC capability model from the Open Compliance and Ethics Group (OCEG) as a framework to evaluate its progress (what went well and what can be improved) in implementing integrated GRC. This model provided a comprehensive set of guidelines and best practices for assessing the maturity of Company X's GRC capabilities and identifying areas for improvement. Additionally, Company X utilized the ISO 31000:2018 standard as a reference for its enterprise risk management practices. This standard offered a structured framework for identifying, assessing, and managing risks in alignment with Company X's strategic objectives and regulatory requirements. By integrating GRC processes and implementing a centralized system, Company X is poised to enhance its enterprise risk management practices. This integration is also expected to foster better coordination and communication across departments, leading to a more comprehensive and holistic approach to risk management.

This study aims to evaluate the implementation of GRC at Company X and assess its impact on the company's enterprise risk management practices. As we dig deeper into this case study, we will look into the particular obstacles Company X faced, the approaches used for GRC integration, and how these actions affected the overall enterprise risk management framework. One of the main obstacles Company X faced in integrating GRC processes was the lack of a centralized system for managing governance, risk, and compliance activities. This led to disjointed and inefficient processes, with different departments handling governance, risk management, and compliance separately. This lack of integration also resulted in a lack of visibility and coordination, making it difficult to identify and address potential risks and compliance issues.

This study has a qualitative research method with a case study approach and GRC Capability Model version 3.5 issued by OCEG as an evaluation framework. This research aims to find out how well Company X implements integrated GRC based on Company X capabilities. The reason for using the GRC Capability Model version 3.5 from OCEG is that OCEG introduces this model as an integrated model, which is the latest model from OCEG. Therefore, this research is important to evaluate Company X's progress (what went well and what can be improved) in implementing integrated GRC with GRC Capability Model version 3.5 as an evaluation framework.

1.2. Research Problem and Questions

The research questions addressed in this study are:

1. What is the progress (what went well and what can be improved) of Company X in implementing integrated GRC based on the GRC Capability Model version 3.5?
2. What are the key challenges and barriers faced by Company X in implementing integrated GRC?
3. How has the implementation of integrated GRC affected Company X's enterprise risk management practices?

To answer these research questions, the study will utilize a qualitative case study approach, drawing from multiple sources of data, including interviews with key stakeholders, document analysis, and observation of the company's GRC integration efforts.

1.3. Objectives of The Study

The primary objectives of this study are:

1. To evaluate the progress of Company X in implementing integrated GRC based on the GRC Capability Model version 3.5 (what went well and what can be improved).
2. To identify the key challenges and barriers faced by Company X in implementing integrated GRC.
3. To analyze the impact of integrated GRC implementation on Company X's enterprise risk management practices.

In the following chapters, we will delve into the specific methodologies employed to achieve these objectives and provide recommendations based on the findings. Moreover, this study aims to evaluate the progress (what went well and what can be improved) of Company X in implementing GRC by assessing its current GRC system and identifying areas for improvement. The integration of GRC processes is vital for enhancing enterprise risk management in Company X. By integrating governance, risk management, and compliance activities, the organization can establish a comprehensive approach to risk identification, assessment, and mitigation that aligns with the organization's objectives and ensures

compliance with regulations and policies. Additionally, the integration of GRC processes can enhance the transparency and accountability of risk management practices within Company X. This study will provide valuable insights into the challenges faced by Company X in integrating GRC processes into their risk management practices.

1.4. Structure of the Thesis

This PhD thesis is organized as follows:

1. Chapter 1 - Introduction presents the background, research problem, objectives, and the structure of the thesis.
2. Chapter 2 - Literature Review provides a comprehensive review of the existing literature on Governance, Risk, and Compliance (GRC) and Enterprise Risk Management (ERM), including the previous researches on GRC and ERM.
3. Chapter 3 - Research Methodology outlines the qualitative case study approach and the data collection and analysis methods used in this study.
4. Chapter 4 - Company X Profile delves into the overview of Company X, its industry, values and purposes, business performance, organizational structure, business process mapping, current business situation and complication, and strategic directions.
5. Chapter 5 - Discussion and Recommendation presents the key findings from the case study and offers recommendations for improving GRC implementation at Company X.
6. Chapter 6 - Summary and Conclusion presents the key findings summary and concludes the study.

Throughout the thesis, citations from the provided sources will be used to support the research findings and provide a comprehensive understanding of the topic.

CHAPTER 2
LITERATURE REVIEW

2.1. Governance Concept

Governance, as defined by the OECD, refers to the system by which organizations are directed and controlled (Abdullah, 2019). It encompasses the processes, policies, and structures that guide the decision-making, oversight, and leadership of an organization. Effective governance involves establishing clear roles and responsibilities, promoting transparency and accountability, and aligning the organization's actions with its strategic objectives and stakeholder interests. Governance is a critical component of any well-run organization and provides the foundation for effective risk management and compliance activities (Chandani & Mehta, 2020).

Corporate governance involves a set of relationships between a company's management, board, shareholders and stakeholders (OECD, 2023). Corporate governance also provides the structure and systems through which the company is directed and its objectives are set, and the means of attaining those objectives and monitoring performance are determined. The *G20/OECD Principles of Corporate Governance* include:

1. **Ensuring the basis for an effective corporate governance framework:** The corporate governance framework should promote transparent and fair markets, and the efficient allocation of resources. It should be consistent with the rule of law and support effective supervision and enforcement.

2. **The rights and equitable treatment of shareholders and key ownership functions:** The corporate governance framework should protect and facilitate the exercise of shareholders' rights and ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights at a reasonable cost and without excessive delay.

3. **Institutional investors, stock markets, and other intermediaries:** The corporate governance framework should provide sound incentives throughout the investment chain and provide for stock markets to function in a way that contributes to good corporate governance.

4. **Disclosure and transparency:** The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, sustainability, ownership, and governance of the company.
5. **The responsibilities of the board:** The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders.
6. **Sustainability and resilience:** The corporate governance framework should provide incentives for companies and their investors to make decisions and manage their risks, in a way that contributes to the sustainability and resilience of the corporation.

According to OCEG (2024), governance is the act of indirectly guiding, controlling, and evaluating an entity, process, or resource by constraining and conscribing resources. It has an indirect influence over the thing being managed. Thus, governing something involves indirect actions & controls that constrain and conscribe resources.

Governance actions and controls are additional controls beyond management controls that assist the governing authority in constraining and conscribing the organization. Additional governance actions and controls are added when management actions and controls are not considered sufficient.

Some key benefits of effective corporate governance include (Costa, 2017):

1. Attracting investment capital and ensuring shareholder trust by demonstrating strong governance practices and a commitment to ethical decision-making
2. Promoting transparency and accountability through clear communication, reporting, and oversight mechanisms
3. Improving company performance and enhancing stakeholder value by aligning strategic objectives with effective risk management and compliance measures

Governance is not just a set of rules and principles. It is a fundamental aspect of modern organizations that shapes the dynamics of decision-making, accountability, and ethical behavior.

Effective governance has a profound impact on the internal dynamics of organizations. Transparent decision-making processes and accessible information foster an environment of trust and confidence among employees. This, in turn, leads to a more engaged and motivated workforce. Moreover, integrity in decision-making ensures that ethical and moral principles are upheld, shaping a culture of fairness and honesty within the organization. Accountability, another crucial element of governance, encourages individuals and organizations to take responsibility for their actions. This not only enhances performance but also instills a sense of discipline and commitment to organizational goals. Furthermore, stakeholder participation ensures that decisions are inclusive and reflective of diverse perspectives, thus promoting a more holistic and well-informed decision-making process. These attributes of effective governance enable organizations to better navigate complex challenges, anticipate and mitigate risks, and drive sustainable performance (Wang et al., 2021).

2.2. Risk Management Concept

According to ISO 31000:2018, risk is the effect of uncertainty on objectives. Risk management is the coordinated activities to direct and control an organization with regard to risk.

In today's business world, characterized by Volatility, Uncertainty, Complexity, and Ambiguity (VUCA), effective risk management becomes crucial as organizations grapple with multifaceted challenges that can significantly impact their strategic objectives and operational effectiveness. The need for integrated governance, risk, and compliance frameworks becomes even more pronounced as companies strive for enhanced agility and resilience, allowing them to proactively address emerging risks while aligning their risk management practices with their overall business strategy to achieve sustainable performance.

According to OCEG (2024), the objectives of risk management help an organization achieve the following goals:

1. Value creation and protection: Risk management contributes to the achievement of organizational objectives and the creation of value for stakeholders
2. Aids decision making: A strong commitment to risk management assists decision-makers in making informed choices, prioritizing actions, and selecting among various alternatives

3. Risk treatment: Risk management helps proactively address risks, reducing the likelihood of financial loss, operational hazards, and other operational disruptions.
4. Facilities continual improvement: Companies with robust risk management programs are better able to develop and implement strategies to improve risk management maturity and organizational risk-awareness
5. Explicitly address uncertainty: Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed
6. Improves resilience: Risk Management enhances the organization's ability to anticipate, prepare for, respond to, and recover from disruptions and adverse events

2.2.1 Principles of Risk Management

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.

The principles offer a framework for effective and efficient risk management. They help communicate the value of risk management and clarify its purpose. These principles serve as the foundation for an organization's risk management approach and should be factored into developing its risk management structure and processes. Ultimately, the principles empower the organization to navigate the uncertainties that impact its objectives. ISO 31000:2018 outlines that effective risk management requires the elements:

1. Integrated: Risk management is an integral part of all organizational activities.
2. Structured and comprehensive: A structured and comprehensive approach to risk management contributes to consistent and comparable results.
3. Customized: The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.
4. Inclusive: Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered, resulting in improved awareness and informed risk management.

5. Dynamic: Risks can emerge, change or disappear as an organization's external and internal context changes.
6. Best available information: The inputs to risk management are based on historical and current information, as well as future expectations.
7. Human and cultural factors: Human behavior and culture significantly influence all aspects of risk management at each level and stage.
8. Continual improvement: Risk management is continually improved through learning and experience.

There are 9 principles for effective risk management (OCEG, 2024) as follows:

1. Holistic integration: Establish a consistent risk management capability that engages all stakeholders, functions and processes across the organization.
2. Systematic approach: Apply a systematic, structured and timely approach to managing risk, aligning with the organization's objectives and context.
3. Customization: Tailor the risk management framework and processes to the specific needs and characteristics of the organization.
4. Stakeholder participation: Actively engage with internal and external stakeholders to ensure their knowledge, views and perceptions are considered.
5. Proactivity and adaptability: Anticipate and respond to changes that can impact objectives, monitoring the internal and external context and adjusting the risk management activities as needed.
6. Ongoing enhancement: Continually develop and improve the risk management activities through learning, experience and performance measurement.
7. Data driven decision making: Use the best available information, including historical data, current conditions and future expectations, to inform risk-based decision making.
8. Influence of human culture elements: Recognize and address the impact of human behavior, attitudes and organizational culture on risk management.
9. Transparency: Enable visibility, accountability and assurance with clear communication and reporting.

2.2.2 Framework: ISO 31000: 2018

The ISO 31000:2018 international standard offers guidelines and principles to assist organizations in establishing, implementing, and continuously refining their risk management frameworks. Designed to be universally applicable, the standard provides organizations, regardless of their size, industry, or sector, with principles, a structured approach, and a process for effectively managing risk within their operations.

The ISO 31000:2018 standard provides a framework and guidelines for organizations to integrate risk management into their overall management system and decision-making processes. This framework emphasizes the importance of embedding risk management into organizational culture and operations, ensuring that it is not treated as a separate activity but rather as a fundamental component that supports all aspects of an organization's functions and strategies, thus enhancing its resilience and ability to achieve its objectives.

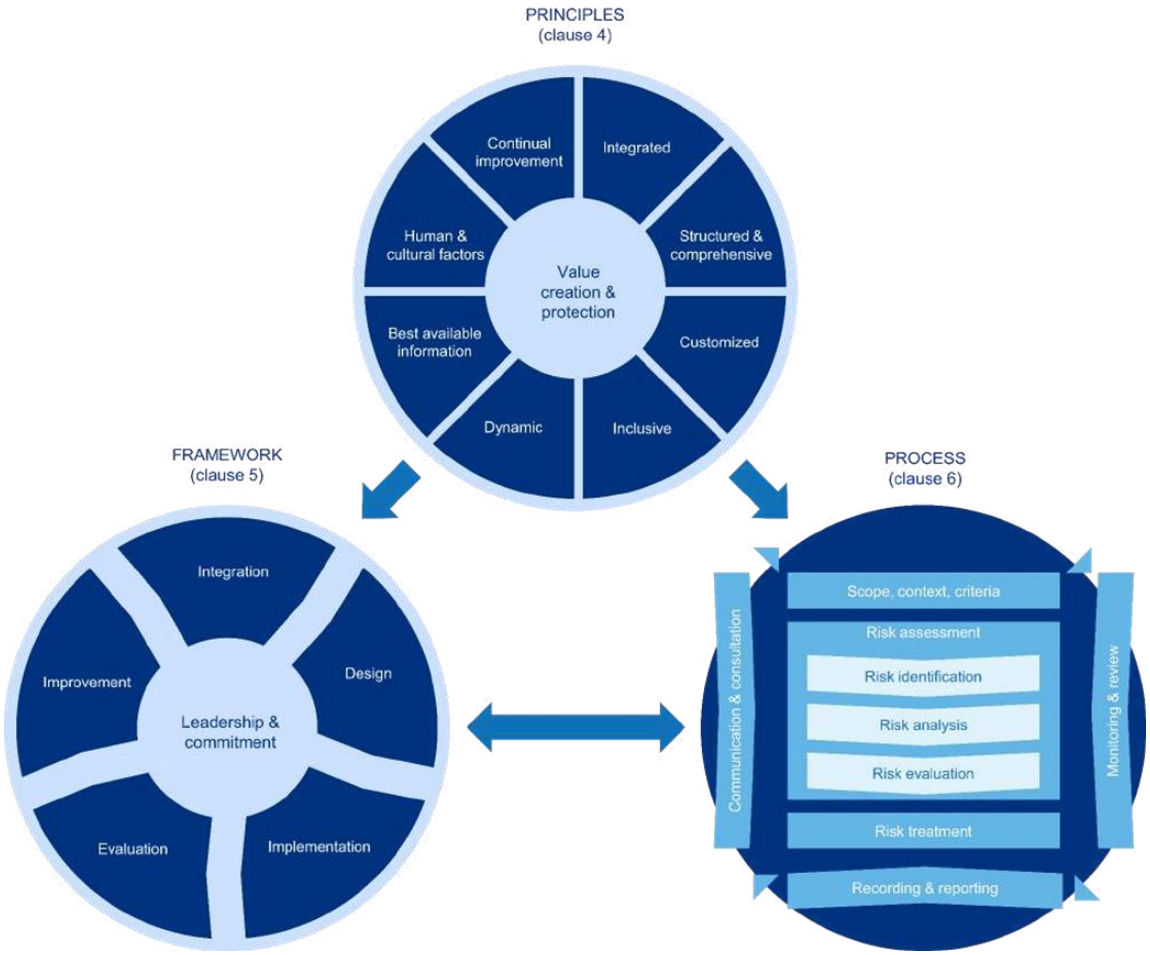

Image 1 – ISO 31000 Framework for Enterprise Risk Management

ISO 31000 framework has the following key aspects:

1) Process

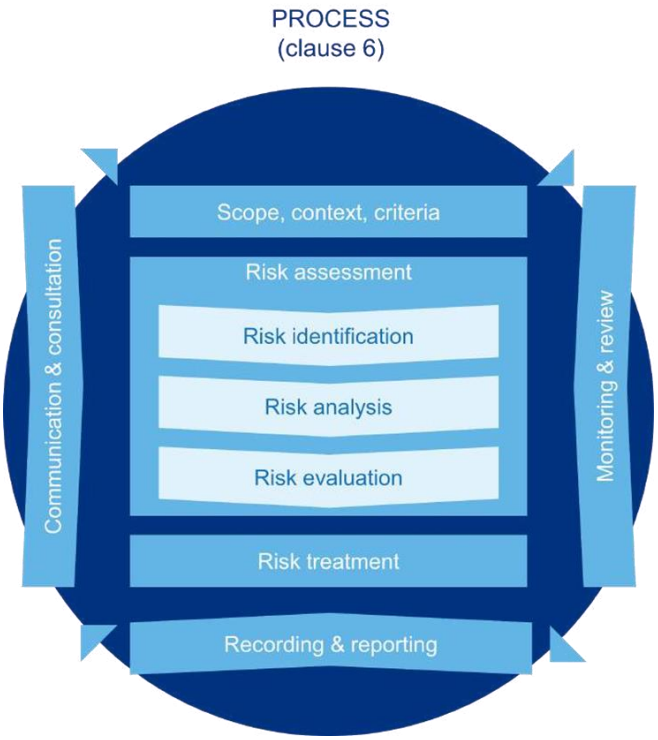

Image 2 – ISO 31000 Process

ISO 31000 outlines a risk management process that includes:

1. Communication and Consultation: Engaging with stakeholders to ensure that risk management is informed by diverse perspectives and that stakeholders are aware of the risks and how they are being managed.
2. Establishing the Context: Defining the external and internal context in which the organization operates, including the scope and criteria for risk management.
3. Risk Assessment:
    - Risk Identification: Identifying risks that could impact the achievement of objectives.
    - Risk Analysis: Analyzing the identified risks in terms of their likelihood and impact.

- Risk Evaluation: Comparing risk analysis results with risk criteria to determine the significance of the risks and prioritize them.

4. Risk Treatment: Developing and implementing strategies to manage risks, which may include avoiding, reducing, transferring, or accepting the risks.
5. Monitoring and Review: Continuously monitoring and reviewing risks and the effectiveness of risk management measures to ensure they remain relevant and effective.
6. Recording and Reporting: Documenting the risk management process and communicating risk information to stakeholders as appropriate.

2) Framework

Image 3 – ISO 31000 Framework

The framework encompasses the following key components:

1. Leadership and Commitment
    - Leadership: Senior management must demonstrate commitment to integrating risk management into the organization's governance structure and strategic planning.

- Governance: Establishing a risk management policy and defining roles, responsibilities, and accountabilities for risk management.

2. Integration
    - Integration into Governance: Embedding risk management within the organization's governance framework, ensuring alignment with overall goals and objectives.
    - Integration into Processes: Integrating risk management into organizational processes, including decision-making, performance management, and business planning.
3. Design
    - Understanding the Organization and Its Context: Analyzing the internal and external environment in which the organization operates.
    - Risk Management Policy: Developing a risk management policy that outlines the organization's approach to risk management.
    - Risk Management Plan: Creating a plan that defines how risk management will be implemented, including resources, responsibilities, and timelines.
4. Implementation
    - Implementation of the Framework: Executing the risk management plan, ensuring that risk management activities are integrated into the organization’s operations.
    - Change Management: Managing changes to the risk management framework and processes as needed to address evolving risks and organizational changes.
5. Evaluation
    - Monitoring and Review: Continuously monitoring and reviewing the risk management framework and processes to ensure their effectiveness and relevance.

- Performance Measurement: Measuring the performance of risk management activities and making necessary adjustments to improve outcomes.

6. Improvement: Continual Improvement: Identifying and implementing opportunities for improving the risk management framework and processes based on lessons learned and feedback.

2) Principles

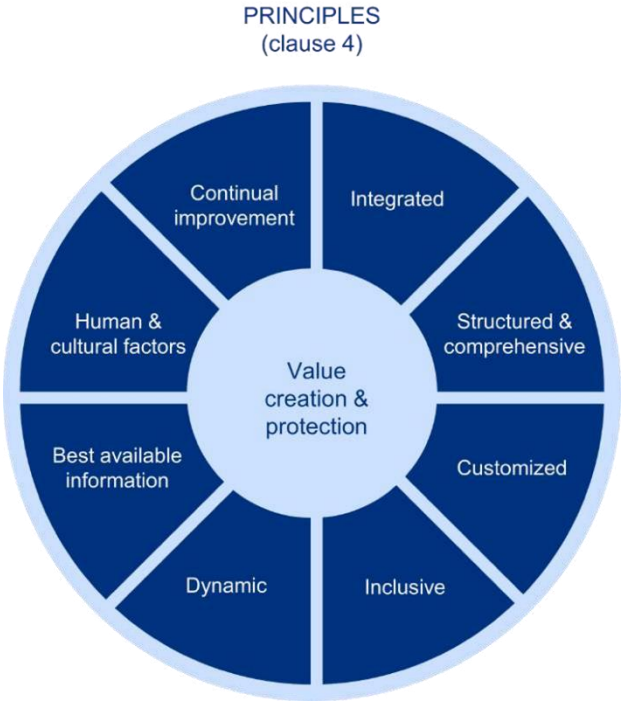

Image 4 – ISO 31000 Principles

The attributes that an effective risk management framework should have:

1. Integrated: Risk management should be an integral part of all organizational activities.
2. Structured and Comprehensive: A systematic, structured, and comprehensive approach to risk management contributes to consistent and comparable results.
3. Customized: The risk management framework and processes should be customized to the organization's external and internal context.

4. Inclusive: Involvement of stakeholders ensures that risk management considers diverse perspectives and insights.
5. Dynamic: Risk management should anticipate, detect, and respond to changes in the environment and emerging risks.
6. Best Available Information: Decisions should be based on the best available information, acknowledging the limitations and uncertainties of data.
7. Human and Cultural Factors: Recognize the impact of human behavior and culture on all aspects of risk management.

2.2.3 Integrated Risk Management (IRM)

Integrated Risk Management is a structured approach using empowered actors for managing, overseeing and assessing the key risks across an organization that ties together functions across an organization which have a role in managing risks, overseeing functions which manage risks or provide assurance over risks (OCEG, 2024). These functions can include those responsible for:

- Governance
- Risk Management
- Compliance
- Information Security
- Quality Control
- Internal Control
- Financial Control
- Data Protection
- Internal Audit
- Business Continuity

The term "integrated" in the context of risk management refers to a comprehensive strategy in which risk management approaches are seamlessly merged and incorporated inside the company.

2.2.3.1 Traditional Risk Management vs. IRM

Risk management has transitioned from a traditional approach to a more comprehensive model known as Integrated Risk Management, according to OCEG. The key differences between traditional risk management and IRM can be summarized as follows:

Image 5 – Difference between traditional risk management and IRM

1. **Emphasis**

Traditional risk management tends to prioritize risk mitigation and control as its primary objective, aiming to reduce potential threats and minimize losses. This approach is often risk-averse, favoring safety and stability over potential gains. Organizations following this method typically seek to avoid risks wherever possible, viewing risk management as a protective measure.

In contrast, Integrated Risk Management emphasizes the development of organizational resilience to risks. This approach focuses on cultivating the organization's capacity to withstand

and recover from adverse events. IRM also encourages selective risk-taking and actively seeks opportunities that align with strategic goals. This approach recognizes that taking calculated risks can lead to significant benefits and innovation, seeking to balance protection with potential growth.

2. Responsibility

In conventional risk management, individual process owners bear the primary responsibility for managing the risks within their respective domains. Department heads oversee this process, ensuring adherence to risk management practices across their areas of oversight.

In contrast, Integrated Risk Management elevates the responsibility for risk oversight to senior leadership, including the board of directors and top management. This shift ensures that risk management is closely aligned with the organization's strategic goals and is seamlessly integrated into high-level decision-making processes.

3. Scope

Traditional risk management typically confines its scope to operational risks, primarily those that have previously materialized. The focus is on mitigating risks related to day-to-day operations and preventing the recurrence of similar issues. This approach is generally reactive, addressing risks as they emerge.

In contrast, Integrated Risk Management encompasses a broader range of risks. It includes strategic-level risks that can impact the organization as a whole, such as those related to sustainability and value creation, as well as emerging risks. IRM adopts a proactive stance, anticipating potential future risks and embedding risk management into the strategic planning process.

4. Approach

The approach in traditional risk management involves reviewing individual risks separately. Each risk is assessed and managed on its own, with strategies developed for specific threats. Decisions are based on the organization’s risk tolerance, often leading to conservative risk management practices that aim to avoid significant exposure.

In contrast, IRM adopts an aggregate view of overall long-term risks. It considers all risks in a comprehensive manner, integrating them into a unified strategy. Decisions are guided by the

organization’s risk appetite, allowing for a more balanced approach that aligns with the organization’s long-term goals.

2.2.3.2 The Main Components of IRM

OCEG (2024) has defined the three main components of IRM as follows:

1. Board Oversight

The board of directors plays a crucial role in Integrated Risk Management by setting the overall strategic direction and governance framework. Their key responsibilities encompass providing oversight and establishing the necessary structures to enable effective risk management across the organization. Crucially, the board defines the organization's risk appetite, which determines the level of risk the entity is willing to accept in pursuit of its objectives. By defining these parameters, the board ensures that the risk management approach is aligned with the organization's strategic goals and that a comprehensive framework is in place to identify, assess, and manage risks effectively.

2. Management Implementation

Management is tasked with the implementation of the IRM framework within the organization. This entails establishing the requisite systems, infrastructure, and processes, as well as delineating roles and responsibilities. Management ensures that the appropriate personnel, technology, and procedures are in place to align with the organization's risk appetite. They also institute accountability mechanisms for risk management, guaranteeing consistent identification, assessment, and mitigation of risks across the organization.

3. Independent Monitoring

The internal audit function plays a crucial role in providing independent oversight of the IRM system. This involves monitoring the effectiveness of the organization's risk management practices, verifying that risks are being managed in alignment with the established framework. Internal auditors offer valuable insights and recommendations, assisting in the identification of areas for improvement and ensuring the continued effectiveness of the IRM system. This independent monitoring is essential for preserving the integrity and reliability of the overall risk management process.

2.3. Compliance Concept

OCEG (2024) defined compliance as a measure of the degree to which obligations and requirements are addressed. An obligation is a requirement that an organization must or should address because of a promise, whether mandatory or voluntary as follows:

1. **Mandatory Obligations:**

   Obligations that an organization must address because of some legitimate authority (e.g., laws, rules, regulations).

2. **Voluntary Obligations:**

   Obligations that an organization chooses to address because of voluntary decisions (e.g., contracts, agreements and values).

Compliance & Ethics provides methods to identify and address mandatory and voluntary obligations and the underlying ethical principles and values. The act of managing processes and resources to achieve the desired level of compliance is called a compliance management.

Compliance refers to the adherence to laws, regulations, policies, and ethical standards by an organization. OCEG provides a comprehensive framework for understanding and implementing compliance within an organization. This framework includes the integration of governance, risk management, compliance, and ethical standards into the organization's operations. It emphasizes the importance of a holistic approach to compliance, focusing on not only meeting legal and regulatory requirements but also on aligning with the organization's values and ethical principles. By adopting the OCEG framework, organizations can establish a culture of compliance that permeates all levels of the company, leading to better risk management and ethical decision-making.

The OCEG framework serves as a valuable guide for organizations seeking to establish a robust compliance program. By integrating governance, risk management, and ethical standards, the framework emphasizes the interconnected nature of compliance with other aspects of organizational management. This interconnected approach ensures that compliance is not viewed in isolation but rather as an integral component of the organization's overall operations.

One of the key strengths of the OCEG framework is its emphasis on aligning compliance with the organization's values and ethical principles. This not only ensures that the organization is

meeting its legal and regulatory obligations but also creates a culture where ethical decision-making is ingrained in the organizational fabric. Moreover, by permeating compliance throughout all levels of the company, the OCEG framework enables organizations to create a culture of compliance that is not limited to a specific department or function.

Furthermore, the OCEG framework's holistic approach to compliance can lead to improved risk management. By embedding compliance within the organization's operations, it becomes easier to identify and address potential risks, thereby enhancing the overall resilience of the organization.

Overall, the OCEG framework provides a comprehensive and integrated approach to compliance that goes beyond mere regulatory adherence, offering organizations a roadmap to cultivate a culture of compliance and ethical decision-making.

According to Gunawan (2016) compliance generally means adjustment to a rule, such as a special rule or policy, standard or law. Compliance with the rule of law explains the objectives of a corporate or public institution in their efforts to ensure that the staff understand and take every step to comply with the rules of law.

Susilo (2017) defined two types of compliance obligations:

1. Compliance requirements or compliance requirements arising from regulations, laws, laws and industry standards. In practice, this obligation is often referred to as "compliance".
2. Compliance commitment, or commitment of compliance, is when a company voluntarily sets certain self-regulation obligations to comply with. This leads to claims to be met. Some of the provisions that are included in it are business ethics guidelines. These provisions, among others, corporate business ethic guideline, industry association agreements, internal operational procedures, and others. This obligation in practice is better known as "business ethics and behavior".

These two types of compliance must be fulfilled, otherwise there will be consequences. The potential for failure to comply with these compliance claims has a potential impact called compliance risk or legal risk according to the infringement occurred. For example, the compliance obligation to be fulfilled is to pay taxes. If the company does not pay it then there will be consequences.

2.4. Governance, Risk, and Compliance (GRC)

2.4.1. Principled Performance

Organizations, regardless of their scale, function within an environment characterized by volatility, uncertainty, complexity and ambiguity (VUCA). The OCEG community developed the concepts of Principled Performance and GRC to address VUCA challenges and disconnection. These frameworks aim to offer a structure for mitigating instability and establishing connections in the midst of widespread unpredictability and disarray.

According to OCEG (2024), principled performance is a noble goal for every organization to "reliably achieve objectives, address uncertainty, and act with integrity." The major parts of the definition are:

1. Reliably (thoughtfully, consistently, dependably, and transparently)
2. Achieve objectives (achieve mission, vision, and balanced objectives)
3. Address uncertainty (address opportunities and obstacles that balance risk and reward)
4. Act with integrity (live out values and stay within mandatory and voluntary boundaries)

When an organization adopts the principles of Principled Performance and GRC, it evolves from operating in siloed departments to integrating capabilities, from isolated individuals to interconnected teams, from scattered goals to a deliberate culture, and from narrow skills to an interdisciplinary approach.

As the organization pursues its objectives, it navigates significant uncertainty, encountering both promising opportunities and challenging obstacles. Additionally, the organization must develop a flexible and resilient business model that can effectively address its obligations while operating within the mandatory and voluntary boundaries set by governing authorities. These include:

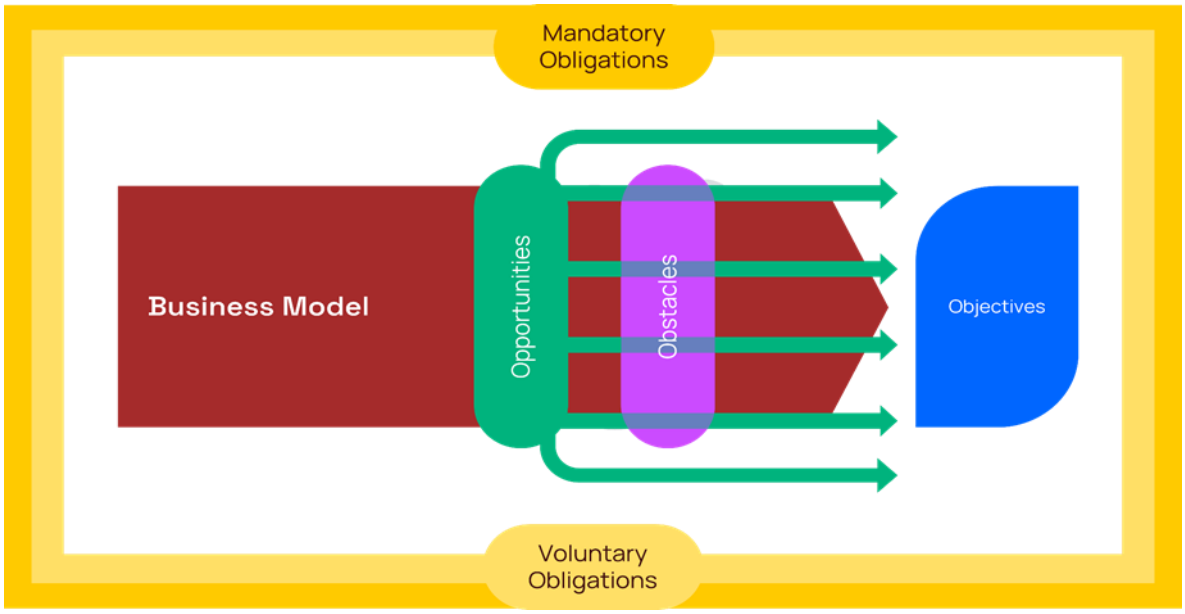

Image 6 - Big Picture of What It Means to Do Business

1. Opportunities are generally associated with reward and represent a positive, favorable effect of uncertainty on objectives. Reward is addressed through performance management systems and key performance indicators.
2. Obstacles are generally associated with risk and signify a negative, unfavorable effect of uncertainty on objectives. Risk is handled using risk management systems and key risk indicators.
3. Obligations are typically linked to compliance, representing the degree to which obligations and requirements are met. Compliance is managed using compliance management systems and key compliance indicators.

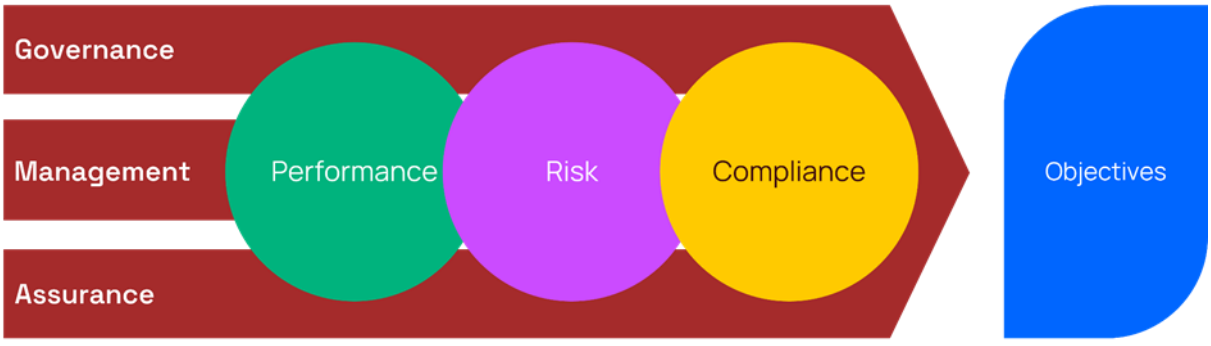

Image 7 - Management, Governance, and Assurance

OCEG (2024) stated that an organization must do more than manage the aspects of performance, risk, and compliance. An organization must also govern and provide assurance around performance (reward), risk, and compliance, thus a complete picture of this approach is the governance, management, and assurance of performance, risk, and compliance, as follows:

1. Management - directly guiding, controlling, and evaluating an entity by arranging and operating resources.
2. Governance - indirectly guiding, controlling, and evaluating an entity by constraining and conscribing resources.
3. Assurance - objectively and competently evaluating subject matter to provide justified conclusions and confidence that statements and beliefs about the subject matter are justified and true.

2.4.2. GRC & Critical Disciplines

According to OCEG (2024), GRC is the "integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty, and act with integrity." GRC is an integration and orchestration of capabilities. It is an umbrella over several Critical Disciplines that share similarities but also have their distinct advantages.

Image 8 - GRC Critical Disciplines by OCEG

1. Governance & Oversight provides methods to guide, constrain and conscribe the organization to achieve its purpose, mission, vision, and values.
2. Strategy & Performance provides methods to guide, arrange and operate resources to achieve objectives and monitor performance.

3. Risk & Decision-Support provides methods to identify and address the e□ect of uncertainty on objectives, including ways to support decisions under uncertainty.
4. Compliance & Ethics provides methods to identify and address mandatory and voluntary obligations and the underlying ethical principles and values.
5. Security & Continuity provides methods to identify and address threats to critical physical and digital assets and infrastructure.
6. Audit & Assurance provides methods to enhance confidence that the organization is reliably achieving objectives, addressing uncertainty, and acting with integrity.

By integrating these disciplines, the unique strengths of each can be used to support the others.

2.4.3. GRC Capability Model Version 3.5

OCEG (2024) developed the GRC capability model that codifies the continuously improving body of knowledge about how GRC works in an organization. There are four (4) components and twenty (20) elements that help an organization ask and answer key questions, such as:

1. LEARN - Who are we? Where are we? What might affect us? Who do we serve? How will they judge us? What is our business model?
2. ALIGN - Where are we going? How will we get there? How will we address the opportunities, obstacles, and obligations along the way?
3. PERFORM - How proactive are we? How do we detect problems and progress? How do we respond to favorable and unfavorable events?
4. REVIEW - Are we making progress? How confident are we? How can we improve?

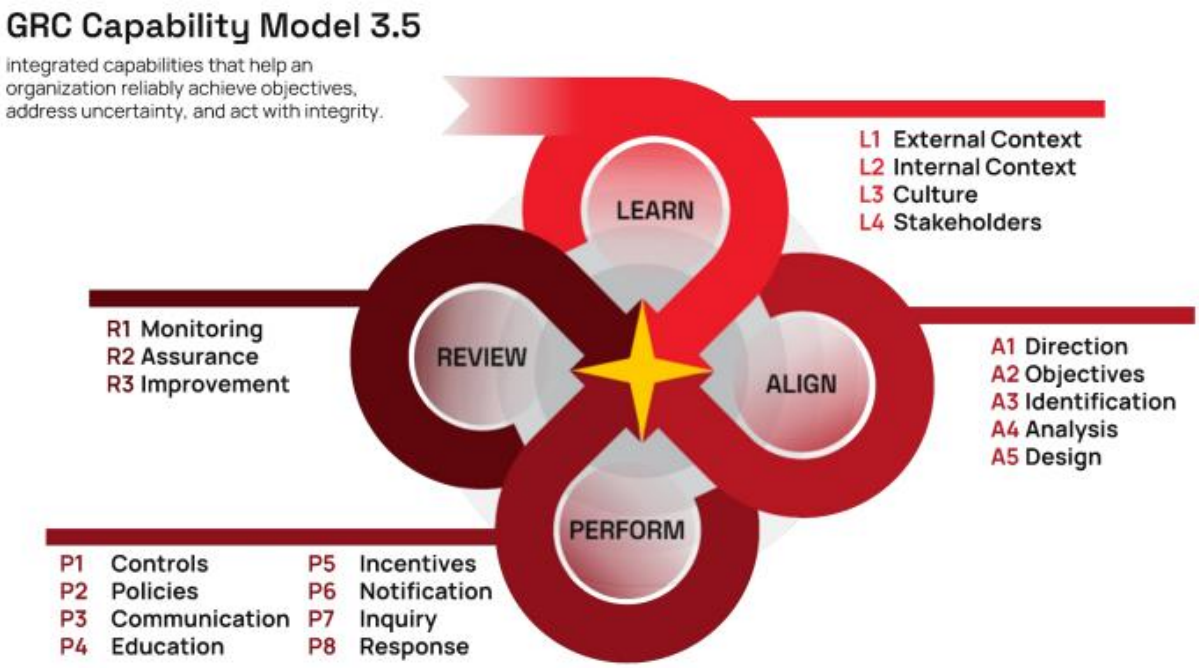

Image 9 - GRC Capability Model Version 3.5

The OCEG GRC Capability Model Version 3.5 is a well-established framework that provides guidance for organizations in enhancing their GRC capabilities. This version incorporates the latest best practices and industry standards, making it a valuable resource for organizations aiming to optimize their GRC processes.

One of the key strengths of the OCEG GRC Capability Model Version 3.5 is its comprehensive approach to GRC, covering areas such as strategy, risk management, compliance, ethics, and performance. By addressing these core components, organizations can develop a holistic understanding of their GRC needs and implement measures to strengthen their overall governance, risk, and compliance framework.

This model also emphasizes the importance of integrating GRC into the organization's overall strategic objectives, fostering alignment between GRC activities and the business's goals. Additionally, it provides a structured approach to identifying and assessing risks, enabling organizations to proactively mitigate potential threats and capitalize on opportunities while remaining compliant with relevant regulations.

Furthermore, the OCEG GRC Capability Model Version 3.5 offers valuable insights for organizations seeking to leverage technology to streamline their GRC processes. By

incorporating technology considerations into the framework, organizations can harness digital tools to enhance their GRC capabilities, improve data analytics for risk assessment, and automate compliance monitoring, leading to greater efficiency and effectiveness in GRC operations.

The OCEG GRC Capability Model Version 3.5 also outlines the significance of fostering a culture of ethics and compliance within the organization. By emphasizing the integration of ethical considerations into GRC activities, the model encourages a proactive approach to ethical behavior, fostering a strong ethical culture within the organization.

Moreover, this capability model underscores the importance of continuous improvement and adaptability in the GRC landscape. It emphasizes the need for organizations to regularly assess and enhance their GRC capabilities to respond to evolving risks, regulations, and business environments. This adaptive approach enables organizations to maintain resilience in the face of dynamic challenges and opportunities.

In conclusion, the OCEG GRC Capability Model Version 3.5 serves as a comprehensive and forward-thinking framework for organizations looking to strengthen their governance, risk, and compliance functions. By addressing key components such as strategy, risk management, compliance, and the integration of technology and ethics, this model equips organizations with the necessary guidance to cultivate robust and agile GRC capabilities.

2.5. Previous Researches on GRC and ERM

Table 1 – Some Previous Researches on GRC and ERM

Research/Journal title	Researcher	Research Results/conclusion	Research Year
Understanding governance, risk and compliance information systems (GRC IS): The experts view	Anastasia Papazafeiropoulou & Konstantina Spanaki	The paper proposes a framework framework of particular GRC characteristics that need to be taken into consideration when these systems are put in place. This framework includes specific areas such as: goals and objectives, purpose of the system, key stakeholders, methodology and requirements prior to implementation, critical success factors and problems/barriers.	2016

Research/Journal title	Researcher	Research Results/conclusion	Research Year
Relevance of GRC in Expanding the Enterprise Risk Management Capabilities	Alina Andronache, Abraham Althonayan & Mandana Matin	The paper suggests a value proposition of integrating GRC into Enterprise Risk Management to increase organizational risk capabilities. The joint approach is suggested to reinforce the effects of Enterprise Risk Management, and last but not least, enable maturity of the concept.	2021
The Importance of GRC in the Enterprise	Gary Long	This paper analyzes the roles of governance, risk, and compliance concepts in an organization. The paper details potential impacts of a poorly implemented GRC program as well as making suggestions to improve the current implementation of GRC concepts within an organization.	2017
Promoting Enterprise Risk Management (ERM) and Governance, Risk and Compliance (GRC) for Managing Cybersecurity Risks	Ward Murray, W Roger	The paper discusses the benefits of ERM and GRC for managing cybersecurity risks and provides a case study of IT GRC and cybersecurity at University of Maryland Baltimore (UMB).	2018
A Conceptual Model for Integrated Governance, Risk, and Compliance	Pedro Vicente, Miguel Mira Da Silva	This paper proposes a set of high-level concepts covering the GRC domain. Through literature review and framework research we propose key functions of governance, risk and compliance and their associations, resulting in a reference conceptual model for integrated GRC. The model was evaluated by comparing the GRC capability model from OCEG with a quality model evaluation framework.	2011
A Framework for Assessing Organisational IT Governance, Risk and Compliance	Mikhel Vunk, Nicolas Mayer, Raimundas Matulevicius	This paper conducts a systematic literature review to understand the processes, roles, strategies, and technologies of IT GRC as well as their integration. Based on the results of the review, the study proposes an assessment framework, which could guide evaluation of the enterprise's IT GRC concerns.	2017
A Context Adaptive Framework for IT Governance, Risk, Compliance and Security	Shree Govindji, Gabrielle Peko, David Sundaram	The paper explores IT GRC and Security and propose an integrated context adaptive framework that addresses the problems of monolithic approaches.	2018

Research/Journal title	Researcher	Research Results/conclusion	Research Year
Toward a New Integrated Approach of Information Security Based on Governance, Risk and Compliance	Mounia Zaydi, Nassereddine Bouchaib	This paper proposes a new integrated approach of information security based on Governance, Risk management and Compliance (ISS-GRC)	2018
A Framework for the Governance of Information Security	Shaun Posthumus, Rossouw von Solms	This paper highlights the importance of protecting an organization's vital business information assets by investigating several fundamental considerations that should be taken into account in this regard. Based on this, it is illustrated that information security should be a priority of executive management, including the Board and CEO and should therefore commence as a corporate governance responsibility	2008
Culture in business process management: A literature review	Jan vom Brocke & Theresa Schmiedel	The paper investigates the role of GRC in BPM and proposes a conceptual model of GRC-BPM alignment. It also provides a case study of GRC-BPM alignment in a financial services company.	2011
A Maturity Model for Governance, Risk Management and Compliance in Hospitals	Ronald Batenburg, Matthijs Neppelenbroek, & Abbas Shahim	The paper proposes a preliminary model (hereafter referred to as maturity model) to assess and monitor Governance, risk and compliance (GRC) and GRC maturity in Dutch hospitals. The paper develops a maturity model for GRC in hospitals based on 14 dimensions.	2014
The Impact of Enterprise Risk Management on Firm Performance: A Meta-Analysis	Amiril Azizah, Ahyar M. Diah, Ratna Wulaningrum	The paper investigates whether there is relationship between risk management and firm performance. Risk disclosure and leverage are the measurements of risk management. Both the variables of risk management have a relationship to increase firm performance.	2022
Enterprise Risk Management and Firm Value within China's Insurance Industry	Qiuying Li, Yue Wu, Udechukwu Ojiako & Alasdair Marshall	The paper examines the impact of ERM on firm value in China's insurance industry. It finds that ERM adoption is positively associated with firm value. The results show the relationship between ERM and firm value at first appears statistically significant within a Pearson correlation matrix but then falls below statistical significance on closer scrutiny through regression analysis. Accordingly, it is	2014

Research/Journal title	Researcher	Research Results/conclusion	Research Year
		recommended that insurers in China should not look to aggressive investment in ERM as a strategy for producing quick gains in firm value	
The Effect of Enterprise Risk Management on Financial Performance: Evidence from the Turkish Insurance Sector	Zekai Senol & Suleyman Serdar Karaca	This study attempts to determine the effect of ERM on firms' financial performance and the determinants of ERM. In panel data analysis, it was seen that the effects of ERM on firm performance were not determined, whereas in the panel logistic regression, firm size was found to be determinant of ERM applications	2017
Corporate governance perspective on enterprise risk management and organizational sustainability	John Nkeobuna Nnah Ugoani	The study was designed to explore the relationship between enterprise risk management and organizational sustainability. Enterprises can only meet the generational intention of founders when they are properly managed exemplified by sustainable performance. Data generated and analyzed through statistical techniques, showed strong positive relationship between enterprise risk management and organizational sustainability. It was recommended that complex organizations must establish good corporate governance structure to promote enterprise risk management and organizational sustainability	2021
GRC360: A framework to help organisations drive principled performance	Scott Mitchell	This paper discusses the concept of principled performance as the clear articulation of an enterprise's financial and non-financial objectives and the boundaries it will observe as it drives toward them. It discusses the GRC360 Framework as a vehicle for organisations to drive and attain principled performance.	2011

CHAPTER 3
RESEARCH METHODOLOGY

3.1. Research Design

This research study adopts a qualitative case study approach to investigate the evaluation of Company X's implementation of an integrated Governance, Risk, and Compliance to enhance its enterprise risk management. Through this methodology, data will be collected via semi-structured interviews and document analysis to gain insights into the organization's current GRC practices, challenges faced during implementation, and the overall impact on enterprise risk management, thereby allowing for a nuanced understanding of how integrated GRC can contribute to improved risk management. Furthermore, the study aims to identify the capabilities that Company X has developed in relation to the GRC framework, which are essential for aligning their risk management processes with organizational objectives and compliance requirements, ultimately shedding light on the effectiveness of the current practices and areas for improvement. In addition to qualitative data collection methods, the research will also incorporate analysis of Company X's strategic alignment with the GRC framework, assessing how the implementation of integrated GRC has facilitated a more cohesive approach to risk management and compliance, which aligns with the organization's overall strategic goals. This alignment is particularly critical as it enables Company X to harness the integrated nature of GRC, allowing for a comprehensive assessment of risks across various business domains while promoting a culture of compliance and ethical behavior within the organization, which ultimately fosters an environment conducive to effective enterprise risk management.

This case study approach is well-suited for this research as it allows for an in-depth look at how Company X has implemented its integrated GRC system in the real world. By giving the researchers a comprehensive understanding of the processes, interactions, and outcomes involved, this method can uncover the complexities and nuances that may be missed in a more quantitative study. This can shed light on how governance, risk, and compliance work together within the company, ultimately providing valuable insights that can guide best practices for other organizations looking to strengthen their risk management through integrated GRC strategies. The focus on qualitative data collection and analysis not only deepens the

understanding of Company X's specific challenges but also captures the broader impacts of integrated GRC systems in helping organizations stay agile and resilient in the face of today's rapidly changing business environment. Additionally, by using qualitative methodologies, this research aims to gain insights into the perspectives of various stakeholders involved in the GRC processes, highlighting their roles, experiences, and views on the effectiveness of the implementation strategies in achieving the organization's objectives, contributing to a more comprehensive understanding of the subject matter.

3.2. Data Collection Method

In order to collect relevant and reliable data for this study, a variety of data collection methods will be employed. These methods include:

1. In-depth Interviews: Semi-structured interviews with key stakeholders will be conducted. The semi-structured interviews will allow for a flexible yet focused dialogue with participants, enabling the collection of rich, qualitative data regarding their experiences and insights related to the GRC implementation.
2. Document Analysis: A thorough analysis of relevant documents, such as risk management policies, standard operating procedures (SOP), and reports, will be conducted to understand the existing practices and the documented challenges and benefits of GRC integration. The document analysis will provide foundational context and historical data on the organization's GRC practices, as well as its strategic objectives.
3. Observation: Observations of GRC-related activities, decision-making processes, and risk management activities will be undertaken to gain a firsthand understanding of how GRC is integrated into the organization's risk management practices.

By utilizing these data collection methods, this study aims to capture a comprehensive picture of Company X's GRC implementation and its impact on enterprise risk management. The findings from this study will not only contribute to the existing body of knowledge on GRC integration and enterprise risk management but also provide valuable insights and practical recommendations for other organizations seeking to enhance their GRC practices.

3.3. Research Sample and Participants

The research participants for this study will be drawn from various levels of management within Company X, including senior leaders and operational leaders. This stratified sampling approach ensures that a diverse range of perspectives and insights is captured, reflecting the complex dynamics involved in the GRC activities across the organization.

3.4. Data Analysis Techniques

The research adopts Design Review Procedure from OCEG Burgundy Book as a framework to evaluate GRC practices of Company X. This methodology provides a structured approach to assess the design and implementation of an organization's GRC program by examining the GRC capability, which consists of 4 components and 20 elements:

3.4.1 LEARN

This component involves examining and analyzing context, culture, and stakeholders to learn what the organization needs to know to establish and support objectives and strategies. The LEARN component has 4 elements. The parameters to be assessed for each element are as follows:

1. **L1 – External Context:**

   To learn more about Company X's understanding of the external business environment in which it operates, the impact of external factors on the company's operations, and how it responds to these factors. The following points to be assessed in this research:

   1) The Company’s approach to understanding and discerning opportunities to shape the external context, including influencing requirements derived from the following forces:

      a. Industry (competitors, supply chain, labor markets, etc.)

      b. Market (customer demographics, economic conditions, etc.)

      c. Technology (technological shifts and breakthroughs, etc.)

d. Society (community needs, media trends, etc.)

e. Regulatory environment

f. Geopolitical environment (current enforcement posture, etc.)

2) The ways in which the personnel stay in the loop about changes to the external context, has taken external factors into consideration and adapted; based on an understanding of external forces.

3) The frequency of planned or scheduled analysis of external forces and the key events and triggers that prompt reassessment of the external context.

2. L2 – Internal Context

To learn more about Company X's understanding of the internal business environment in which it operates, the impact of internal factors on the company's operations, and how it responds to these factors. The following points to be assessed in this research:

1) The Company's approach to understanding the internal context and changes thereto, including the following attributes:

   a. Goals, business objectives, and values
   b. Organizational structure
   c. Key human capital assets
   d. Technology assets
   e. Information assets
   f. Physical assets
   g. Business processes
   h. Products and services

2) The ways in which Company X has adapted to consider effective measures based on changes to relevant internal factors.

3) The frequency of planned or scheduled analysis and the key events and triggers that prompt reassessment of the internal context.

4) Communication and reporting plan for change or transformation function.

3. **L3 – Culture**

   To assess the existing culture, including how leadership models culture, the organizational climate, and individual mindsets about the governance, assurance, and management of performance, risk, and compliance. The following points to be assessed in this research:

   1) The ways in which Company X has adapted to take into consideration what would be effective given the existing cultural factors; and, how the Company plans to change aspects of the culture, if needed, over what period of time and how such change is to be monitored/measured.

   2) The process for monitoring cultural indicators, including what indicators are monitored, frequency of monitoring, and action triggers.

4. **L4 – Stakeholders**

   1) The approach to monitoring key authorities, stakeholders, and influencers including how changes to requirements, rewards, cultural norms, the risk environment and conformance are recognized and communicated for purposes of risk analysis.

   2) The process for developing and maintaining the Communication and Reporting Plan including how contact with stakeholders is controlled to ensure all communications and reports are included.

   3) Segregation of duties matrix.

3.4.2. ALIGN

This component involves aligning performance, risk, and compliance objectives, strategies, decision- making criteria, actions, and controls with the context, culture, and stakeholder

requirements. The ALIGN component has 5 elements. The parameters to be assessed for each element are as follows:

1. **A1 – Direction**

   To assess if Company X has clear mission, vision and values statements, high-level objectives, as well as guidance about how decisions will be made. The following points to be assessed in this research:

   1) The process of aligning GRC initiatives with organizational mission, vision, and values.
   2) PDCA cycle implementation and how GRC initiatives are integrated into the PDCA cycle, especially for all aspects of the plan.
   3) Charter related to GRC capability.
   4) Ways in which the GRC implementation is championed / endorsed by the top management or oversight authority and management.

2. **A2 - Objectives**

   To assess if Company X has a balanced set of measurable objectives that are consistent with decision-making criteria and appropriate for the established frame of reference. The following points to be assessed in this research:

   1) The process of mapping the capability objectives to organizational objectives.
   2) The contribution of the GRC metrics to the measures tracking progress on organizational objectives.
   3) The method how GRC capability incorporates the prioritization of objectives into capability design, risk prioritization, and prioritization of initiatives in the Integrated Plan.

3. **A3 – Identification**

To assess how Company X conduct identification of forces that may cause desirable (opportunity) or undesirable (threat) effects on the achievement of objectives. The following points to be assessed in this research:

1) The methodology(ies) / process(es) used to identify applicable laws, rules, regulations, and standards to which the firm has represented compliance or by industry practices must adhere to maintain presence in the market (requirements).
2) The methodology(ies) / process(es) used to identify other sources of risks (threats) which create potential obstacles to business success.
3) The methodology(ies) / process(es) used to identify potential desirable effects (opportunities) on the achievement of business objectives.
4) The methodologies / process(es) used to manage changes to the Risk / Control Matrix based upon changes to the sources of opportunities, threats and requirements.
5) The process for assigning responsibility to an individual or department for monitoring each identified risk, reward and requirements.

4. A4 – Analysis

To assess how Company X conduct analysis on current and planned approach to address opportunities, threats and requirements using decision-making criteria with quantitative and qualitative methods. The following points to be assessed in this research:

1) The process for analyzing risks, rewards, and conformance, creating applicable profiles, and assigning optimization strategies to each threat, opportunity and requirement.
2) If multiple assessment methodologies are used, describe the process used to consolidate/translate and compare the analytical information produced.
3) The process for assigning priorities to each risk, reward, and requirement identified.

5. **A5 – Design**

   To assess how Company X develops strategic and tactical plans to achieve the objectives, while addressing uncertainty and acting with integrity, consistent with decision-making criteria. The following points to be assessed in this research:

   1) The process utilized to design the GRC capability and its measurement, including development of the GRC Business Case, GRC Strategic Plan, and GRC Assessment Plan.
   2) The process for designing, implementing, and maintaining the Third- Party Risk Management Plan.
   3) The process utilized to design the GRC Technology Plan and to integrate GRC technology solutions with the organizational technology plan including the degree of information sharing and collaboration.

3.4.3. PERFORM

This component involves addressing threats, opportunities, and requirements by encouraging desired conduct and events, and preventing what is undesired, through the application of proactive, detective, and responsive actions and controls. The PERFORM component has 8 elements. The parameters to be assessed for each element are as follows:

1. **P1 – Controls**

   To assess if Company X has established a mix of management, process, human capital, technology, information, and physical actions and controls that serve governance, management, and assurance needs. The following points to be assessed:

   1) Proactive Actions and Controls:

      a. The process defining and modifying proactive, detective, and responsive actions and controls.

b. Background check methodology for hiring and promotion.

c. The key actions and controls implemented as part of your ongoing third-party oversight program (e.g., vendor and/or partners oversight), including organizational and individual due diligence during the entire relationship life cycle and any variances depending on physical presence or technological access.

2) Detective Actions and Controls: The process utilized to determine appropriate detective controls, including:

a. Authority to determine application of detective controls (human capital, process, physical, and technology).

b. Criteria for determining the utilization, intensity, and frequency of a detective control.

c. Criteria for determining which detective controls will be monitored for proper application.

d. Criteria for aggregation and reporting of information gathered by detective controls.

3) Responsive Actions and Controls

The process for monitoring detected undesirable conduct, events and conditions and capability failures until corrective action has been implemented, including reporting on completion of such actions.

2. P2 – Policies

To assess if Company X has implemented policies and associated procedures to address opportunities, threats and requirements and set clear expectations of conduct for the governing authority, management, and the workforce. The following points to be assessed:

1) The process for developing, implementing, maintaining, and enforcing throughout the workforce and extended enterprise, including the molding of champions and securing buy-in to:
    - The Code of Conduct;
    - Any Ethical Decision Guidelines;
    - Policies; and
    - Procedures
2) The process used by management to inform the board regarding workforce (including all employees) commitment to and adherence to the Code of Conduct, including:
    - Percentage of personnel that received the code
    - Percentage that have received training on the code
    - Percentage that have confirmed receipt and understanding
    - Passage rate statistics on any assessments of understanding
    - Number of code of conduct violations remediated by various types of responsive actions or controls
    - Dollar value of losses experienced from violations, and
    - Dollar value of rewards for adherence to violation reporting.

3. P3 – Communication

To assess the process for developing and maintaining the Communication and Reporting Plan including how contact with stakeholders is controlled and recorded to ensure all communications and reports are included.

4. P4 – Education

To assess the governing authority, management, the workforce, and the extended enterprise about expected conduct, and increase the skills and motivation needed to help the organization address opportunities, threats, and requirements, including:

a) The components of the organization's GRC awareness and education plan.

b) The assessment tools used to measure awareness, training, knowledge, support, and understanding of the policies, procedures, and code(s) of conduct by all target recipient groups.

c) The procedure used to train and confirm that individuals understand how to report an issue (i.e., incident, concern, inquiry) including the curriculum required and the frequency of refresher training.

5. P5 – Incentives

To assess if Company X has implemented incentives that motivate desired conduct and recognize those who contribute to positive outcomes to reinforce desired conduct, including:

1) The process used during the past year to recognize and reward individuals for exhibiting ethical conduct.

2) The ways in which adherence to ethical conduct expectations and organizational values are considered during hiring, promotion and compensation decisions.

6. P6 – Notification

To assess if Company X has provided multiple pathways to report progress toward objectives, and the actual or potential occurrence of undesirable and desirable conduct, conditions, and events by evaluating the process (test data, real time supervisory monitoring, electronic monitoring, and analytical procedures) for monitoring issue notification (intake), filtering, and management activities to determine that the applicable policies and procedures are consistently applied.

7. P7 – Inquiry

To assess if Company X has periodically analyzed data and seek input about progress towards objectives; and the existence of undesirable conduct, conditions and event by evaluating the workforce and stakeholder feedback process, including all procedures used routinely to ask stakeholders throughout the extended enterprise.

8. **P8 - Response**

   To assess if Company X has designed and, when necessary executed responses to identified or suspected undesirable conduction, conditions, events, or weaknesses in capabilities, including investigation processes, crisis situation, and resolution processes.

3.4.4. REVIEW

This component involves conducting activities to monitor and improve design and operating effectiveness of all actions and controls, including its continued alignment to objectives and strategies. The REVIEW component has 3 elements, as follows:

1. **R1 – Monitoring**

   To assess if Company X has monitored and periodically evaluated the performance of the capability to ensure it is designed and operated to be effective, efficient, and responsive to change by reviewing the process utilized to evaluate the design and performance of the GRC capability during the past three (3) years and the current year to date explaining any changes or improvements implemented during that period and how information from prior and subsequent years are compared and reconciled to assess trends.

2. **R2 - Assurance**

   To assess if Company X has provided assurance to management, the governing authority, and other stakeholders that the capability is reliable, effective, efficient and responsive. The following points to be assessed:

   1) The process for determining which portions of the capability will be audited in any given year and by whom (internal auditors or external auditors).

2) The process followed to ensure the objectivity, independence, and competency of internal and external auditors assigned to GRC capability engagements.

3. R3 - Improvement

To assess if Company X has reviewed information from periodic evaluations, detective and responsive actions and controls, monitoring, and assurance to identify opportunities for continuous improvements. The following points to be assessed:

1) The methodology used to continuously improve the GRC capability, including the process for identifying, prioritizing, managing, and reporting improvement initiatives for incorporation into the Integrated Plan.
2) The process for incorporating the recommendations of investigations and other issue resolutions into the GRC capability Improvement process.

CHAPTER 4
COMPANY X PROFILE

4.1. Company X Overview

Company X is one of the Strategic Business Unit (SBU) of the largest publicly listed pharmaceutical company in Southeast Asia. Company X manufactures and markets health-related consumer products including supplements and other preventative products. The company is based in Jakarta, Indonesia and it has established its footprint in other ASEAN countries (Singapore, Malaysia, Myanmar, and Cambodia) and Africa countries (Nigeria and South Africa), positioning Company X as a national pharmaceutical company with a competitive edge in the export market.

For over 27 years, Company X has been a trusted choice for families and the community. Company X provides the best health product options and quality. The Company provides Over-The-Counter (OTC) drugs with therapeutic benefits. Company X's OTC portfolio categories cover more than six therapeutical classes, with solid brands holding a dominant market share in recent decades. Innovation is the key to Company's success, and it remains committed to nourishing the nation, which it strives for together. The Company offers a variety of health products including digestive & skin, multivitamins, and respiratory care. The Company provides innovative and trustworthy products and services as a solution for daily health management.

4.2. Overview of OTC Industry in Indonesia

4.2.1 Market Overview

The Over-The-Counter (OTC) drugs market in Indonesia is a vital segment of the country's pharmaceutical industry, catering to the healthcare needs of a large and diverse population. OTC drugs are medications that can be purchased without a prescription, including common

products like pain relievers, cold and flu remedies, digestive aids, vitamins, and skincare products. This market segment plays a crucial role in providing accessible and convenient healthcare solutions to consumers across Indonesia.

4.2.2. Market Dynamics

1. **Market Size and Growth**

   The OTC drugs market in Indonesia has been experiencing steady growth in recent years, driven by factors such as increasing health awareness, rising disposable incomes, and changes in consumer behavior towards self-care and self-medication.

2. **Consumer Behavior**

   Indonesian consumers are increasingly turning to OTC drugs for managing minor health issues and preventive care. Factors like convenience, affordability, and easy availability contribute to the growing popularity of OTC products.

3. **Regulatory Environment**

   The Indonesian government plays a significant role in regulating the OTC drugs market to ensure product safety, quality, and efficacy. Regulations governing the sale, distribution, and advertising of OTC drugs help maintain standards and protect consumer health.

4.2.3. Key Drivers

1. **Growing Health Awareness**

   Rising health consciousness among Indonesians is leading to increased demand for OTC drugs as consumers seek to take control of their health and well-being.

2. **Urbanization and Lifestyle Changes**

   Rapid urbanization and changing lifestyles are influencing health behaviors, with more people opting for self-medication and OTC remedies for common health issues.

3. **Economic Development**

Indonesia's improving economic conditions and expanding middle-class population are driving greater spending on healthcare products, including OTC drugs.

4.2.4. Market Trends

1. **Digitalization**

   The digital transformation of the healthcare industry has impacted the OTC market, with the rise of e-commerce platforms and online pharmacies offering consumers convenient access to a wide range of OTC products.

2. **Herbal and Natural Products**

   There is a growing preference for herbal and natural OTC products in Indonesia, driven by a shift towards holistic health and wellness practices.

3. **Product Innovation**

   Companies are investing in research and development to introduce innovative OTC products with improved formulations, better efficacy, and unique selling points to attract consumers.

4. **Health and Wellness Trends**

   Increasing focus on preventive healthcare, dietary supplements, and lifestyle-related OTC products reflects broader health and wellness trends in the Indonesian market.

4.2.5. Challenges

1. **Regulatory Compliance**

   Navigating the complex regulatory landscape and ensuring compliance with evolving regulations can pose challenges for companies operating in the OTC drugs market.

2. **Counterfeit Products**

   The presence of counterfeit and substandard OTC drugs remains a significant concern, impacting consumer trust, safety, and the overall reputation of the industry.

3. **Distribution Challenges**

   Establishing efficient distribution networks to reach remote and underserved areas of Indonesia can be a logistical challenge for OTC drug manufacturers and distributors.

4. **Competition**

   The OTC drugs market in Indonesia is highly competitive, with local and international players vying for market share through aggressive marketing, product differentiation, and pricing strategies.

4.2.6. Major Players

1. **Kalbe Farma**

   A leading Indonesian pharmaceutical company with a diverse portfolio of OTC products and a strong market presence.

2. **Kimia Farma**

   A well-established state-owned enterprise involved in the production and distribution of a wide range of OTC drugs.

3. **Sanbe Farma**

   Known for its innovation and quality, Sanbe Farma offers various OTC products and has a strong market reputation.

4. **International Brands**

   Companies like Johnson & Johnson, GlaxoSmithKline, P&G, and Bayer have a significant presence, bringing global expertise and trusted brands to the Indonesian market.

4.2.7. Distribution Channels

1. **Pharmacies and Drugstores**

   These are the primary channels for OTC drug distribution, providing consumers with easy access to a wide range of products.

2. **Convenience Stores and Supermarket**

   Increasingly popular for OTC purchases, these outlets offer convenience and accessibility, catering to urban consumers.

3. **Online Platforms**

   E-commerce and online pharmacies are rapidly growing, offering a convenient option for purchasing OTC drugs, especially among tech-savvy consumers.

4. **Traditional Markets**

   In rural and remote areas, traditional markets still play a crucial role in distributing OTC drugs, though they may have limited product ranges.

4.2.8. Marketing Strategy

1. **Consumer Education**

   Companies are investing in consumer education campaigns to raise awareness about the benefits and correct use of OTC drugs.

2. **Branding and Advertising**

   Strong branding and advertising campaigns are essential to differentiate products in a competitive market and build consumer trust.

3. **Partnerships and Collaborations**

   Collaborations with healthcare professionals and partnerships with retail chains help expand reach and credibility.

4.2.9. Future Outlook

The OTC drugs market in Indonesia is poised for continued growth, driven by demographic trends, economic development, and increased health consciousness. Companies are likely to focus on:

1. **Expanding Product Portfolios**

   Developing new products and expanding existing lines to meet diverse consumer needs and preferences.

2. **Enhancing Distribution Networks**

   Improving logistics and distribution to ensure wider availability of OTC products across urban and rural areas.

3. **Leveraging Technology**

   Utilizing digital platforms and data analytics to better understand consumer behavior and optimize marketing strategies.

4. **Ensuring Quality and Safety**

   Addressing counterfeit issues and maintaining high standards of product safety and efficacy to build consumer trust.

4.3. Company X's Values and Purpose

The Company X's values are based on the following principles:

1. **Trust –** with mutual trust and respect, and by upholding openness and honesty, manage the company to deliver the very best for all
2. **Mindfulness –** mindfulness is the foundation to take actions that are consistent with the Company's values in order to always be responsive to the needs of all stakeholders, society, and the environment
3. **Innovation –** starting from simplicity combined with a spirit to sustainable innovation, grow to improve quality of life
4. **Strive -** provide equal opportunity to every individual to develop their potentials and become a reliable human being throughout the culture of continuous learning and improvement
5. **Interconnectedness –** as part of life, maintain diversity and harmony by making efforts that are useful to others and to the future generations.

Company X's purpose is "Empowering health for a meaningful life". The purpose "Empowering health for a meaningful life" for an over-the-counter (OTC) company reflects a

commitment to enhancing individuals' well-being and overall quality of life through accessible health products. Here's a breakdown of its meaning:

1. **Empowering Health:** This emphasizes the company's role in providing consumers with the tools, information, and products necessary for managing their health proactively. It suggests a focus on enabling people to make informed choices about their health and wellness.
2. **For a Meaningful Life:** This part highlights that the ultimate aim of promoting health is to enhance life satisfaction and overall happiness. It signifies that health is not just about the absence of illness but also about the ability to engage fully in life, pursue goals, and maintain relationships.

Overall, this purpose indicates that the OTC company values not only the effectiveness of its products but also the broader impact they have on improving people's lives, fostering independence, and supporting a holistic approach to health. The company strives to be a partner in helping individuals achieve a fulfilling and healthy lifestyle.

4.4. Business Performance

In 2023, Company X reached net sales at IDR 2.05 trillion with achievement 84.1% of target and minus growth at -10.8% compared to last year. Sales of Company X in 2023 is underperformed and recorded minus growth due to declining sales volume in Indonesia and unstable performances in African countries.

In terms of profitability, in 2023 Company X still records good profitability with operating profit at IDR 673 billion or operating profit-to-net sales ratio at 32.8%. Although the operating profit only achieves 83.2% of budget with minus growth at -11%

4.5. Organizational structure

Company X has a lean organization structure with total number of employees around 370 employees. The below chart shows the core organizational structure at Company X. There are 9 Departments that operate under the President Director. The structure is quite in line with the business process mapping at Company X.

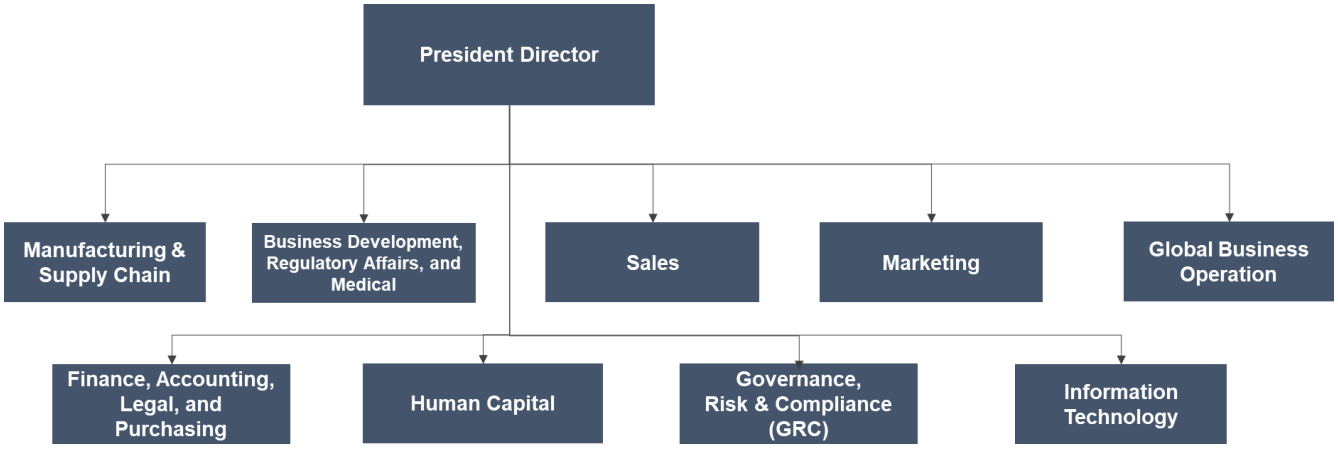

Image 10 – Core Organizational Structure at Company X

4.6. Business Process Mapping (BPM)

The below image is the business process mapping for Company X that shows its main business processes as well as the supporting business processes.

Image 11 – Company X's Business Process Mapping

There are 7 main processes at Company X, which are:

1. Business development, regulatory affairs, and medical
2. Inbound logistics

3. Production
4. Outbound logistics – for distribution (product delivery from warehouse to customers), it is not part of the main process at Company X because the distribution is handled by Company X's sister company.
5. Marketing
6. Sales, and
7. Global business operations, which include marketing and sales functions for global countries outside Indonesia (i.e., ASEAN and Africa countries)

Meanwhile, there are 7 supporting processes at Company X, as follows:

1. Human capital
2. Information technology
3. Quality operations
4. Management system, risk management, and internal audit, which are included in the Governance, Risk, and Compliance Department
5. Finance, accounting, and tax
6. Legal
7. Purchasing

4.7. Current Business Situation & Complication

1. Global OTC market is predicted to grow with a CAGR of 3.8% by 2028. Globally, OTC market is dominated by the curative category with a contribution of ±80% (source: IQVIA estimation).
2. Preventive category (growth +5.4%) is growing faster than the curative category (growth +3.3%), driven by the consumers' more health consciousness and promoting preventive lifestyle (source: IQVIA estimation).

3. Company X has high dependence on curative categories and the product format is still conventional (in 2023 curative category contribution: 94%, preventive category contribution: 6%)
4. Fragmented market with low single-digit business growth.
5. Stricter regulation in Indonesia both in terms of product quality and product distribution, especially for curative category, impacting to increase in manufacturing cost, distribution cost, and decrease in numeric distribution.
6. International (global) business is relatively small with contribution less than 20% to the total Company X business, of which 62% come from unstable countries and 95% of the business relies on single category (Respiratory Care).
7. Manual processes in several areas, which lead to inefficient operations/processes, data silo, and fraud.
8. High good employee turnover rate (Company X: 8.3%; Target: 4%)
9. Low achievement of new product sales with small contribution to total Company X business (Ctr. 2.8%)

4.8. Strategic Directions

Company X has the following strategic directions for the next five years (2024-2029):

1. Improve product competitiveness and increase NBC by strengthening core products' efficacies, expanding herbal categories, tapping into wellness category, and strengthening distribution.
2. Global strong foothold through Category Expansion (while strengthening the existing RC categories) and Country Expansion.
3. Improve efficiency through Operational Excellence improvements and optimizing manufacture utilization.
4. Strengthen talents by improving key competencies needed and improving retention & succession programs.

5. Accelerate digital transformation by improving business processes in all areas (commercial, supporting function, and manufacturing), improving data analytics, and strengthening data protection & privacy.

CHAPTER 5
DISCUSSION AND RECOMMENDATION

In this chapter, the analysis and findings of the research on the implementation of Integrated Governance, Risk, and Compliance to enhance Company X's Enterprise Risk Management will be discussed.

The research adopts Design Review Procedure from OCEG Burgundy Book as a framework to evaluate GRC practices of Company X. This methodology provides a structured approach to assess the design and implementation of an organization's GRC program by examining the GRC capability, which consists of 4 components and 20 elements.

5.1. LEARN Component Analysis at Company X

This section discusses the GRC capability related to examining and analyzing context, culture, and stakeholders to learn what the organization needs to know to establish and support objectives and strategies.

L1 - External Context Element at Company X

Company X operates in a highly regulated industry that requires compliance with various laws and regulations, such as product quality, pricing, distribution, and marketing standards. At Company X, the external context analysis includes the assessment of the company's regulatory environment, industry trends, and economic factors. The findings from the external context assessment are used to identify risks and opportunities that may impact the company's ability to achieve its objectives.

The regulatory environment in the healthcare industry is constantly evolving, with new regulations and guidelines being introduced. Company X closely monitors changes in regulations, both at the national and international levels and assesses the potential impact on its operations.

There are two major functions at Company X that are responsible for monitoring and analyzing external context: the Regulatory Affairs and the Consumer Insight Divisions. The Regulatory Affairs Division is responsible for tracking and ensuring compliance with all relevant

regulations, while the Consumer Insight Division conducts market research to understand industry trends and consumer preferences. Risk Management team works closely with these two functions to integrate the findings from the external context assessment into the company's overall risk management strategy.

What went well:

1. Company X has dedicated teams/functions responsible for monitoring the external context, including the regulatory environment, industry trends, and economic factors, and assessing their potential impact on the business.
2. The findings from the comprehensive external context assessment are used to inform the company's strategic planning process and identify risks and opportunities that may affect the achievement of its objectives.
3. There is a clear, well-established process in place for identifying and addressing changes in relevant laws, regulations, and guidelines at both the national and international levels.
4. Solid mechanisms to share insights and learnings from the external context analysis across the organization are in place through regular management reviews and other structured communication channels.
5. There are structured, data-driven approaches to analyze industry trends, consumer behavior, and other relevant market dynamics to inform decision-making and strategic initiatives.

Improvement Opportunities:

1. The process for collecting and analyzing external context information could be further streamlined and integrated to improve decision-making by leveraging data analytics and automating certain data collection and analysis tasks. This would enable faster and more efficient processing of relevant information to support timely and informed decision-making (Azhar and Rahadian 2022).
2. The insights from external context analysis could be more systematically and proactively shared with functional teams to inform their risk assessments and mitigation plans. This could involve establishing regular briefing sessions, creating a centralized knowledge repository, and defining clear communication protocols to ensure critical

insights are effectively disseminated across the organization (Francis and Paladino 2008).

3. A more formal and comprehensive approach to horizon scanning and emerging risk identification could be beneficial to enhance the company's ability to anticipate and prepare for future challenges. This could include implementing a structured process to regularly review and assess emerging trends, technologies, and potential disruptions that may impact the business (Griffy- Brown et al. 2019).
4. Increased collaboration between the Regulatory Affairs, Consumer Insight, and Risk Management Divisions could lead to a more holistic understanding of the external environment. By regularly sharing information, insights, and concerns, these teams could develop a more comprehensive view of the company's operating context and identify potential areas of convergence or conflict (Ross and Beath 2007).
5. The framework for assessing the potential impact of external changes on the company's objectives and strategies could be further enhanced by incorporating more sophisticated analytical tools, stress testing scenarios, and cross-functional reviews. This would strengthen the company's ability to anticipate and respond to changes in the external environment in a timely and effective manner (Ghezzi 2013).

L2 - Internal Context Element at Company X

1. Company X has a well-established process for assessing its internal context, which includes an evaluation of the following aspects:
2. Goals, business objectives, and values: Company X has clearly defined its strategic goals, business objectives, and core values, which are well-understood and aligned throughout the organization. Company X’s purpose is “Empowering health for a meaningful life” with mission “To be the no.1 innovative & sustainable self-healthcare company offering top-to-toe health solutions”
3. Organizational structure: The organizational structure at Company X is hierarchical, with clear reporting lines and responsibilities. The company has functional departments which are:

a) Manufacturing & Supply Chain,

b) Business Development, Regulatory Affairs, and Medical

c) Sales

d) Marketing

e) Global Business Operations

f) Finance, Accounting, Legal, and Purchasing

g) Human Capital

h) Governance, Risk, and Compliance

i) Information Technology

This structure enables effective decision-making and accountability while allowing for specialization and expertise in key areas. Each department has a well-defined role and set of responsibilities, and there are mechanisms in place for cross-functional collaboration and information sharing.

4. Key human capital assets: The company has a strong workforce with good expertise and experience in the healthcare and FMCG industries. The company has invested in training and developing its employees to ensure they have the necessary skills and knowledge to drive innovation and deliver high-quality products and services.

5. Technology assets: Company X has made investments in its technology infrastructure, including enterprise resource planning systems, supply chain management software, and data analytics capabilities. All the digital transformation projects are governed and monitored by Digital Transformation Committee.

6. Information assets: The organization has well-established processes and systems to capture, manage and leverage its information assets, including product data, customer information, market intelligence, and industry trends.

7. Physical assets: Company X's production facilities and office spaces are designed to support its operational requirements and sustainability objectives.

8. Business processes: The company has documented and standardized its core business processes across functions, which contributes to operational efficiency and consistency. Risk Management team regularly review and update the business process map as per the evolving business needs.

9. Products and services: Company X offers a diverse portfolio of over-the-counter medical products, which cater to the diverse needs of its customers. There are four lines of product categories: Digestive, Respiratory Care, Vitamin & Supplements, and Skin. The curative product categories make up the largest portion of the business, while the preventive product categories still account for the smallest share. This highlights an opportunity to further invest in and promote the preventive healthcare solutions, which could drive future growth and better serve the evolving needs of the customer base.

10. Adaptation to internal changes: The company has a track record of successfully navigating internal changes, such as organizational restructuring, process improvements, and the integration of new technologies.

11. Communication and reporting plan for change: Company X has defined formal channels and protocols for communicating changes and initiatives, both top-down and bottom-up, which helps to ensure alignment and engagement across the organization. The monthly and quarterly business reviews, weekly commercial meeting, and monthly departmental meetings are some of the key forums for internal communication and reporting.

What went well:

1. The assessment highlighted the key strengths and capabilities of Company X, including its clear strategic direction, well-established organizational structure, talent management practices, technology infrastructure, and standardized business processes - all of which contribute to its operational efficiency and ability to adapt to change.

2. The analysis provided a comprehensive view of the company's internal context by examining various aspects such as goals, organizational structure, human capital, technology, information assets, physical assets, business processes, product portfolio, and adaptation to internal changes.

3. The identification of the opportunity to further invest in preventive healthcare solutions aligns with the evolving market trends and customer needs, and could potentially drive future growth for the company.
4. The evaluation of internal context is conducted in a systematic manner using framework of PICAPA (Problem Identification Corrective Action Preventive Action) which provides a structured approach to assess the company's readiness for implementing the integrated GRC framework.
5. The evaluation of internal context aligns with PDCA cycle, which is a widely accepted framework for continuous improvement.

Improvement Opportunities:

1. While the evaluation covers a broad range of internal aspects, it could be further strengthened by including a more detailed assessment of the company's risk management practices, particularly in the context of the goal to enhance its enterprise risk management (Antikarov 2012).
2. The analysis could be enhanced by incorporating a more robust assessment of the company's stakeholder landscape, including customers, suppliers, regulatory bodies, and other external parties, as they can significantly influence the implementation and efficacy of the integrated GRC framework.
3. The evaluation could be complemented by a benchmarking exercise to compare Company X's internal capabilities and practices with industry peers or best-in-class organizations, which could help identify additional areas for improvement (Papazafeiropoulou and Spanaki 2015).
4. The analysis could be further strengthened by incorporating a more detailed assessment of the potential risks and challenges associated with the implementation of the integrated GRC framework, and how the company plans to mitigate them.
5. The quantitative analysis of the company's financial performance and its impact on the implementation of the integrated GRC framework could provide additional insights to support the evaluation (Abdullah 2019).

L3 - Culture Element at Company X

With the understanding of Company X's external context and internal context, the next step is to assess the organizational culture and its alignment with the integrated GRC framework. Corporate culture plays a critical role in the successful implementation of any strategic initiative, including the adoption of an integrated GRC framework.

What went well:

1. The culture assessment is conducted regularly using a survey that evaluates various aspects of the organizational culture, such as leadership, communication, decision-making, risk awareness, and ethical behavior.
2. The culture assessment provides a holistic view of the organizational culture, including the strengths, weaknesses, and areas for improvement.
3. The Company X already has plans to address the identified cultural gaps through targeted interventions, such as leadership development programs, communication campaigns, and process improvements.

Improvement Opportunities:

1. The culture assessment could be further strengthened by incorporating external benchmarking to understand how Company X's culture compares to industry peers or best-in-class organizations (Bolboli and Reiche 2014).
2. The analysis could be enhanced by exploring the potential correlations between the company's cultural attributes and its operational and financial performance, which could provide additional insights to guide the cultural transformation efforts (Graham et al. 2022).
3. The evaluation of the organizational culture could be more closely integrated with the assessment of the company's readiness for the implementation of the integrated GRC framework, to ensure a seamless alignment between the cultural aspects and the GRC objectives.
4. The implementation of the cultural transformation initiatives could benefit from a more structured change management approach, with clearly defined roles, responsibilities, and accountability mechanisms to ensure the desired outcomes are achieved (Wankhade and Brinkman 2014).

5. The communication of the culture assessment results and the progress on cultural transformation initiatives could be enhanced to foster greater transparency and employee engagement (Craig 2020).

L4 - Stakeholder Element at Company X

The successful implementation of the integrated GRC framework at Company X requires a comprehensive understanding of its stakeholder landscape and their expectations.

What went well:

1. The stakeholder assessment at Company X includes the identification of key stakeholder groups, such as customers, suppliers, regulators, investors, and employees, and their respective interests and influence on the company's operations.
2. The stakeholder mapping is included in a comprehensive Company Manual, which documents the key stakeholder groups, their respective interests and influence, both at the corporate level and across the various operational departments within the organization. This stakeholder information is readily accessible and updated regularly to ensure it remains relevant and aligned with the evolving business environment.
3. The stakeholder engagement process at Company X involves regular interactions and feedback mechanisms, such as customer surveys, supplier meetings, investor briefings, and employee town halls, to gather insights and address stakeholder concerns in a proactive manner.
4. The stakeholder assessment is integrated with the company's risk management framework, enabling the identification and mitigation of stakeholder-related risks that could impact the successful implementation of the integrated GRC framework.
5. The stakeholder engagement process has been instrumental in enhancing the company's reputation and building trust with its key stakeholders, which is crucial for the successful implementation of the integrated GRC framework.

Improvement Opportunities:

1. The stakeholder assessment could be further strengthened by incorporating a more detailed analysis of the evolving stakeholder expectations, particularly in the context of the integrated GRC framework.
2. The company could explore the use of more advanced stakeholder engagement tools, such as digital platforms and analytics, to better understand and respond to stakeholder needs in a more timely and effective manner (Jun and Kim 2021).
3. The stakeholder assessment could be more closely aligned with the company's overall strategic planning process, to ensure that the stakeholder perspectives are fully integrated into the decision-making and resource allocation processes related to the implementation of the integrated GRC framework.
4. The communication and reporting on the stakeholder engagement activities and their impact on the GRC implementation could be enhanced to demonstrate the company's commitment to transparency and accountability.
5. The company could consider establishing dedicated stakeholder engagement roles or functions to oversee the continuous monitoring and management of stakeholder relationships, particularly in the context of the integrated GRC framework. This could involve creating new positions or designating existing personnel to be responsible for coordinating stakeholder engagement activities, analyzing stakeholder feedback, and ensuring that stakeholder perspectives are effectively integrated into the decision-making and implementation processes related to the integrated GRC framework. By having dedicated resources focused on stakeholder engagement, the company can enhance its ability to proactively identify and address stakeholder needs, mitigate risks, and foster stronger relationships with its key stakeholders throughout the GRC implementation journey.

5.2. ALIGN Component Analysis at Company X

This component involves aligning performance, risk, and compliance objectives, strategies, decision- making criteria, actions, and controls with the context, culture, and stakeholder requirements. The ALIGN component has 5 elements, which are:

A1 - Direction Element at Company X

This element involves defining clear strategic directions, performance indicators, and target levels of performance that are aligned with the organization's context, culture, and stakeholder requirements.

1. At Company X, the process of aligning GRC initiatives with organizational mission, vision, and values starts with establishing a clear set of strategic goals and performance indicators that are directly linked to the company's overall business objectives.
2. At Company X, GRC initiatives are integrated into the PDCA cycle at both the corporate and operational levels, ensuring continuous alignment between GRC activities and the company's strategic priorities, as follows:
    - PLAN-Phase: The PLAN phase at Company X is the phase to get commitment. It involves management system, policy and standard, stakeholder needs identification, management commitment & leadership through strategic directions (tone at the top), target setting (budgeting), risk assessment & mitigation plan; business continuity plan; internal control design to address operational risks, and cascading strategies to individual KPIs. This planning phase is crucial in breaking down silos by aligning cross-departmental goals, enabling an integrated approach to GRC.
    - DO-Phase: The DO phase at Company X is the phase to get achievement. It involves resources allocation; operational planning execution; project management; training and education; document management system, and implementing contingency plan.
    - CHECK-Phase: The CHECK phase at Company X is the phase to get motivation. It involves business performance monitoring through regular management reviews to evaluate what went well, what can be improved, and the root causes, and motivate the team to perform better; This phase also involves risk-based internal audit and investigations, and performance and risk reporting.
    - ACT-Phase: The ACT phase at Company X is the phase to get improvement. It involves corrective actions development and implementation; continuous improvement and Innovation

At Company X, the GRC initiatives are also aligned with the important aspects of the organization (CULTURE-PEOPLE-PROCESS-TECHNOLOGY), resulting in a holistic approach, and collaborative projects that involve all functions/departments to encourage stronger integration and break down Silos.

What went well:

1. The strategic alignment of GRC initiatives with Company X's overall mission, vision, and values is a key strength.
2. The integration of GRC into the PDCA cycle at both the corporate and operational levels ensure continuous alignment between GRC activities and the company's strategic priorities.
3. The holistic approach to aligning GRC with important aspects of the organization (e.g., management systems, policies, stakeholder requirements) promotes stronger cross-functional collaboration and integration.
4. The clear identification of strategic goals, performance indicators, and target levels of performance provides a robust framework for measuring the success of the integrated GRC implementation.
5. The cascading of GRC strategies into individual KPIs helps to drive accountability and ensure that all employees are aligned with the company's GRC objectives.

Improvement Opportunities:

1. The company could consider enhancing the strategic linkages between the GRC objectives and the overall enterprise risk management framework. This would help ensure a more cohesive and holistic approach to risk management across the organization.
2. Additionally, Company X could explore opportunities to further automate the process of aligning GRC initiatives with the PDCA cycle. This could improve the efficiency of the alignment process and reduce the manual efforts required, freeing up resources to focus on other strategic priorities.

3. The company could also consider implementing a more comprehensive and data-driven performance measurement system. This would provide a more holistic view of the effectiveness of the integrated GRC framework, enabling the organization to make more informed decisions and continuously improve the framework over time.
4. Key risk indicators (KRI) should be defined to track the overall effectiveness of the GRC implementation and ensure that it continues to be aligned with the company's strategic objectives (Hey 2017). These indicators could include metrics related to the achievement of GRC-related goals, the timeliness of risk mitigation actions, the level of stakeholder engagement, and the overall maturity of the GRC framework within the organization. By establishing a comprehensive set of key risk indicators, the company can gain better visibility into the performance of its integrated GRC efforts and make data-driven decisions to continuously improve and optimize the framework over time.
5. Key Compliance Indicators (KCI) should be established to monitor the organization's adherence to relevant laws, regulations, and industry standards (Johnson 2015). Each department should maintain an up-to-date registry of all relevant regulations applicable to their operations, enabling continuous monitoring of compliance.

A2 - Objective Element at Company X

This element involves defining clear GRC objectives that are aligned with the organization's strategic directions and performance targets.

1. The process of mapping the capability objectives to organizational objectives and key risk areas is a critical step in the implementation of integrated GRC at Company X. The mapping is done by correlating the GRC objectives to the organization's strategic priorities and key risk areas.
2. GRC metrics refer to the set of performance indicators that are used to measure the achievement of the GRC objectives. GRC metrics at Company X still focus on KPI threshold achievement, rather than directly measuring the effectiveness of controls or the mitigation of key risks. KRI and KCI should also be integrated to provide a more holistic view of GRC performance.

3. The method of how the GRC capability incorporates the prioritization of objectives into the capability design, risk prioritization, and prioritization of initiatives in the Integrated Plan should be further developed. This would involve establishing a more robust and structured process for aligning the GRC objectives with the organization's strategic priorities, as well as clearly defining the criteria and methodology used to prioritize risks and initiatives. By enhancing this aspect of the GRC framework, Company X can ensure that the integrated GRC approach is optimally focused on the organization's key risk areas and strategic goals, leading to more effective risk mitigation and better alignment with the overall business objectives.

What went well:

1. The strategic alignment of GRC initiatives with Company X's overall mission, vision, and values is a key strength, as it ensures that the GRC framework is closely integrated with the organization's core strategic priorities and objectives. This helps to ensure that the implementation of GRC is not viewed as a standalone compliance exercise, but rather as a critical enabler of the company's overall success and growth.
2. The integration of GRC into the PDCA cycle at both the corporate and operational levels is a strong practice, as it helps to ensure continuous alignment between GRC activities and the company's strategic priorities.
3. The holistic approach to aligning GRC with important aspects of the organization, such as culture, governance, and operations, promotes stronger cross-functional collaboration and integration, breaking down traditional silos and fostering a more cohesive and unified approach to risk management.

Improvement Opportunities:

1. The company could consider enhancing the strategic linkages between the GRC objectives and the overall enterprise risk management framework. This would help ensure a more cohesive and holistic approach to risk management across the organization, aligning the GRC initiatives more closely with the company's overarching risk management strategy and priorities. By strengthening these connections, the company can leverage the GRC framework to provide a more comprehensive and

integrated view of its risk landscape, enabling more informed decision-making and more effective risk mitigation efforts.

2. Additionally, Company X could explore opportunities to further automate the process of aligning GRC initiatives with the PDCA cycle. This could improve the efficiency of the alignment process and reduce the manual efforts required, freeing up resources to focus on other strategic priorities. By leveraging automation and technology, the company can streamline the integration of GRC activities within the PDCA framework, ensuring a more seamless and responsive approach to risk management across the organization.

3. To enhance the effectiveness of the GRC framework, the company could consider implementing a more robust performance measurement system. This would involve defining a comprehensive set of key performance indicators and key risk indicators to track the overall efficiency and impact of the integrated GRC program. By establishing clear, data-driven metrics to assess the GRC framework's performance, the company can gain better visibility into the effectiveness of its risk management efforts and make more informed, evidence-based decisions to continuously improve the program over time. Additionally, the company may consider incorporating feedback from key stakeholders, such as employees, customers, and regulatory bodies, to further refine the performance measurement system and ensure it is aligned with the organization's strategic priorities and risk management objectives.

4. Finally, Company X should consider enhancing the integration of its GRC framework with emerging technologies, such as artificial intelligence, machine learning, and data analytics. By leveraging these technologies, the company can potentially automate certain GRC processes, enhance the identification and assessment of risks, and provide more robust and data-driven insights to support more informed decision-making.

By addressing these improvement opportunities, Company X can further strengthen its integrated GRC framework, aligning it more closely with the organization's strategic objectives, enhancing its overall effectiveness, and positioning the company for continued success in managing its enterprise-wide risks (Kalaimani, 2016) (Alharbi et al., 2022).

A3 – Identification Element at Company X

This is to assess how Company X conduct identification of forces that may cause desirable (opportunity) or undesirable (threat) effects on the achievement of objectives

What went well:

1. The regulatory affairs team at Company X closely monitors changes in all relevant laws, regulations, and industry standards, ensuring the organization remains compliant and aware of emerging compliance requirements.
2. Company X regularly conducts cross-functional risk identification workshops and brainstorming sessions, engaging diverse stakeholders across the organization to systematically identify new and emerging risks that could impact the achievement of strategic objectives.
3. Risk registers are maintained, thoroughly documenting key risks, corresponding control measures, and designated risk owners responsible for monitoring and mitigating these risks.
4. A risk matrix is utilized to prioritize risks based on a careful assessment of their likelihood of occurrence and potential impact on the organization, enabling Company X to focus its risk management efforts on the most critical areas.

Improvement Opportunities

1. While the regulatory affairs team monitors changes in laws and regulations, the company could consider expanding its horizon scanning to also encompass emerging industry trends, technological advancements, and shifts in the competitive landscape. By broadening the scope of its risk identification, Company X can better anticipate and prepare for a wider range of potential disruptive forces that could impact its operations and strategic objectives.
2. In addition to the Regulatory Affairs team's monitoring of changes in laws, regulations, and industry standards, other key departments across the organization, such as Sales, Marketing, and Manufacturing & Supply Chain, should also proactively monitor shifts in the external environment, including emerging industry trends, technological advancements, and changes in the competitive landscape. By adopting a cross-

functional approach to horizon scanning, Company X can better anticipate and prepare for a wider range of potential disruptive forces that could impact its operations and strategic objectives.

3. The company could consider enhancing the risk identification process by incorporating more diverse perspectives and inputs. This could include seeking feedback and insights from external stakeholders, such as customers, suppliers, and industry experts, to gain a more comprehensive understanding of the risks facing the organization (Merna and Merna 2004).
4. Risk matrix should be periodically reviewed and updated to reflect changing risk profiles and priorities, ensuring the company's risk management efforts remain aligned with its evolving strategic objectives and the dynamic business environment (Francis and Paladino 2008).
5. A quantitative approach to risk assessment, such as the use of probability-impact grids or failure modes and effects analysis, could be implemented to supplement the current qualitative risk matrix, providing a more robust and data-driven approach to risk prioritization (Griffis and Whipple 2012).
6. Additionally, Company X could explore the use of advanced data analytics and predictive modeling techniques to identify emerging risks more proactively. By leveraging data-driven approaches, the company can analyze historical data, market trends, and external factors to forecast and anticipate potential risks before they materialize. This could involve the implementation of predictive analytics algorithms, machine learning models, and scenario-planning simulations to provide early warning signals and enable more proactive risk mitigation strategies. Through the adoption of these advanced analytical tools, Company X can enhance its risk sensing capabilities and stay ahead of the curve in managing enterprise-wide risks.

A4 - Analysis Element at Company X

This section is to assess how Company X conduct analysis on current and planned approach to address opportunities, threats and requirements using decision-making criteria with quantitative and qualitative methods.

What Went Well:

1. Company X has established a risk assessment process, which involves the use of a well-defined risk matrix to systematically evaluate the likelihood and potential impact of identified risks. This risk assessment framework enables the organization to prioritize its risk management efforts by focusing on the most critical risks that could have the greatest impact on the achievement of its strategic objectives.
2. The company's risk assessment process involves cross-functional collaboration, with key stakeholders from various departments, such as finance, operations, and compliance, participating in the risk identification and analysis workshops.
3. Company X has a comprehensive risk register that documents all identified risks, their corresponding controls, and designated risk owners responsible for monitoring and mitigating these risks.
4. Each Department is required to update what went well and what needs to be improved in every management review session to enable the organization to continually enhance its risk management practices. This iterative approach ensures that the company's risk management framework remains responsive to changing internal and external factors.
5. The company has established PICAPA (Problem Identification, Corrective Action, and Preventive Action) process to address emerging risks and non-conformities, ensuring that appropriate mitigation strategies are implemented in a timely manner and SIRA (Success Identification and Replicative Action) framework to assess the suitability, adequacy, and effectiveness of risk controls, risk responses, and risk management activities.

Improvement Opportunities

1. While the existing risk matrix provides a structured approach to risk prioritization, the company could consider incorporating more quantitative elements into its risk assessment process. This could involve the use of probability-impact grids, failure modes and effects analysis, or other advanced analytical techniques to supplement the current qualitative risk matrix. By integrating quantitative risk assessment methods, Company X can gain a more robust and data-driven understanding of the likelihood and

potential impact of identified risks, enabling more informed decision-making and resource allocation for its risk management efforts.

2. To further embed risk management into the organizational culture, Company X could explore ways to empower and encourage all employees to actively participate in the risk identification and analysis process. This could involve providing risk management training and awareness programs to help employees at all levels understand their role in identifying, assessing, and mitigating risks within their respective functions. By fostering a risk-aware culture where everyone is responsible for proactively identifying and managing risks, Company X can leverage the diverse perspectives and domain expertise of its workforce to enhance its overall risk management capabilities.
3. The company could consider expanding its horizon scanning activities to look beyond its immediate industry and competitive landscape. This could involve monitoring broader economic, technological, and societal trends that may have indirect, yet significant, impacts on the company's operations and strategic objectives. By adopting a more holistic and forward-looking approach to risk identification, the company can better anticipate and prepare for a wider range of potential disruptive forces that could affect its long-term sustainability and growth.

A5 - Design Element at Company X

This section is to assess how Company X develops strategic and tactical plans to achieve the objectives, while addressing uncertainty and acting with integrity, consistent with decision-making criteria.

What Went Well:

1. Company X has started to integrate its Governance, Risk, and Compliance framework with its strategic objectives. This integrated approach enables the company to holistically manage risks, ensure compliance, and make informed decisions that enhance its overall enterprise risk management capabilities.
2. The company has established a centralized Enterprise Risk Management function that is responsible for coordinating the organization's risk management activities. This ERM

team works closely with business units and support functions to ensure that risks are consistently identified, assessed, and managed across the enterprise.

3. Company X has established a digital transformation committee that is responsible for overseeing the implementation of emerging technologies and digital initiatives. This committee ensures that the company's digital transformation efforts are aligned with its strategic goals and that appropriate risk mitigation measures are in place to address the risks associated with these initiatives.
4. The company has initiated a preliminary stage of business continuity management that outlines the procedures and resources required to maintain critical business operations in the event of a disruption.
5. The Company has established a Compliance function under Regulatory Affairs Division that is responsible for monitoring and ensuring adherence to relevant laws, regulations, and industry standards.
6. The Company has established Consumer Insight Division that is responsible for monitoring market share, market trends, and competitive landscape to inform the strategic decision-making process.
7. The company has implemented adequate internal controls system, including segregation of duties, authorization limits, and periodic reviews, to mitigate the risk of fraud, errors, and unauthorized activities.

Improvement Opportunities

1. The process utilized to design the GRC capability and its measurement, including the development of the GRC Business Case, GRC Strategic Plan, and GRC Assessment Plan, could be further formalized and documented. Formalizing these processes would help ensure consistent implementation and enable continuous improvement of the company's GRC framework. To provide clear guidance and accountability, the company could consider developing a GRC Charter, GRC Policy, and GRC Standard Operating Procedures. These formalized documents would define the objectives, roles, responsibilities, and procedures for the effective management of governance, risk, and compliance within the organization.

2. The process for designing, implementing, and maintaining the Third-Party Risk Management Plan could be further enhanced to ensure a more comprehensive and proactive approach to managing risks associated with the company's third-party relationships. The Purchasing Division should conduct regular due diligence assessments on all third-party vendors, suppliers, and partners to identify, assess, and mitigate any potential risks (Zsidisin, Panelli, and Upton 2000). This should include evaluating the financial stability, operational resilience, information security controls, and regulatory compliance of the third parties. Additionally, the company could consider implementing a robust onboarding and ongoing monitoring process to ensure that third-party relationships remain aligned with the company's strategic objectives and risk appetite throughout the duration of the engagement. By taking a more holistic and systematic approach to third-party risk management, the company can better safeguard its operations, reputation, and long-term sustainability.

3. The company could also explore opportunities to enhance the integration between its Enterprise Risk Management, Digital Transformation, and Compliance functions. This could involve establishing stronger communication channels, aligning risk assessment and mitigation strategies, and leveraging shared data and analytics to drive a more cohesive and holistic approach to managing risks across the organization. By fostering closer collaboration and integration between these key functions, the company can ensure that its risk management efforts are aligned with its strategic digital initiatives and regulatory compliance requirements, leading to more effective and efficient risk management outcomes.

4. The process utilized to design the GRC Technology Plan and to integrate GRC technology solutions with the organizational technology plan including the degree of information sharing and collaboration could be further enhanced. The company could explore the implementation of a centralized GRC technology platform that can provide a unified view of the company's governance, risk, and compliance activities, as well as enable the integration of data, workflows, and reporting across the different functional areas. This would help the company to better identify, assess, and manage risks in a more cohesive and efficient manner, while also improving the overall visibility and transparency of its risk management efforts.

5.3. PERFORM Component Analysis at Company X

This component involves addressing threats, opportunities, and requirements by encouraging desired conduct and events, and preventing what is undesired, through the application of proactive, detective, and responsive actions and controls. The analysis of PERFORM Component involves the following eight elements:

P1 - Controls Element at Company X

This section is to assess if Company X has established a mix of management, process, human capital, technology, information, and physical actions and controls that serve governance, management, and assurance needs to address the identified risks and opportunities.

What Went Well:

1. Proactive Actions and Controls:
    - The company has established a robust Enterprise Risk Management framework to proactively identify, assess, and manage key strategic, operational, financial, and compliance risks across the organization. This ERM framework enables the company to take a comprehensive and systematic approach to risk management, helping to ensure that material risks are effectively mitigated.
    - The company has implemented a Risk and Control Self-Assessment process, which empowers all business units to regularly evaluate and report on the effectiveness of their internal control systems. This allows the company to maintain visibility over the control environment and identify any potential weaknesses or areas for improvement in a timely manner.
    - The company has established policies and standard operating procedures across the organization to guide employee conduct and ensure compliance with relevant laws, regulations, and industry best practices. These formalized guidelines and protocols help to promote ethical behavior, mitigate compliance risks, and align the actions of all personnel with the company's strategic objectives and risk management framework.

2. Detective Actions and Controls:
    - The company has implemented Key Performance Indicators that are monitored on a regular basis to detect any emerging risks or deviations from the expected performance.
    - The Internal Audit function conducts periodic, comprehensive reviews and audits to assess the design, implementation, and operating effectiveness of the company's internal control systems across all business units and functional areas. These audits provide an independent and objective evaluation of the adequacy and efficiency of the company's governance, risk management, and control processes, enabling the identification of potential weaknesses or areas for improvement. The findings and recommendations from these internal audits are then communicated to the relevant stakeholders, including senior management and the Board of Directors, to support the continuous enhancement of the company's internal control environment.
    - Regular management reviews are conducted to monitor the implementation and assess the ongoing effectiveness of the company's risk mitigation strategies and internal control measures. These reviews enable the identification of any gaps or weaknesses in the control environment, allowing the company to promptly address issues and continuously enhance its risk management capabilities.
3. Responsive Actions and Controls:
    - The company has established a formal Incident Response Plan and a dedicated Crisis Management Team to ensure the effective and coordinated management of any significant incidents, disruptions, or crises that may impact the organization.
    - The company has implemented whistle-blower hotlines and other mechanisms to encourage the reporting of any suspected misconduct, compliance breaches, or ethical violations.
    - The company has implemented comprehensive fraud investigation and remediation procedures to promptly identify, address, and mitigate any instances of fraudulent activities or financial irregularities within the organization. These

procedures enable the thorough examination of suspected fraud cases, the implementation of appropriate corrective actions, and the development of targeted controls and measures to prevent future occurrences and protect the company's assets and reputation.

Improvement Opportunities:

1. Proactive Actions and Controls
    - The company could further enhance its proactive risk management by implementing Key Risk Indicators and Key Compliance Indicators to provide early warning signals of potential risks and compliance issues (Marchetti 2012). KRIs would enable the company to proactively monitor key risk factors and identify emerging risks, while KCIs would help the organization track and manage its compliance posture across various regulatory requirements. By establishing a comprehensive set of KRIs and KCIs, the company could gain greater visibility into its risk landscape and be better positioned to anticipate, prevent, and mitigate risks in a timely and effective manner.
    - While the company has established an ERM framework, it could further enhance its risk management capabilities by implementing a more integrated and data-driven approach to risk identification, assessment, and mitigation.
    - The company could further strengthen its proactive risk management by implementing a more integrated and data-driven approach to risk identification, assessment, and mitigation. This could involve leveraging advanced analytics, real-time risk monitoring, and predictive modeling to enhance the company's ability to anticipate, identify, and respond to emerging risks in a more timely and effective manner.
    - The company could also consider implementing a more robust risk appetite framework to better align its risk management activities with its strategic objectives and risk tolerance levels (Burnaby and Hass 2009).
    - Implement comprehensive background checks for all new hires and periodic re-checks for existing employees to verify qualifications, employment history, and any potential conflicts of interest or criminal records (Brody 2010). This will

help ensure the integrity of the workforce and mitigate risks associated with hiring unqualified or untrustworthy personnel.

- Due diligence for third party vendors, suppliers, and other business partners is critical to mitigate risks associated with third-party relationships. The company should implement a thorough due diligence process to evaluate the qualifications, financial stability, compliance history, and ethical practices of all third parties before engaging them. This may include conducting background checks, financial assessments, reference checks, and on-site visits to ensure the integrity and reliability of the third parties. Ongoing monitoring and periodic re-evaluations should also be conducted by Purchasing Team to identify any changes or emerging issues that could pose risks to the company.

2. Detective Actions and Controls

- The company could further enhance its detective controls by implementing more advanced data analytics and continuous monitoring capabilities to enable the real-time identification and mitigation of emerging risks (Engemann 2019). For example, the company could leverage exception reporting, predictive analytics, and automated alerts to quickly detect anomalies, deviations from expected performance, and other early warning signs of potential issues. This would allow the company to respond proactively and address risks before they escalate into significant problems.
- The company could also consider enhancing its independent assurance function by strengthening the role and capabilities of its Internal Audit team. The Internal Audit team currently only covers a limited number of business units and functional areas on a periodic basis. To enhance the effectiveness of the company's detective controls, the Internal Audit function could be expanded to conduct more comprehensive and frequent reviews across all critical business operations and control processes. This would provide the company with more extensive and timely insights into the design, implementation, and operating effectiveness of its internal control systems, enabling the identification of a broader range of potential weaknesses or areas for improvement.

- The size of the Internal Audit team should also be expanded to provide more comprehensive and frequent reviews across all critical business operations and control processes. This would enable the Internal Audit function to conduct a more extensive and timely evaluation of the design, implementation, and operating effectiveness of the company's internal control systems, thereby facilitating the identification of a broader range of potential weaknesses or areas for improvement.
- To further strengthen its detective controls, the company could consider implementing a more robust compliance monitoring program. This could involve the establishment of dedicated compliance teams or the assignment of compliance responsibilities to specific business units or functional areas.

3. Responsive Actions and Controls
    - The company should implement a comprehensive Incident Response Plan and a dedicated Crisis Management Team to ensure the effective and coordinated management of any significant incidents, disruptions, or crises that may impact the organization.
    - The company could further enhance its responsive capabilities by conducting more frequent tabletop exercises and simulations to test the effectiveness of its Incident Response Plan and the Crisis Management Team's preparedness.

P2 - Policies Element at Company X

The effectiveness of the company's GRC and ERM framework is also heavily dependent on the strength and clarity of its policies, procedures, and guidelines. This section is to asses if Company X has implemented policies and associated procedures to address opportunities, threats and requirements and set clear expectations of conduct for the governing authority, management, and the workforce.

What Went Well:

1. The company has established a comprehensive and well-documented set of policies and procedures that cover a wide range of critical business areas, including finance,

operations, human resources, information technology, and compliance. These policies provide clear guidance and set expectations for the governing authority, management, and the workforce to ensure effective governance, risk management, and compliance across the organization.

2. The company has implemented a robust policy management system under supervision of Quality System function that includes a centralized policy repository, regular policy reviews and updates, and a defined policy exception and waiver process. This helps ensure that all policies remain current, relevant, and effectively communicated to all stakeholders.
3. The company has invested significant efforts in establishing a strong ethical and compliance culture, with the Code of Conduct being a central component. The Code of Conduct clearly defines the company's core values, behavioral expectations, and zero-tolerance approach to unethical conduct or non-compliance.
4. The company has implemented compliance program that includes regular training on policies and procedures, as well as regular monitoring and auditing to ensure compliance across the organization.
5. The company has established an effective whistleblower program that enables employees to confidentially and anonymously report any suspected violations of policies, laws, or ethical standards.
6. Control self-assessment programs have been implemented across the organization, enabling business unit leaders and subject matter experts to regularly evaluate the design and operating effectiveness of key controls and identify any potential gaps or weaknesses.

Improvement Opportunities

1. The company could consider further enhancing its policy management system by implementing more robust version control, digital signatures, and automated workflow capabilities to streamline the policy review, approval, and distribution process.
2. The company could also explore opportunities to leverage technology and data analytics to enhance the monitoring and testing of policy compliance, such as by automating

controls testing, deploying real-time compliance dashboards, and implementing advanced anomaly detection capabilities.

3. The company may benefit from strengthening the linkage between its policies and procedures, and the organization's key business processes, risks, and controls.
4. The company could consider implementing more structured and comprehensive compliance training programs, including role-based training, scenario-based learning, and periodic assessments to reinforce employee understanding and application of policies and procedures.
5. The company could enhance its whistleblower program by implementing more robust case management, investigation, and reporting capabilities to improve the efficiency and transparency of the process.
6. The company could explore opportunities to leverage its Control Self-Assessment program to gather more comprehensive insights into the overall design and operating effectiveness of the GRC and ERM frameworks, and to identify areas for improvement.
7. Rewards and punishment mechanisms could be strengthened to promote a stronger culture of accountability and compliance across the organization.
8. The company could consider enhancing its policy management governance by establishing a dedicated Policy Steering Committee or a similar oversight body to ensure consistent policy development, implementation, and enforcement across the organization.
9. Anti-Bribery & Corruption policy could be reviewed and strengthened to ensure alignment with evolving regulatory requirements and industry best practices.
10. The Company could start to use a register to record the following information regarding Code of Conduct:
    - Percentage of personnel that received the code
    - Percentage that have received training on the code
    - Percentage that have confirmed receipt and understanding
    - Passage rate statistics on any assessments of understanding

- Number of breaches
- Number of code of conduct violations remediated by various types of responsive actions or controls
- Dollar value of losses experienced from violations, and
- Dollar value of rewards for adherence to violation reporting.

P3 - Communication Element at Company X

Effective communication is a critical enabler for successful implementation and sustainment of the GRC and ERM frameworks. This section is to assess the process for developing and maintaining the Communication and Reporting Plan including how contact with stakeholders is controlled and recorded to ensure all communications and reports are included.

What Went Well:

1. The company has developed a comprehensive Communication and Reporting Plan that defines the key stakeholders, communication channels, and reporting requirements for the GRC and ERM programs. The stakeholders involved in the company's GRC and ERM programs are divided into two main categories: internal stakeholders and external stakeholders. The internal stakeholders include the governing body, management, and the entire workforce. The external stakeholders encompass regulatory authorities, industry associations, customers, suppliers, and other relevant third parties who have a stake in the company's governance, risk management, and compliance initiatives.
2. The Communication and Reporting Plan is well-documented, regularly reviewed, and readily accessible to all relevant internal and external stakeholders. The plan outlines clear communication channels, reporting requirements, and a defined process for collecting and addressing feedback from stakeholders to ensure the continuous improvement of the GRC and ERM programs.

Improvement Opportunities

1. The timeliness and responsiveness of communication to key stakeholders, particularly in the event of critical risk events or compliance issues, could be further enhanced. This

would enable more proactive and transparent engagement, ensuring that information is shared in a timely manner and that stakeholders are kept informed and involved throughout the process. Improving the speed and transparency of communication can help build trust, facilitate better decision-making, and support the overall effectiveness of the company's governance, risk, and compliance efforts.

2. The company could consider expanding its Communication and Reporting Plan to include more targeted and tailored communication strategies for different stakeholder groups, taking into account their unique information needs, communication preferences, and levels of influence or impact on the organization.
3. Several reports are still maintained manually using spreadsheets and other static formats, which can limit the ability to provide real-time insights, perform advanced data analysis, and generate customized reports for different stakeholders. In this case, the company could explore opportunities to leverage technology and digital platforms to enhance the accessibility, interactivity, and user-experience of its GRC and ERM-related communications and reporting.
4. Whistleblowing and incident reporting channels could be further highlighted and promoted to all stakeholders, both internal and external, to encourage greater awareness, trust, and utilization of these critical communication avenues for reporting concerns or non-compliance.

P4 - Education Element at Company X

Providing comprehensive and effective education and training to all relevant stakeholders is a crucial aspect of ensuring the successful implementation and ongoing sustainability of the company's GRC and ERM frameworks. This section is to assess the governing authority, management, the workforce, and the extended enterprise about expected conduct, and increase the skills and motivation needed to help the organization address opportunities, threats, and requirements.

What Went Well

1. Risk management education is a key component of the company's overall training curriculum, available to all employees and third party (i.e., suppliers, vendors). Risk education is conducted through a combination of in-person sessions, online socialization, campaign (Email and WhatsApp Group) and targeted workshops/forums.
2. The company has developed compliance training programs that cover topics such as Code of Conduct, Anti-Fraud, Cybersecurity, and Data Privacy, although it is still very early in the implementation journey.

Improvement Opportunities

1. The current education program only focuses on raising risk and compliance awareness, there is a need to further develop employees' risk management skills and competencies.
2. The current education program could be expanded to cover more comprehensive topics on holistic GRC principles, including the integration of governance, risk management, and compliance across the organization. This would help employees gain a deeper understanding of the interconnected nature of these elements and how they collectively support the company's overall risk management and compliance efforts.
3. The training programs could leverage a combination of in-person instructor-led sessions, engaging e-learning modules, and interactive case-based exercises to cater to the diverse learning preferences of the workforce (Morgunova and Bolkina 2020). This multi-modal approach promotes active engagement, knowledge retention, and the practical application of the training content. The training programs aim to equip employees with the necessary skills and understanding to effectively support the organization's governance, risk management, and compliance initiatives.
4. Specific training for the governing body and senior leaders on their GRC and ERM-related roles, responsibilities, and oversight accountabilities should be mandatory and conducted on a regular basis. This training should equip the governing body and senior leaders with a comprehensive understanding of the key principles, frameworks, and best practices in governance, risk management, and compliance. It should cover their fiduciary duties and strategic oversight responsibilities in these critical areas, as well as provide guidance on how they can effectively monitor the implementation and

performance of the company's GRC and ERM initiatives. The training should also address the governing body's role in providing support and direction to management in strengthening the organization's overall risk management capabilities.

5. The assessment tools used to measure awareness, training, knowledge, support, and understanding of the policies, procedures, and code(s) of conduct by all target recipient groups are not sufficiently robust and meaningful, only limited to pre and post-tests. The company should consider implementing more comprehensive and continuous assessment methods, such as surveys, interviews, and performance-based evaluations, to better gauge the effectiveness of the training programs and identify areas for improvement (Mollahoseini and Farjad 2012).
6. The procedure used to train and confirm that individuals understand how to report an issue (i.e., incident, concern, inquiry) including the curriculum required and the frequency of refresher training could be enhanced. The company should ensure that all employees and third parties are aware of the reporting channels, the process for escalating concerns, and the non-retaliation policy.

P5 - Incentive Element at Company X

An effective incentive and accountability framework is crucial for driving desired behaviors, fostering a culture of compliance, and ensuring the continuous improvement of the organization's governance, risk management, and compliance practices. This section is to assess if Company X has implemented incentives that motivate desired conduct and recognize those who contribute to positive outcomes to reinforce desired conduct.

What Went Well

1. The company has a performance management system that incorporates risk management and compliance-related metrics as part of the key performance indicators and objectives for senior leadership team.
2. The Company has a well-established ethics and compliance hotline, available to both internal and external stakeholders, to report any suspected misconduct or violations.

3. The company has a non-retaliation policy in place to protect whistleblowers and other individuals who report concerns in good faith.
4. The leadership team consistently reinforces the importance of ethical conduct and compliance through regular town halls, newsletters, and other communication channels, setting the proper "tone at the top" to drive the desired behaviors and culture.

Improvement Opportunities

1. The current performance management system focuses primarily on financial and operational metrics, with limited weight given to risk management and compliance-related objectives. Therefore, there is an opportunity to increase the emphasis on these critical areas and ensure they are adequately reflected in the performance evaluation and incentive structures across all levels of the organization.
2. The company should consider expanding the performance evaluation and incentive framework to include more explicit risk management and compliance-related metrics, such as measures of risk identification and mitigation, adherence to policies and procedures, and successful implementation of compliance initiatives. These elements should be weighted appropriately, carrying significant influence on performance assessments and compensation decisions, to effectively incentivize the desired behaviors and outcomes that support the organization's governance, risk management, and compliance objectives.
3. The company should explore the feasibility of implementing a formal recognition and rewards program that celebrates and incentivizes employees who demonstrate exemplary adherence to the company's ethical standards, risk management practices, and compliance requirements. This could include initiatives such as an "Employee of the Month" award for individuals who go above and beyond in upholding the company's compliance and risk management policies, or a "Risk Management Champion" program that acknowledges and rewards those who proactively identify and mitigate potential risks. Additionally, the company could consider incorporating risk management and compliance metrics into the existing employee bonus and promotion structures to further drive the desired behaviors and reinforce the importance of these critical areas to the organization's overall success.

4. The company should periodically review and assess the effectiveness of its whistleblower program to ensure that employees and third parties feel empowered and encouraged to report any suspected misconduct or violations without fear of retaliation.
5. The company should also explore the feasibility of implementing a formal recognition program that celebrates and rewards employees who demonstrate exemplary adherence to the company's ethical standards, risk management practices, and compliance requirements.

P6 - Notification Element at Company X

This section is to assess if Company X has provided multiple pathways to report progress toward objectives, and the actual or potential occurrence of undesirable and desirable conduct, conditions, and events by evaluating the process (test data, real time supervisory monitoring, electronic monitoring, and analytical procedures) for monitoring issue notification (intake), filtering, and management activities to determine that the applicable policies and procedures are consistently applied.

What Went Well

1. The company has an established ethics and compliance reporting hotline, available to both internal and external stakeholders, that enables the communication of any suspected misconduct or violations.
2. The compliance team investigates all reported incidents and concerns in a timely and thorough manner, ensuring that appropriate corrective actions are taken and that the root causes are addressed.
3. Regular reviews and audits of the company's compliance program, including the reporting and incident management processes, are conducted to identify any gaps or areas for improvement.
4. Issues are updated and reported in the regular GRC meeting updates to ensure that the leadership team is aware of any significant compliance incidents or emerging risks.

Improvement Opportunities

1. The company should consider expanding the communication channels and methods for reporting compliance concerns, such as implementing an anonymous online reporting portal, a mobile app, or secure email addresses, to make it easier and more accessible for employees and third parties to raise issues.
2. Exception reports and key performance indicators related to the compliance reporting and incident management processes should be incorporated into the regular GRC reporting to the board and senior leadership team, providing greater visibility into the effectiveness of these critical processes.
3. Early warning system should be established to proactively identify and address emerging compliance risks, such as through the use of data analytics, predictive modeling, and real-time monitoring of key compliance indicators.
4. The company should consider implementing a more robust and structured compliance training program, covering topics such as the code of conduct, reporting procedures, and specific compliance requirements, to ensure that all employees are well-informed and equipped to identify and report any suspected misconduct (Lieber 2010).

P7 - Inquiry Element at Company X

This section is to assess if Company X has periodically analyzed data and seek input about progress towards objectives; and the existence of undesirable conduct, conditions and event by evaluating the workforce and stakeholder feedback process, including all procedures used routinely to ask stakeholders throughout the extended enterprise.

What Went Well

1. The company has established various channels for employees to provide feedback and raise concerns, such as through anonymous employee surveys, focus groups, and open-door policies with management.
2. The company regularly engages with key external stakeholders, such as customers, suppliers, and industry associations, to obtain their perspectives and feedback on the

company's performance, including areas related to governance, risk management, and compliance.

3. The GRC Department proactively gathers and analyzes data from various sources, including internal audits, regulatory filings, and industry benchmarks, to identify potential compliance risks and areas for improvement.

Improvement Opportunities

1. The company should consider implementing a more structured and comprehensive stakeholder engagement program, with clearly defined objectives, roles, and responsibilities, to ensure that feedback is consistently collected, analyzed, and incorporated into the company's GRC strategy and initiatives.
2. The company should explore the use of advanced data analytics and visualization tools to better identify trends, patterns, and correlations within the GRC-related data, enabling more informed decision-making and proactive risk mitigation.
3. The company should consider establishing a GRC advisory board or council, comprised of internal and external subject matter experts, to provide independent and objective feedback on the company's GRC performance and to help identify emerging risks and best practices.

P8 - Response Element at Company X

This section is to assess if Company X has designed and, when necessary executed responses to identified or suspected undesirable conduction, conditions, events, or weaknesses in capabilities, including investigation processes, crisis situation, and resolution processes.

What Went Well:

1. Company X has a well-defined incident response plan and crisis management framework that outlines the procedures for investigating, escalating, and addressing any significant compliance breaches or risk events.

2. The compliance team works closely with the legal, human resources, and IT departments to ensure that appropriate corrective actions are taken in a timely and consistent manner, including disciplinary measures, system enhancements, and process improvements.
3. The company has a strong focus on root cause analysis, ensuring that the underlying issues are identified and addressed to prevent the recurrence of similar incidents.

Improvement Opportunities

1. The company should regularly conduct crisis simulations and tabletop exercises to test the effectiveness of its incident response and business continuity plans, and to identify areas for improvement (Marwitz et al. 2007). These exercises can help the company assess its readiness, identify gaps, and fine-tune its response procedures.
2. To enable better data-driven decision-making and reporting, the company should consider implementing a more centralized and integrated system for tracking and managing compliance incidents and risk events. This system could consolidate data from various sources, provide real-time visibility, and facilitate comprehensive analysis.
3. The company should explore opportunities to enhance its collaboration and information-sharing with relevant industry associations, regulatory bodies, and peer organizations. This can help the company stay abreast of emerging risks and best practices in crisis response and resolution, and allow for the exchange of insights and lessons learned.
4. The company should strengthen its post-incident review process to ensure that lessons learned are systematically captured and incorporated into its GRC framework, policies, and procedures. This will help the company continuously improve its crisis response and prevention capabilities.

5.4. REVIEW Component Analysis at Company X

For REVIEW component, this study will assess if the Company X conducts activities to monitor and improve design and operating effectiveness of all actions and controls, including its

continued alignment to objectives and strategies. The REVIEW component has 3 elements, as follows:

R1 – Monitoring Element at Company X

This section is to assess if Company X has monitored and periodically evaluated the performance of the capability to ensure it is designed and operated to be effective, efficient, and responsive to change by reviewing the process utilized to evaluate the design and performance of the GRC capability during the past three (3) years and the current year to date explaining any changes or improvements implemented during that period and how information from prior and subsequent years are compared and reconciled to assess trends.

What Went Well:

1. Company X has established an internal audit function that regularly reviews the design and operating effectiveness of the company's governance, risk management, and compliance processes and controls. The internal audit team closely examines the GRC framework, including the policies, procedures, and systems in place, to ensure they are operating as intended and effectively mitigating risks across the organization. This ongoing monitoring and evaluation help the company identify areas for improvement and make necessary adjustments to enhance the overall GRC capabilities.
2. The Regulatory Affairs team and stakeholders from related Departments collaborate with the risk management and internal audit functions to proactively monitor changes in regulations, industry standards, and best practices, and to assess the impact on the company's GRC framework.
3. Risk Management Team conducts periodic risk assessments, including the evaluation of emerging risks and the effectiveness of existing controls, to ensure the company's risk profile and mitigation strategies remain current and aligned with the evolving business landscape.
4. Internal Audit Team conducts periodic control self-assessments of the GRC program, utilizing appropriate performance metrics to track the effectiveness of risk management activities and compliance controls.

Improvement Opportunities:

1. GRC framework should be developed to provide a more holistic and integrated view of the company's governance, risk, and compliance posture.
2. Introduce more structured and centralized feedback loops to better capture and address recommendations from internal and external audits, as well as insights from risk assessments and control self-evaluations.
3. GRC steering committee or dedicated GRC program management office should be established to centrally coordinate the monitoring and review activities across the organization, ensuring consistency, completeness, and timeliness of reviews (OCEG 2019).
4. The company should consider implementing a more-robust-data-analytics and reporting capabilities to enhance the internal audit team's ability to identify trends, patterns, and emerging risks more proactively (Knechel et al. 2012).
5. Risk Management Team should further strengthen its collaboration with other functions, such as business strategy, operations, and IT to holistically evaluate the impact of changes in the business environment and technology landscape on the company's GRC framework (Alharbi et al. 2022).
6. Develop a more structured approach to benchmarking the company's GRC practices against industry peers and recognized standards to identify additional areas for improvement.
7. Incorporate more user feedback, including from operational teams and compliance Champions, to continuously enhance the design and user experience of GRC tools and processes.
8. Establish a formal process to regularly review the adequacy and effectiveness of the Whistleblower and Incident Management programs to ensure they are operating as intended.
9. Implement a more robust post-incident review process to thoroughly analyze the root causes of significant risk events or compliance breaches, and to ensure that lessons learned are effectively incorporated into the GRC framework.

10. Foster a stronger culture of risk awareness and compliance accountability throughout the organization by implementing ongoing training and awareness programs for all employees.
11. Risk Committee should be established to provide strategic oversight and guidance on the company's GRC framework, and to ensure it remains aligned with the overall business objectives and risk appetite.

R2 - Assurance Element at Company X

This section is to assess if Company X has provided assurance to management, the governing authority, and other stakeholders that the capability is reliable, effective, efficient and responsive.

What Went Well:

1. The internal audit function provides independent and objective assurance to the Board of Directors and senior management on the design, implementation, and operating effectiveness of the company's GRC framework and processes. Internal audit reports highlight key findings, risks, and recommendations for improvement, which are reviewed by the Audit Committee and addressed by management.
2. The Regulatory Affairs team actively engages with external regulatory bodies and industry associations to stay abreast of changing compliance requirements and to obtain guidance on best practices, which are then incorporated into the company's GRC program.
3. The Risk Management team provides regular updates to the Senior Leadership Team on the company's risk profile, risk mitigation strategies, and the overall performance of the enterprise risk management program, including the GRC capabilities.
4. The company has established a secure whistleblower hotline and incident reporting process, which are well-communicated to employees and provide a confidential channel for raising concerns related to potential compliance breaches or unethical conduct.

Improvement Opportunities:

1. The process for determining which portions of the GRC capability will be audited in any given year and by whom could be strengthened to ensure comprehensive coverage. The company should implement a more structured and risk-based approach to selecting the areas of the GRC framework that will be subject to internal and external audits. This could involve developing a formal audit plan that considers factors such as the inherent risk profile of each GRC component, the results of previous audits, changes in the business or regulatory environment, and the input of key stakeholders. Additionally, the company should ensure that the internal audit function has the appropriate expertise, resources, and independence to effectively evaluate the design and operating effectiveness of the GRC framework across the organization.

2. The process followed to ensure the objectivity, independence, and competency of internal and external auditors assigned to GRC capability engagements could be further strengthened. The company should establish a robust audit governance framework that clearly defines the criteria and procedures for selecting, evaluating, and overseeing both internal and external audit resources. This could involve developing formal policies and guidelines on auditor independence, rotation, and performance evaluation to mitigate potential conflicts of interest and ensure the integrity of the audit process. Additionally, the company should invest in building the specialized skills and expertise of the internal audit team, potentially through targeted training and certification programs, to enhance their ability to effectively assess the design and operating effectiveness of the GRC framework. Regular reviews of the audit function's competency and alignment with industry leading practices should also be conducted to identify opportunities for continuous improvement.

3. The process for tracking and remediating audit findings related to the GRC capability could be more robust and formalized. The company should implement a centralized, technology-enabled system for logging, monitoring, and reporting on the status of audit recommendations and corrective actions.

4. The governance processes for reviewing and approving the annual internal audit plan, audit findings, and management's responses to recommendations should be strengthened. This could involve establishing a dedicated GRC steering committee or

working group, with representation from key functions such as risk management, compliance, legal, and IT, to provide oversight and strategic direction on the GRC audit agenda.

5. The company should consider obtaining an independent, third-party assessment of the overall design and operating effectiveness of its GRC framework to provide an unbiased and comprehensive evaluation. Such an assessment could help the company identify additional areas for improvement and enhance the credibility of the GRC capability with external stakeholders.
6. The reporting of GRC-related audit findings, risks, and remediation efforts to the senior leadership and other key stakeholders could be more transparent and comprehensive. The company should establish clear KPIs and dashboards to regularly communicate the performance and health of the overall GRC framework, including the status of significant audit findings, the effectiveness of risk mitigation actions, and the maturity of compliance activities.

R3 - Improvement Element at Company X

This section is to assess if Company X has reviewed information from periodic evaluations, detective and responsive actions and controls, monitoring, and assurance to identify opportunities for continuous improvements.

What Went Well:

1. The company has a well-established and independent internal audit function that regularly reviews the design, implementation, and operating effectiveness of the GRC framework and associated processes across the organization. The internal audit team provides objective assurance to the senior management on the adequacy and performance of the company's GRC capabilities, highlighting key findings, risks, and recommendations for continuous improvement.
2. The company has an annual Innovation Awards event that promotes and recognizes employees who have developed novel solutions to improve operations. These solutions are typically based on identifying and addressing pain points or seizing future

opportunities within each department or business function. The awards ceremony celebrates the creativity, problem-solving skills, and impact of these employee-driven initiatives, which help drive continuous improvement across the organization.

3. The progress of key projects for continuous improvements is monitored regularly during the monthly management reviews. These reviews provide a structured forum for the leadership team to assess the status, challenges, and outcomes of various initiatives aimed at enhancing the company's GRC capabilities. The discussions cover topics such as the implementation timelines, resource allocation, risk mitigation strategies, and the realization of expected benefits. This regular review process helps ensure that the improvement efforts remain on track, emerging issues are promptly addressed, and key learnings are incorporated to drive continuous enhancements to the company's overall strategy.
4. The company has started to implement a robust Learning Management System to support the continuous development and upskilling of its employees. The LMS provides a centralized platform for delivering, tracking, and reporting on various training programs, including those focused on enhancing the organization's GRC capabilities. By leveraging the LMS, the company can ensure that its workforce is equipped with the necessary knowledge, skills, and competencies.
5. The company has embraced a culture of continuous improvement, with a strong emphasis on driving innovation and digital transformation to streamline operations and enhance business resilience.
6. The company has established a dedicated GRC function that works closely with the business units to continuously monitor and improve the design and implementation of the GRC framework.

Improvement Opportunities:

1. The methodology used to continuously improve the company's Governance, Risk, and Compliance capability could be further formalized and documented. This should include a clearly defined process for identifying, prioritizing, managing, and reporting on improvement initiatives that can be incorporated into the Integrated Plan. Formalizing and documenting this process would help promote consistency,

transparency, and accountability across the organization. The process could involve establishing structured procedures for gathering feedback from relevant stakeholders, analyzing performance data, and evaluating the impact of potential improvements. By documenting the end-to-end GRC capability improvement methodology, the company can ensure a systematic and well-governed approach to driving continuous enhancements to its GRC framework.

2. The company could consider implementing a dedicated GRC technology platform or integrated suite of tools to enhance the automation, integration, and reporting capabilities of its Governance, Risk, and Compliance activities. The deployment of a centralized GRC system could enable more efficient data management, risk assessment, control monitoring, and compliance reporting across the organization.

3. The company should formalize and document a structured process to incorporate recommendations from investigations and issue resolutions into the continuous improvement of its Governance, Risk, and Compliance capabilities (Anon, Filowitz, and Kovatch 2007). This would help ensure a systematic and well-governed approach to driving enhancements to the GRC framework based on feedback and learnings derived from various review and remediation activities.

4. Risk mitigation action plan implementation progress could be monitored more closely, with clearly defined accountability and timelines. RACI matrices could be introduced to clarify the roles and responsibilities of key stakeholders involved in the execution and oversight of risk mitigation initiatives.

5. The process for systematically tracking the implementation and effectiveness of audit recommendations could be further strengthened. This could involve establishing a centralized repository or dashboard to monitor the status of audit recommendations, the timeliness of management responses, and the realized benefits of implemented corrective actions. Periodic reviews of the audit recommendation tracking process, including analyzing key performance metrics and soliciting feedback from audit stakeholders, would help ensure the process remains effective and responsive to the organization's evolving needs.

6. Risk monitoring can be quantified and measured more effectively through the development and adoption of meaningful key risk indicators and key performance indicators.

7. GRC steering committee could be formed to provide strategic oversight and guidance on the continuous improvement of the company's Governance, Risk, and Compliance capabilities.

8. Repetitive findings or issues identified across multiple audits and reviews can be analyzed to pinpoint the underlying root causes. By taking a holistic approach to addressing these recurring problems, the company can develop more comprehensive mitigation strategies that tackle the core issues rather than just the symptoms. Furthermore, these repetitive findings can be transformed into key performance indicators to enable the ongoing tracking and monitoring of the recurrence of such issues. This proactive approach can help the company strengthen its overall Governance, Risk, and Compliance framework by identifying patterns, addressing systemic weaknesses, and implementing effective controls to prevent the reoccurrence of similar problems in the future.

9. Budget allocation should be optimized to align with the priorities identified through the risk assessment and management processes. Securing sufficient resources to support the continuous improvement of the company's GRC capabilities should be a key consideration in the budgeting and resource allocation decisions.

10. Rewards and recognition programs can be leveraged to incentivize employees to actively participate in and contribute to the continuous improvement of the company's Governance, Risk, and Compliance framework (Anon, Filowitz, and Kovatch 2007). This could include providing financial incentives, career development opportunities, or public acknowledgment for employees who demonstrate exemplary efforts in enhancing the organization's GRC capabilities. Conversely, disciplinary measures or performance management processes may be utilized to address instances where employees fail to comply with established GRC policies and procedures, in order to reinforce the importance of effective Governance, Risk, and Compliance practices throughout the organization.

CHAPTER 6
SUMMARY AND CONCLUSION

6.1. Summary and Key Findings

The case study utilizes primary data sources, such as direct observation and document/record review, to assess the company's implementation of an integrated Governance, Risk, and Compliance framework. The analysis reveals that the company has made significant strides in establishing a comprehensive GRC program, including the development of a centralized risk management process, the implementation of a robust internal control environment, and the adoption of various compliance monitoring mechanisms. However, the study also identifies several opportunities for improvement to further enhance the company's GRC capabilities and drive continuous performance optimization.

The case study demonstrates that Company X has made progress in implementing an integrated Governance, Risk, and Compliance framework to enhance its Enterprise Risk Management capabilities. The company has established a dedicated GRC function that works closely with the business units to continuously monitor and improve the design and implementation of the GRC framework.

Some of the key findings from the case study include:

1. The company has made progress in implementing an integrated Governance, Risk, and Compliance framework, which has enabled a more holistic and coordinated approach to managing various aspects of risk, compliance, and control across the organization. The GRC framework has helped the company take a more comprehensive view of its risk landscape and align its risk management, compliance, and control activities to enhance its overall Enterprise Risk Management capabilities.
2. The company has established a dedicated GRC function that collaborates with the business units to oversee the implementation and continuous improvement of the GRC framework. The GRC function plays a pivotal role in driving the integration of risk management, compliance, and control activities, as well as ensuring consistent application of policies, standards, and procedures across the organization.

3. The company has made efforts to strengthen its risk assessment and management processes, including the development of a risk management framework, processes, and reporting mechanisms. However, there are opportunities to further enhance the risk assessment and prioritization methodologies, and to strengthen the monitoring and reporting of key risk indicators and control effectiveness (Papazafeiropoulou & Spanaki, 2015).
4. The company has implemented a digital transformation initiative to strengthen its Governance, Risk, and Compliance framework. This digital transformation has enabled the company to automate and streamline its controls, risk monitoring, compliance monitoring, and performance monitoring processes. By leveraging digital technologies, the company has been able to enhance the efficiency, effectiveness, and visibility of its GRC activities, leading to improved risk management, compliance, and overall enterprise performance.
5. The company has established an internal audit function that provides independent and objective assurance on the design and operating effectiveness of the GRC framework. However, there are opportunities to further enhance the internal audit function's ability to provide timely and actionable insights, including through improved tracking of audit (Lehmann, 2010)

The case study of Company X's implementation of an integrated Governance, Risk, and Compliance framework to enhance its Enterprise Risk Management capabilities provides valuable insights and lessons learned. The key findings highlight the importance of adopting a holistic and integrated approach to GRC, establishing a dedicated GRC function, strengthening risk assessment and management processes, leveraging digital technologies, and enhancing the internal audit function's ability to provide timely and actionable insights. Specifically, the case study demonstrates that Company X has made progress in integrating its risk management, compliance, and control activities through the GRC framework, which has enabled a more comprehensive view of the organization's risk landscape. The establishment of a dedicated GRC function has played a pivotal role in driving this integration and ensuring consistent application of policies, standards, and procedures across the company. However, the case study also identifies opportunities to further enhance the risk assessment and prioritization methodologies, as well as to strengthen the monitoring and reporting of key risk indicators and control

effectiveness. Additionally, the case study highlights Company X's successful digital transformation initiative, which has enabled the automation and streamlining of its GRC processes, leading to improved efficiency, effectiveness, and visibility. Finally, the case study points to the need to enhance the internal audit function's ability to provide timely and actionable insights to support the continuous improvement of the GRC framework.

The case study of Company X's implementation of an integrated Governance, Risk, and Compliance framework provides valuable insights and lessons that can be applied by other organizations seeking to enhance their Enterprise Risk Management capabilities. The case study demonstrates the importance of adopting a holistic and integrated approach to GRC, which can enable a more comprehensive view of an organization's risk landscape and better align its risk management, compliance, and control activities. The key findings highlight the critical role of a dedicated GRC function in driving this integration and ensuring consistent application of policies, standards, and procedures across the organization. Additionally, the case study underscores the value of leveraging digital technologies to automate and streamline GRC processes, leading to improved efficiency, effectiveness, and visibility. Finally, the case study emphasizes the need to enhance the internal audit function's ability to provide timely and actionable insights to support the continuous improvement of the GRC framework. Overall, the lessons learned from Company X's experience can serve as a valuable reference for other organizations seeking to strengthen their Enterprise Risk Management through the implementation of an integrated GRC approach.

6.2. Limitation of the Study

The case study of Company X's implementation of an integrated Governance, Risk, and Compliance framework is limited in its scope and may not be fully representative of the challenges and considerations faced by all organizations in implementing a GRC framework. Specifically, the case study focuses on a single organization within the pharmaceutical industry in Indonesia, and the findings may not be directly applicable to organizations in other sectors, geographies, or with different organizational structures, resources, and risk profiles. The insights and lessons learned from this case study should be considered within the appropriate context and may require further validation or adaptation to suit the specific needs and circumstances of other organizations interested in implementing an integrated GRC framework.

6.3. Recommendations for Future Research

Building on the findings and insights from the case study of Company X, future research could explore the following areas:

1. Comparative analysis of GRC implementation approaches and their effectiveness across different industries and organizational contexts: This could provide a more comprehensive understanding of the factors that influence the success or challenges of GRC implementation and help identify best practices that can be applied more broadly.
2. Examination of the role of organizational culture and change management in the successful implementation of integrated GRC frameworks: The case study suggests that organizational culture and the ability to effectively manage change are critical factors in the success of GRC implementation, and further research could explore these dynamics in more depth.
3. Evaluation of the impact of integrated GRC frameworks on Enterprise Risk Management and organizational performance: While the case study highlights the potential benefits of an integrated GRC approach, further research could quantify the measurable impacts on risk mitigation, compliance, and financial and operational performance.
4. Exploration of the evolving role of internal audit in supporting the continuous improvement of GRC frameworks: The case study identifies the need to enhance the internal audit function's ability to provide timely and actionable insights, and further research could investigate the best practices and competencies required for internal audit to fulfill this role effectively.
5. Investigation of the technological and digital transformation challenges in GRC implementation: The case study emphasizes the importance of leveraging digital technologies to automate and streamline GRC processes, and additional research could delve into the specific technological and change management challenges organizations face in this area.
6. Examination of the role of governance and leadership in driving the successful adoption of integrated GRC frameworks: The case study suggests that strong governance and committed leadership are critical success factors, and further research could explore the

specific governance structures, decision-making processes, and leadership attributes that enable effective GRC implementation.

7. The impact of GRC on Enterprise Risk Management can be explored through a mixed-methods study, combining a quantitative analysis of key performance indicators with qualitative insights from interviews with key stakeholders and subject matter experts.

8. Conducting an empirical study to examine the relationship between the implementation of an integrated Governance, Risk, and Compliance framework and the overall effectiveness of enterprise-wide risk management within organizations. This study could explore the influence of key factors, such as the organization's structural design, prevailing risk culture, and the maturity of existing risk management practices, on the successful integration and impact of GRC initiatives. By taking a comprehensive, multi-faceted approach, the research could provide valuable insights into the critical elements that enable organizations to leverage GRC as a strategic tool to enhance their enterprise-wide risk management capabilities.

9. The current study primarily focuses on the successes and areas for improvement identified from Company X's GRC implementation. Future research could build on this by conducting a comprehensive GRC maturity level assessment. This would provide a more detailed analysis of the current state of GRC implementation, allowing researchers to pinpoint the specific areas that require further strengthening and optimization within the organization. By assessing the maturity of GRC across key domains such as governance, risk management, compliance, and supporting processes, future studies can offer more granular insights to guide the continuous improvement of the integrated GRC framework at Company X and similar organizations.

By exploring these areas, future research can build upon the insights gained from the case study of Company X and contribute to a more comprehensive understanding of the key considerations, best practices, and success factors in implementing integrated Governance, Risk, and Compliance frameworks to enhance Enterprise Risk Management within organizations.

REFERENCES

Abdullah, Hanifa. 2019. "Analyzing the technological challenges of Governance, Risk and Compliance (GRC)" https://doi.org/10.1109/iceeccot46775.2019.9114642.

Alharbi, Fawaz, Mohammed Nour A. Sabra, Nawaf Alharbe, and Abdulrahman A. Almajed. 2022. "Towards a Strategic IT GRC Framework for Healthcare Organizations" Science and Information Organization 13 (1). https://doi.org/10.14569/ijacsa.2022.0130125.

Andronache, A., Brunel University London, Althonayan, A., Brunel University London, Matin, M., & Brunel University London. (2021). Relevance of GRC in Expanding the Enterprise Risk Management Capabilities. In *Conference Paper*. https://www.researchgate.net/publication/354035618

Anon, Louis, J., Harry Filowitz, and Jeffrey M. Kovatch. 2007. "Integrating Sarbanes- Oxley controls into an investment firm governance framework" Emerald Publishing Limited 8 (1) : 40-43. https://doi.org/10.1108/15285810710739364.

Antikarov, Vladimir. 2012. "Enterprise Risk Management for Nonfinancial Companies: From Risk Control and Compliance to Creating Shareholder Value" RELX Group (Netherlands). https://doi.org/10.2139/ssrn.2571500.

Azhar, Murdifin, and Yan Rahadian. 2022. "THE EVALUATION OF PT.X READINESS IN IMPLEMENTING GOVERNANCE, RISK, AND COMPLIANCE"

Azizah, Amiril & Diah, Ahyar & Wulaningrum, Ratna. (2022). The Impact of Risk Management on Firm Performance. 10.2991/assehr.k.220301.139.

Batenburg, Ronald & Neppelenbroek, Matthijs & Shahim, Abbas. (2014). A maturity model for governance, risk management and compliance in hospitals. Journal of Hospital Administration. 3. 10.5430/jha.v3n4p43.

Bolboli, Amir, Seyed, and Markus Reiche. 2014. "Culture-based design and implementation of business excellence" Emerald Publishing Limited 26 (4) : 329-347. https://doi.org/10.1108/tqm-01-2014-0015.

Brody, G., Richard. 2010. "Beyond the basic background check: hiring the "right" employees" Emerald Publishing Limited 33 (3) : 210-223. https://doi.org/10.1108/01409171011030372.

BS ISO 31000:2018

Burnaby, Priscilla, and Susan Hass. 2009. "Ten steps to enterprise- wide risk management" Emerald Publishing Limited 9 (5) : 539-550. https://doi.org/10.1108/14720700910998111.

Chandani, Arti, and Mita Mehta. 2020. "Corporate Governance in Indian perspective: A case of Grasim Industries" 07 (02) : 37-47. https://doi.org/10.30726/ijmrss/v7.i2.2020.72008.

Costa, da, Paulino, Paula, Ana. 2017. "Corporate Governance and Fraud: Evolution and Considerations" https://doi.org/10.5772/intechopen.68489.

Craig, W., Gary. 2020. "Cultural Assessment: Considerations, Approaches, and Implications" Wiley 59 (5) : 26-37. https://doi.org/10.1002/pfi.21915.

CRMS Indonesia (2022). It's Time to Realize GRC Implementation with an Integrated Approach. URL: https://crmsindonesia.org/publications/saatnya-merealisasikan-implementation-grc-with-integrated-approach/. Retrieved October 2023

Engemann, J., Kurt. 2019. "Emerging developments in organizational risk" Emerald Publishing Limited 1 (1) : 26-35. https://doi.org/10.1108/crr-03-2019-0011.

Francis, Sebastian, and Bob Paladino. 2008. "Enterprise risk management: A best practice approach" Wiley 19 (3) : 19-33. https://doi.org/10.1002/jcaf.20382.

Long, G. (Gary). (2017). *The Importance of GRC in the Enterprise*. https://ssrn.com/abstract=2951123

Ghezzi, Antonio. 2013. "Revisiting business strategy under discontinuity" Emerald Publishing Limited 51 (7) : 1326-1358. https://doi.org/10.1108/md-05-2012-0388.

Govindji, Shree & Peko, Gabrielle & Sundaram, David. (2018). A Context Adaptive Framework for IT Governance, Risk, Compliance and Security. 10.1007/978-3-319-77818-1_2.

Graham, R., John, Jillian Grennan, Campbell R. Harvey, and Shivaram Rajgopal. 2022. "Corporate culture: Evidence from the field" Elsevier BV 146 (2) : 552-593. https://doi.org/10.1016/j.jfineco.2022.07.008.

GRC Forum Indonesia (2020). Guide to Achieving the Governance, Risk, and Compliance (GRC) Model of Excellence.

Griffis, E., Stanley, and Judith M. Whipple. 2012. "A Comprehensive Risk Assessment and Evaluation Model: Proposing a Risk Priority Continuum" Penn State University Press 51 (4) : 428-451. https://doi.org/10.5325/transportationj.51.4.0428.

Griffy- Brown, Charla, Howard A. Miller, Vincent Zhao, Demetrios Lazarikos, and Mark Chun. 2019. "Emerging Technologies and Risk: How Do We Optimize Enterprise Risk When Deploying Emerging Technologies?" https://doi.org/10.1109/temscon.2019.8813743.

Hey, Bruce, Robert. 2017. "Governance Framework"

Johnson, Leighton. 2015. "Statutory and Regulatory GRC" Elsevier BV : 11-33. https://doi.org/10.1016/b978-0-12-802324-2.00003-8.

Jun, Hannah, and Minseok Kim. 2021. "From Stakeholder Communication to Engagement for the Sustainable Development Goals (SDGs): A Case Study of LG Electronics" Multidisciplinary Digital Publishing Institute 13 (15) : 8624-8624. https://doi.org/10.3390/su13158624.

Kalaimani, Jayaraman. 2016. "SAP Governance, Risk, and Compliance" : 235-246. https://doi.org/10.1007/978-1-4842-1389-6_18.

Knechel, Robert, W., Gopal V. Krishnan, Mikhail Pevzner, Lori Shefchik Bhaskar, and Uma Velury. 2012. "Audit Quality Indicators: Insights from the Academic Literature" RELX Group (Netherlands). https://doi.org/10.2139/ssrn.2040754.

Lehmann, M., Constance. 2010. "Internal Controls: A Compendium of Short Cases" American Accounting Association 25 (4) : 741-754. https://doi.org/10.2308/iace.2010.25.4.741.

Lieber, D., Lynn. 2010. "HR's role in creating and maintaining a code of conduct to promote an ethical organizational culture" Wiley 37 (1) : 99-106. https://doi.org/10.1002/ert.20290.

Li, Qiuying & Wu, Yue & Ojiako, Udechukwu & Marshall, Alasdair & Chipulu, Max. (2014). Enterprise risk management and firm value within China's insurance industry. Acta Commercii. 14. 10.4102/ac.v14i1.198.

Marchetti, M., Anne. 2012. "The Time has Come for ERM" : 39-56. https://doi.org/10.1002/9781119201502.ch3.

Marwitz, Steve, Neil Maxson, Bill Koch, Todd Aukerman, Jim Cassidy, and David Belonger. 2007. "Corporate Crisis Management: Managing a Major Crisis in a Chemical Facility"

Merna, Anthony, and Tony Merna. 2004. "Development of a Model for Risk Management at Corporate, Strategic Business, and Project Levels" Euromoney Institutional Investor 10 (1) : 79-85. https://doi.org/10.3905/jsf.2004.79.

Mitchell, Scott. (2007). GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance. 4. 279-296. 10.1057/palgrave.jdg.2050066.

Mollahoseini, Ali, and Shahrooz Farjad. 2012. "Assessment Effectiveness on the Job Training in Higher Education (Case Study: Takestan University)" Elsevier BV 47 : 1310-1314. https://doi.org/10.1016/j.sbspro.2012.06.817.

Morgunova, P., E., and G I Bolkina. 2020. "ERM for an Insurer: Challenges and Prospects" Atlantis Press. https://doi.org/10.2991/aebmr.k.200312.199.

Murray, P., J., and W Roger. 2018. “Promoting Enterprise Risk Management (ERM) and Governance, Risk and Compliance (GRC) for Managing Cybersecurity Risks” University of Maryland Baltimore. https://archive.hshsl.umaryland.edu/handle/10713/7891?show=full

OCEG. 2024. "GRC Capability Model Version 3.5" OCEG Version 3.5. https://www.oceg.org/grc-capability-model-red-book/

OCEG. 2024. "Integrated Risk Management Framework"

OECD. 2023. "G20/OECD Principles of Corporate Governance 2023" OECD. https://doi.org/10.1787/ed750b30-en.

Papazafeiropoulou, Anastasia, and Konstantina Spanaki. 2015. "Understanding governance, risk and compliance information systems (GRC IS): The experts view" Springer Science+Business Media 18 (6) : 1251-1263. https://doi.org/10.1007/s10796-015-9572-3.

Posthumus, Shaun. (2004). A framework for the governance of information security. Computers & Security. 23. 638-646. 10.1016/j.cose.2004.10.006.

Ross, W., Jeanne, and Cynthia Mathis Beath. 2007. "Agility and Risk Management at Pacific Life: Optimizing Business Unit Autonomy" RELX Group (Netherlands). https://doi.org/10.2139/ssrn.1114796.

Şenol, Zekai & Karaca, Süleyman. (2017). The Effect of Enterprise Risk Management on Firm Performance: A Case Study on Turkey.

Siahaan, Magda, Harry Suharman, Tettet Fitrijanti, and Haryono Umar. 2022. "Will the integrated GRC implementation be effective against corruption?" Emerald Publishing Limited 30 (1) : 24-34. https://doi.org/10.1108/jfc-12-2021-0275.

Ugoani, John. (2021). Corporate governance perspective on enterprise risk management and organizational sustainability. Independent Journal of Management & Production. 12. 1496-1517. 10.14807/ijmp.v12i5.1403.

Vicente, P., Mira Da Silva, M., & Instituto Superior T´ecnico, Universidade T´ecnica de Lisboa. (2011). A Conceptual Model for Integrated Governance, Risk and Compliance. In CAiSE 2011 (Vols. 6741–6741, pp. 199–213).

Vom Brocke, J., ERCIS - European Research Center for Information Systems, Schmiedel, T., & University of Applied Sciences and Arts Northwestern Switzerland. (2011). Culture in Business Process Management: A Literature Review. *Business Process Management Journal*. https://doi.org/10.1108/1463715122383

Vunk, M., Mayer, N., Matulevičius, R. (2017). A Framework for Assessing Organisational IT Governance, Risk and Compliance. In: Mas, A., Mesquida, A., O'Connor, R., Rout, T., Dorling, A. (eds) Software Process Improvement and Capability Determination. SPICE 2017. Communications in Computer and Information Science, vol 770. Springer, Cham. https://doi.org/10.1007/978-3-319-67383-7_25

Wang, Chunhong, Minru Zhao, and Zhenhua Zhang. 2021. "Research on the Relationship Between Corporate Governance Performance and Financing Cost Under the Background of ESG Theory" EDP Sciences 235 : 01054-01054. https://doi.org/10.1051/e3sconf/202123501054.

Wankhade, Paresh, and J. A. Brinkman. 2014. "The negative consequences of culture change management" Emerald Publishing Limited 27 (1) : 2-25. https://doi.org/10.1108/ijpsm-05-2012-0058.

Zaydi, M., & Nassereddine, B. (2018). Toward a New Integrated Approach of Information Security Based on Governance, Risk and Compliance. In *Smart innovation, systems and technologies* (pp. 337–341). https://doi.org/10.1007/978-3-030-03577-8_37

Zsidisin, A., George, Alex Panelli, and R. Travis Upton. 2000. "Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study" Emerald Publishing Limited 5 (4) : 187-198. https://doi.org/10.1108/13598540010347307.