

ENTERPRISE RISK MANAGEMENT AS A CATALYST FOR STRATEGIC  
GOVERNANCE, RISK, AND COMPLIANCE (GRC)  
ALIGNMENT IN IT COMPANIES

by

Karan Kumar, PGDIT, MBA, BA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

OCTOBER, 2024

ENTERPRISE RISK MANAGEMENT AS A CATALYST FOR STRATEGIC  
GOVERNANCE, RISK, AND COMPLIANCE (GRC)  
ALIGNMENT IN IT COMPANIES

by

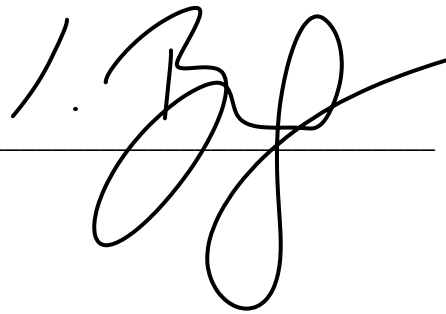
Karan Kumar

Supervised by

Dr. Mario Silic

APPROVED BY

\_\_\_\_\_  
Dissertation chair

A handwritten signature in black ink, appearing to be 'M. Silic', written over a horizontal line. The signature is stylized and cursive.

RECEIVED/APPROVED BY:

\_\_\_\_\_  
Admissions Director

## **Dedication**

This DBA research project is dedicated to the many persons and groups who have helped me along my academic and personal path, making this accomplishment possible.

To my dear family, whose unfailing love and encouragement have been my continual source of strength. To my parents, who taught me the value of education and the necessity of perseverance, and to my siblings, who have been by my side through thick and thin, always cheering me on.

To my spouse, whose love, patience, and understanding have served as the foundation for my life. Even when I doubted myself, your conviction in my ability served as a beacon of light, guiding me through the most difficult circumstances. To my children, whose innocent grins and boundless curiosity have encouraged me to strive for perfection and be a role model for lifelong learning.

To my mentors and advisors, whose wisdom, guidance, and skill helped define my academic career. Your commitment to my academic development has been critical in achieving this milestone. Special thanks to my dissertation advisor, whose insightful feedback and persistent support were critical to the completion of this project.

To my friends and coworkers who have been a source of encouragement, friendship, and intellectual stimulation. Your encouragement, whether via intellectual conversations or simple words of motivation, has been essential.

To my research participants, whose willingness to share their time and insights was critical to the study's success. Your contributions have been critical in increasing our understanding of the subject.

Finally, I want to thank everyone who has believed in me and supported me from afar. Your silent encouragement has not gone forgotten. Each of you has had a role in our trip, and I am deeply appreciative.

This work reflects many people's joint efforts, sacrifices, and support. I commend this accomplishment to all of you, with sincere admiration and genuine gratitude.

## **Acknowledgements**

The completion of this doctoral research project would not have been possible without the assistance, direction, and encouragement of several persons and institutions. I'd like to take this moment to thank everyone who has helped make this journey possible.

First and foremost, I want to express my heartfelt gratitude to my dissertation mentor and adviser, Dr. Mario Silic, whose excellent assistance, insightful input, and continual support have helped shape this research. Your skill and dedication have considerably enhanced my academic experience, and I am really thankful for your consistent support during this process.

I am also indebted to the members of my dissertation committee, for their time, constructive criticism, and insightful suggestions, which have significantly contributed to the refinement and completion of this research. Your diverse perspectives and expertise have been crucial in enhancing the quality of this work.

My heartfelt appreciation goes to the faculty and staff of the SSBM Geneva, whose support and resources have been vital in my academic journey. Special thanks to Dr. Mario Silic for providing the necessary administrative and logistical assistance.

I am deeply grateful to the participants of my research study, whose willingness to share their experiences and insights has been fundamental to the success of this work. Without their cooperation and openness, this research would not have been possible.

A special note of thanks to my colleagues and peers, whose camaraderie, intellectual exchange, and moral support have been a source of motivation and inspiration. Our discussions and collaborative efforts have enriched my understanding and perspective, contributing significantly to this research.

I would like to express my deepest gratitude to my family, whose unconditional love, patience, and support have been my anchor throughout this journey. To my parents, for instilling in me the values of hard work and perseverance. To my spouse, Shaifali Bhatnagar for your unwavering belief in me, and to my children, Kavya Karan, for their understanding and sacrifices.

Finally, I would like to acknowledge all my friends, both near and far, for their encouragement and support. Your words of motivation and understanding have been a source of strength.

To all those who have touched my life and contributed to this achievement, I extend my heartfelt thanks. This journey has been a collective effort, and I am forever grateful for your support and encouragement.

ABSTRACT

ENTERPRISE RISK MANAGEMENT AS A CATALYST FOR STRATEGIC  
GOVERNANCE, RISK, AND COMPLIANCE (GRC)  
ALIGNMENT IN IT COMPANIES

Karan Kumar  
2024

Dissertation Chair: <Chair's Name>  
Co-Chair: <If applicable. Co-Chair's Name>

Enterprise Risk Management (ERM) is increasingly recognized as a strategic mechanism for fostering alignment among IT companies' Governance, Risk, and Compliance (GRC) functions. Such alignment enables companies to respond effectively to dynamic risk landscapes and regulatory demands while supporting resilience and strategic flexibility. This study examines ERM as a catalyst for GRC alignment, focusing on the role of stakeholder influence, the effectiveness of alignment strategies, the utility of assessment tools, and the barriers encountered in achieving cohesive ERM-GRC integration.

The role of key stakeholders, including board members, senior management, and regulatory bodies, is pivotal in shaping the priorities and approaches within ERM-GRC alignment processes. Their influence is not limited to setting alignment objectives, but

also extends to actively shaping the success of strategic initiatives aimed at achieving coherence across governance, risk, and compliance domains. The study delves into the influence of these stakeholders, revealing that their engagement is a fundamental component of successful ERM-GRC alignment.

To evaluate alignment progress, the study also assesses the tools and techniques employed by IT companies, such as automated GRC platforms, data analytics tools, and real-time risk monitoring systems. The effective use of these tools provides organizations with valuable insights into alignment status, helping them identify gaps, mitigate potential risks, and refine their approaches. However, the research identifies various challenges that hinder alignment efforts, including the complexity of integrating diverse compliance requirements, resource constraints, and the evolving nature of regulatory standards. Quantitative analysis highlights that these challenges are particularly pronounced in rapidly evolving IT environments, where agility and adaptability are essential.

Overall, this study demonstrates that successful ERM-GRC alignment in IT companies depends heavily on stakeholder engagement, strategic adaptability, and the strategic selection of assessment tools. By addressing identified challenges, IT companies can leverage ERM to enhance governance, manage risks proactively, and maintain compliance more effectively, ultimately supporting organizational resilience and long-term strategic growth.

**Key words:** Enterprise Risk Management, ERM, Catalyst, Strategic Governance, Risk, Compliance, GRC, GRC Alignment, IT Companies, Challenges in ERM-GRC Alignment



## TABLE OF CONTENTS

List of Figures .....	xi
CHAPTER I: INTRODUCTION.....	1
1.1 Background of study .....	1
1.2 Evolution of ERM and GRC Frameworks in IT .....	2
1.3 Importance of ERM in IT Sector .....	4
1.4 Overview of Enterprise Risk Management (ERM).....	10
1.5 GRC: Governance, Risk, and Compliance in IT Companies.....	12
1.6 Problem Statement .....	15
1.7 Research Objectives.....	16
1.8 Research Questions .....	16
1.9 Significance of the Study .....	17
1.10 Structure of the Thesis .....	19
CHAPTER II: REVIEW OF LITERATURE .....	21
2.1 Theoretical Foundations for ERM-GRC Alignment.....	21
2.2 Governance, Risk, and Compliance (GRC) Frameworks in IT Companies .....	24
2.3 Evolution of ERM and GRC Frameworks in IT .....	29
2.4 Theoretical Foundations for ERM-GRC Alignment.....	34
2.5 Benefits of ERM-Driven GRC Alignment in IT Companies.....	38
2.6 Challenges of Implementing ERM-GRC Alignment in IT Companies .....	42
2.7 Emerging Trends in ERM and GRC Alignment for IT .....	47
2.8 Summary .....	51
CHAPTER III: METHODOLOGY .....	53
3.1 Overview of the Research Problem .....	53
3.2 Operationalization of Theoretical Constructs .....	55
3.3 Research Purpose and Questions .....	59
3.4 Research Design .....	59
3.5 Population and Sample.....	63
3.6 Participant Selection .....	67
3.7 Instrumentation .....	71
3.8 Data Collection Procedures.....	77
3.9 Data Analysis .....	82
3.10 Research Design Limitations .....	88
3.11 Conclusion .....	91
CHAPTER IV: RESULTS.....	93
4.1 Data collections and analysis process .....	93

4.2 Descriptive Statistics .....	95
4.3 Inferential Statistics for Assessing Stakeholder Influence on ERM-GRC Processes	100
4.4 Inferential Statistics for Evaluating the Effectiveness of Strategies for ERM-GRC Alignment .....	121
4.5 Inferential Statistics for Evaluation of Tools and Techniques for ERM-GRC Alignment Assessment.....	138
4.6 Inferential Statistics for Challenges to ERM-GRC Alignment.....	155
4.7 Final Summary .....	175
 CHAPTER V: DISCUSSION.....	 178
5.1 Discussion of Results .....	178
5.2 Discussion on Stakeholder Influence on ERM-GRC Alignment in IT Companies..	178
5.3 Discussion on Effectiveness of Strategies for ERM-GRC Alignment in IT Companies .....	179
5.4 Discussion on Top Tools and Techniques for Assessing ERM-GRC Alignment in IT Companies .....	180
5.5 Discussing on Key Challenges in ERM-GRC Alignment in IT Companies: Insights from Quantitative Analysis .....	180
5.6 Conclusion .....	181
 CHAPTER VI: SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS.....	 183
6.1 Summary .....	183
6.2 Implications .....	184
6.3 Recommendations for Future Research .....	185
6.4 Conclusion .....	185
 APPENDIX A SURVEY COVER LETTER .....	 188
 REFERENCES .....	 197

## LIST OF FIGURES

Figure 1 Likert Scale.....	93
Figure 2 Data Cleaning-Shortened the names .....	94
Figure 3 Data Cleaning-Mapping to ordinal values.....	94
Figure 4 Division of dataframes into 5 sections .....	95
Figure 5 Belonging to Risk Management Domain .....	95
Figure 6 Proportion of Gender .....	96
Figure 7 Proportion of Age Group.....	97
Figure 8 Proportion of Educational Background .....	98
Figure 9 Proportion of Industry Experience .....	98
Figure 10 Involvement in Risk Assessment.....	99
Figure 11 Histograms.....	101
Figure 12 Correlation Matrix of Responses.....	104
Figure 13 Results of Krushkal Wallis Test .....	109
Figure 14 With involvement of risk assessment activities.....	113
Figure 15 Cliff’s Delta with risk management .....	117
Figure 16 Cliff’s Delta with risk assessment .....	119
Figure 17 Histograms.....	122
Figure 18 Correlation Matrix of Responses.....	125
Figure 19 Kruskal Wallis Test .....	128
Figure 20 Being involved in risk assessment activities .....	131
Figure 21 With risk management domain.....	134
Figure 22 Being involved in risk assessment activities .....	136
Figure 23 Histograms of all variables .....	139
Figure 24 Correlation matrix of variables.....	142
Figure 25 Kruskal Wallis test with risk management domain .....	145
Figure 26 Kruskal wallis test with being involved in risk assessment .....	148
Figure 27 With risk management domain.....	151
Figure 28 Being involved in risk assessment.....	153
Figure 29 Histogram for inexperience in Risk Assessment.....	156

Figure 30 Histograms for all variables.....	158
Figure 31 Correlation Matrix of Responses.....	161
Figure 32 Kruskal Wallis Test Results .....	164
Figure 33 With being involved in risk assessment .....	167
Figure 34 With risk management domain.....	170
Figure 35 With being involved in risk assessment activities.....	173

## CHAPTER I: INTRODUCTION

### **1.1 Background of study**

In today's rapidly evolving IT landscape, organizations face complex challenges in balancing operational efficiency with regulatory compliance, risk management, and governance standards. As organizations grow, so does the intricacy of risks they encounter, from cybersecurity threats and data privacy issues to shifting regulatory requirements and stakeholder expectations (Mikes & Kaplan, 2015; Hoyt & Liebenberg, 2011). Enterprise Risk Management (ERM) has emerged as a strategic approach to addressing these risks, enabling companies to embed risk management into their core processes and decision-making frameworks (Power, 2009; Beasley, Clune & Hermanson, 2005). For IT companies, in particular, the integration of ERM with Governance, Risk, and Compliance (GRC) frameworks has become a crucial strategy to enhance organizational resilience and ensure the alignment of risk management with overall business objectives (Frigo & Anderson, 2011).

ERM in IT companies is not only a protective mechanism but also a driver of strategic alignment. By synchronizing risk management efforts with governance and compliance processes, IT organizations can create a more cohesive and proactive approach to navigating their risk landscape (Racz, Weippl & Seufert, 2010). The alignment of ERM and GRC is vital for organizations aiming to maintain a competitive edge, avoid compliance penalties, and build trust with stakeholders (Ashby, Palermo & Power, 2012; Freeman, 1984). Thus, understanding how ERM can act as a catalyst for GRC alignment is of increasing importance, particularly in sectors where digital innovation and rapid adaptation are crucial for success (Gates, Nicolas & Walker, 2012; Barney, 1991).

## **1.2 Evolution of ERM and GRC Frameworks in IT**

The evolution of Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) frameworks in Information Technology (IT) has undergone a significant transformation, expanding from isolated, department-specific risk mitigation strategies to integrated systems that support organizational resilience, regulatory compliance, and strategic growth. Initially, ERM in IT began as a reactive measure, primarily focused on mitigating isolated risks within departmental silos. This approach created fragmented risk management practices that restricted the organization's ability to coordinate effectively across departments, often resulting in duplicated efforts and missed insights. According to a Deloitte report, 59% of organizations initially managed IT risks separately from other enterprise risks, contributing to disjointed governance structures and limited response efficiency (Deloitte, 2019).

A pivotal shift occurred in the early 2000s with the introduction of regulatory mandates such as the Sarbanes-Oxley Act (SOX) of 2002 in the United States. This law mandated strict internal controls for financial reporting, compelling organizations to establish governance structures that ensured regulatory compliance while minimizing operational risks. This legislation marked the emergence of GRC frameworks designed to align IT practices with broader organizational governance and compliance requirements. According to PwC, 91% of surveyed organizations stated that compliance with SOX was a significant driver for adopting GRC frameworks, establishing GRC as an essential component of IT and enterprise risk management practices (PwC, 2020).

As businesses recognized the benefits of a unified governance, risk, and compliance approach, GRC frameworks evolved to include integrated risk-based decision-making. This shift allowed IT to function as a strategic enabler of enterprise-wide risk management rather than a reactive operational unit. A Gartner study revealed

that 71% of companies with an integrated GRC framework reported a marked improvement in their ability to manage risks proactively rather than reactively (Gartner, 2021). During this phase, organizations began implementing consolidated risk dashboards and cross-functional teams to foster inter-departmental alignment. The goal was to create a cohesive structure that allowed IT and other departments to assess, anticipate, and respond to risks collectively rather than addressing them in isolation.

The rapid pace of digital transformation introduced new complexities to the IT landscape, necessitating advanced GRC tools capable of managing an increasingly intricate risk environment. Automation, artificial intelligence (AI), and data analytics emerged as critical components of modern GRC frameworks, enabling real-time risk detection, compliance tracking, and predictive insights. Automated tools, such as robotic process automation (RPA), reduced manual compliance processes by 30-50%, as estimated by McKinsey, freeing IT teams to focus on higher-level strategic tasks (McKinsey & Company, 2020). Additionally, AI-driven risk models have demonstrated a 25% increase in risk identification accuracy, allowing organizations to anticipate risks and develop proactive risk-mitigation strategies (IBM, 2021). With these advancements, IT departments can streamline compliance processes and contribute to a more agile and resilient risk management structure.

In the current landscape, ERM and GRC frameworks have evolved to emphasize value creation beyond mere compliance, positioning governance and risk management as critical components of organizational strategy. Today's frameworks are designed to protect the organization from risks and enable a competitive advantage by embedding governance and risk insights into strategic planning, operational processes, and innovation initiatives. According to a recent KPMG report, 67% of business leaders view ERM and GRC as critical enablers of long-term growth and resilience, indicating a

paradigm shift in how organizations perceive the role of governance and risk (KPMG, 2022). In industries where regulatory compliance, data security, and operational efficiency are crucial, such as finance and healthcare, robust GRC frameworks have become essential in maintaining trust, ensuring data protection, and driving innovation.

Furthermore, the convergence of ERM and GRC frameworks reflects a growing recognition of the critical role of IT in enterprise success. These frameworks help organizations adapt to and thrive in an environment where risks are continually evolving, driven by factors such as cybersecurity threats, data privacy regulations, and the pressures of digital transformation. The COVID-19 pandemic underscored the need for adaptable risk management practices, as businesses with integrated GRC and ERM frameworks were found to be 45% more resilient in the face of unexpected disruptions, according to research by Forrester (Forrester, 2021). As organizations evolve, ERM and GRC frameworks will likely expand to include emerging technologies, such as blockchain for secure compliance tracking and advanced data analytics for enhanced risk modelling.

In conclusion, the evolution of ERM and GRC frameworks in IT reflects a journey from fragmented, isolated risk management practices to comprehensive, integrated frameworks that safeguard organizational interests and create value by aligning governance, risk, and compliance with corporate strategy. This evolution underscores the strategic role of IT in fostering organizational resilience, driving regulatory compliance, and enhancing competitive advantage in a dynamic and complex business environment. As organizations face new and more complex challenges, the role of ERM and GRC in IT will continue to expand, helping businesses anticipate risks, streamline compliance, and create strategic opportunities for growth and innovation.

### **1.3 Importance of ERM in IT Sector**



The IT sector places great emphasis on Enterprise Risk Management (ERM) due to the imperative of proactively identifying, assessing, and mitigating risks to ensure operational stability and overall organizational success. ERM plays a critical role in helping IT departments address a wide range of risks, including cybersecurity threats and data breaches, while also ensuring adherence to regulatory standards. Given that IT systems underpin most organizational functions, a well-executed ERM framework empowers businesses to protect their information assets and improve strategic decision-making and business resilience (PwC, 2020).

The IT sector relies heavily on ERM to address the increasing complexity of cyber risks. With a 125% surge in cybersecurity incidents over the past decade, according to IBM (2021), IT departments are in dire need of strong risk management protocols. Cyber threats like malware, phishing, and ransomware can cause significant financial and reputational harm if not managed effectively. ERM frameworks enable organizations to establish structured processes for identifying, analyzing, and mitigating these risks, thus reducing potential losses. Additionally, studies indicate that companies with active ERM practices can decrease the financial impact of cyber-attacks by an average of 20-30%, highlighting the financial advantages of a robust ERM framework (McKinsey & Company, 2020).

ERM also aids in regulatory compliance, which is crucial in industries with strict data protection requirements such as healthcare, finance, and telecommunications. In recent years, the number and scope of data privacy regulations, like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, have increased. Non-compliance with these laws can result in substantial fines and penalties, with GDPR violations alone amounting to \$1.2 billion globally in 2022 (KPMG, 2022). ERM frameworks in IT assist organizations in adhering

to these regulations by integrating compliance protocols into risk management practices, thus reducing the risk of regulatory breaches (PwC, 2020).

In addition to security and compliance, ERM in IT facilitates strategic decision-making and promotes organizational resilience. By systematically evaluating potential risks, ERM enables IT leaders to anticipate disruptions and proactively address vulnerabilities that could affect business continuity. Research by PwC (2020) indicates that 73% of organizations with comprehensive ERM frameworks are better equipped to respond to unexpected risks, ensuring business continuity and operational stability. For example, during the COVID-19 pandemic, companies with established ERM frameworks were 40% more likely to transition quickly to remote work, maintaining service levels and data security (Forrester, 2021).

It's important to note that the financial impact of unmanaged IT risks can be significant. According to McKinsey (2020), organizations without ERM frameworks are 45% more likely to experience costly system downtimes due to preventable IT issues, resulting in productivity, revenue, and customer satisfaction losses. For a mid-sized organization, downtime costs can reach up to \$300,000 per hour, making ERM an essential investment in risk mitigation. Additionally, implementing ERM can lead to a 15-20% improvement in IT operational efficiency, as it helps streamline processes, identify redundancies, and ensure effective resource allocation for risk mitigation (McKinsey & Company, 2020).

ERM also plays a crucial role in fostering a risk-aware culture across the IT organization, empowering employees at all levels to recognize and respond to risks more effectively. A Deloitte (2019) survey found that 62% of companies with a mature ERM framework reported higher levels of risk awareness and risk mitigation efforts among employees. This culture of risk awareness is particularly important in IT, where

operational errors, insider threats, and unaddressed vulnerabilities can compromise organizational security and stability. By integrating risk management into the organizational culture, ERM helps mitigate human-related risks and supports proactive risk management (Deloitte, 2019).

In today's digital landscape, where technological advancements bring both opportunities and risks, ERM serves as a foundational pillar for maintaining IT security, compliance, and operational continuity. As technology continues to evolve and new risks emerge, such as those related to AI and quantum computing, ERM will play an even more critical role in helping organizations navigate the complexities of the IT risk landscape (Gartner, 2021). In a Gartner study, 69% of CIOs indicated that effective ERM practices are central to achieving strategic IT goals, emphasizing that ERM is not just about risk prevention but also about enabling innovation and supporting business growth (Gartner, 2021).

Enterprise risk management (ERM) is essential in the IT sector, offering a methodical approach to recognizing, evaluating, and addressing risks that could jeopardize security, compliance, and business continuity. By integrating risk management with organizational goals, ERM improves strategic decision-making, reinforces operational resilience, and promotes a culture of risk awareness, positioning IT departments as proactive facilitators of business success. As the digital landscape grows more intricate, ERM's role in the IT sector will continue to broaden, ensuring that organizations can adjust to new challenges and thrive in an ever-changing environment (PwC, 2020).

### **1.1.1 Challenges of Strategic GRC Alignment**

Strategic alignment of Governance, Risk, and Compliance (GRC) frameworks is crucial for organizations seeking to integrate risk management and compliance into broader business strategies. However, it comes with various challenges. Successfully aligning GRC requires bridging complex processes across departments to support cohesive decision-making, effective risk management, and regulatory adherence. Although GRC alignment enhances resilience and supports long-term objectives, obstacles often arise, particularly regarding organizational silos, technology limitations, regulatory complexity, cultural resistance, and resource constraints.

One of the main challenges is the persistence of siloed structures within organizations. Governance, risk management, and compliance activities are often managed by separate departments, leading to fragmented processes and inconsistent reporting. These silos limit risk visibility across the enterprise and prevent effective coordination between teams. A recent study by Deloitte highlights that 64% of organizations operate with partially integrated GRC functions, which restricts a unified view of risks and increases operational inefficiencies (Deloitte, 2021). Breaking down these silos to foster cross-departmental collaboration is challenging, especially for larger organizations, yet it is crucial to create a cohesive GRC framework aligned with business strategy.

Technological limitations and data fragmentation further complicate GRC alignment. Effective GRC requires a robust technology infrastructure that supports seamless data integration, real-time monitoring, and advanced analytics. Many organizations, however, struggle with outdated systems and incompatible software across departments. According to a Gartner survey, 55% of risk and compliance leaders report that their technology infrastructure must be improved to fully support integrated GRC practices (Gartner, 2021). Fragmented data further complicates efforts to achieve

comprehensive risk analysis. Although modern GRC solutions, such as unified risk dashboards, can help, these often require substantial investment and a reallocation of IT resources toward GRC initiatives.

Regulatory complexity and dynamic compliance requirements also pose significant challenges. The regulatory landscape constantly evolves, with stringent standards varying across industries and regions. This complexity can lead to resource-intensive compliance management, as organizations must continuously adapt to new regulations. PwC found that 69% of companies struggle to keep up with regulatory changes and effectively manage compliance, which is essential to avoid fines and reputational damage (PwC, 2022). For example, global penalties for data privacy violations exceeded \$1.2 billion in 2022, highlighting the financial impact of non-compliance. Organizations need adaptive compliance processes to accommodate these changes while supporting strategic objectives, though such adaptability is challenging.

Cultural resistance within organizations often impedes successful GRC alignment as well. Embedding GRC principles into business strategy requires a cultural shift at all levels, which is often met with resistance. Employees accustomed to operating autonomously may view GRC requirements as burdensome rather than as strategic tools. A report from KPMG indicates that 62% of organizations experience cultural resistance in their GRC transformation efforts, slowing progress and diminishing GRC effectiveness (KPMG, 2022). To address this, organizations must emphasize change management, internal communication, and training to foster a risk-aware culture that recognizes the value of GRC alignment.

Finally, resource constraints and competing priorities present considerable challenges. Aligning GRC with corporate strategy demands a significant commitment of time, finances, and personnel, which can be difficult for organizations with limited

budgets. McKinsey's research shows that 47% of organizations cite budget and personnel constraints as significant barriers to implementing effective GRC practices (McKinsey & Company, 2020). Strategic GRC alignment thus requires prioritizing GRC investments to ensure sustainable alignment with business objectives.

In summary, while aligning GRC strategically with organizational goals can enhance resilience, compliance, and decision-making, it is a complex undertaking. Overcoming challenges related to silos, outdated technology, regulatory changes, cultural resistance, and resource limitations is critical for organizations to realize the full potential of integrated GRC frameworks. With strategic investment, cross-functional collaboration, and a focus on fostering a risk-aware culture, organizations can create a GRC framework that supports both compliance and strategic growth

#### **1.4 Overview of Enterprise Risk Management (ERM)**

Enterprise Risk Management (ERM) is a structured, organization-wide approach to identifying, assessing, managing, and monitoring risks that can impact an organization's strategic objectives, operations, and overall resilience. ERM provides a comprehensive framework for understanding risks across all levels of an organization, from financial and operational risks to strategic and reputational risks. A key distinction of ERM from traditional risk management is its integration of risk assessment and mitigation into the organization's strategy. This alignment ensures a cohesive approach that directly supports and enhances the achievement of business objectives.

At its core, ERM involves systematically identifying and analyzing potential risks that could impact an organization's mission or goals. This process begins with a thorough risk assessment, where organizations examine internal and external risks, including cybersecurity threats, regulatory compliance, operational disruptions, and market volatility. Once identified, each risk is evaluated based on its likelihood and potential

impact. According to a PwC survey, 79% of organizations that adopted ERM practices noted improved risk visibility, highlighting the role of ERM in providing a holistic view of risks across all business areas (PwC, 2021). This visibility enables leaders to make informed decisions and allocate resources to address critical risks.

ERM frameworks often follow standardized methodologies, such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) or ISO 31000, which provide structured risk assessment and management approaches. These frameworks outline essential components of ERM, including governance and culture, strategy and objective-setting, performance monitoring, and risk review. Governance, for instance, ensures that ERM practices are embedded into the organizational culture, with senior management and board oversight to monitor risk initiatives. Organizations can prioritize risk management strategies to support their objectives and long-term success by aligning ERM with strategic goals (COSO, 2017).

The benefits of ERM extend beyond risk mitigation. ERM also supports compliance, operational efficiency, and strategic decision-making. For example, ERM frameworks ensure that organizations remain compliant with evolving laws and standards in industries where regulatory compliance is critical, such as finance or healthcare. In a recent Deloitte study, 72% of organizations reported that ERM helped them reduce regulatory risk, demonstrating the framework's value in managing compliance (Deloitte, 2020). ERM's emphasis on risk oversight and reporting also enables organizations to respond more effectively to unforeseen challenges, fostering resilience in crises and market shifts.

Technology plays an increasingly important role in ERM, with modern tools such as predictive analytics, artificial intelligence, and data integration allowing for real-time

risk monitoring and more accurate risk assessments. For instance, predictive analytics can help organizations anticipate and manage emerging risks. At the same time, data integration solutions enable risk data to be consolidated from various sources, creating a unified view of potential threats. Many organizations are adopting these technologies to enhance their ERM capabilities; according to Gartner, 65% of risk management leaders plan to increase their use of analytics within their ERM frameworks over the next few years (Gartner, 2021).

ERM not only identifies and manages risks but also fosters a risk-aware culture throughout the organization. This culture encourages employees at all levels to actively engage in risk identification and reporting. By empowering teams to make informed decisions and understand the potential impact of their actions on the organization's objectives, ERM significantly contributes to the organization's resilience. Companies with a strong risk-aware culture, often established through ERM practices, are 45% more likely to recover quickly from disruptions, according to McKinsey (McKinsey & Company, 2020).

In conclusion, ERM is a vital component of modern organizational strategy, offering a structured approach to risk management that enhances resilience, promotes compliance, and supports strategic alignment. By providing a holistic view of risks and embedding risk management into the decision-making process, ERM enables organizations to navigate uncertainty, leverage opportunities, and pursue growth while effectively managing potential threats. As businesses face an increasingly complex risk landscape, ERM's role in ensuring stability, agility, and long-term success continues to grow in importance.

## **1.5 GRC: Governance, Risk, and Compliance in IT Companies**



In the rapidly evolving information technology landscape, Governance, Risk, and Compliance (GRC) frameworks are essential for helping IT companies achieve regulatory compliance, safeguard critical assets, and align risk management with organizational objectives. GRC in IT is the integrated strategy combining governance, risk management, and compliance processes to create a structured approach to managing regulatory requirements, cyber risks, and operational controls. As IT companies increasingly rely on digital platforms and data-driven services, implementing effective GRC frameworks has become critical for protecting assets, maintaining trust, and ensuring sustainable growth.

Governance in GRC involves setting clear policies, standards, and structures that guide decision-making and define accountability within an organization. Effective governance is crucial for IT companies, where regulatory requirements and security standards are often stringent. Governance structures ensure that senior leadership can monitor policy adherence, effectively direct IT projects, and foster a risk-aware culture. By implementing strong governance, IT companies can align their technological operations with business goals, ensuring technology investments support broader strategic objectives. According to a KPMG survey, 78% of IT leaders cite governance as essential for aligning technology investments with company strategy, underscoring its importance in driving long-term growth (KPMG, 2022).

Risk management is the second component of GRC, focused on identifying, assessing, and mitigating risks that could impact an IT company's operations or objectives. In the IT industry, where cybersecurity threats, data breaches, and system failures are prevalent, effective risk management is essential to protect information assets and ensure business continuity. GRC frameworks in IT enable organizations to identify potential threats, assess their impact, and develop mitigation strategies that reduce the

likelihood of adverse outcomes. With the growing sophistication of cyber threats, IT companies increasingly utilize advanced risk management tools such as predictive analytics and AI-driven risk assessment models. According to Gartner, 70% of IT companies invest in risk management technologies to enhance their ability to detect and respond to emerging cyber risks in real time (Gartner, 2021).

Compliance, the third pillar of GRC, is a critical focus area for IT companies. It centers on adherence to external regulations, industry standards, and internal policies. For IT companies, compliance is often complex due to diverse and frequently changing regulations, such as data protection laws (e.g., GDPR, CCPA) and industry-specific standards like ISO/IEC 27001 for information security. Non-compliance can lead to severe financial and reputational consequences; for example, GDPR fines have reached over \$1 billion annually globally (PwC, 2022). GRC frameworks play a key role in helping IT companies establish and maintain compliance by embedding regulatory standards into operational processes, conducting regular audits, and ensuring continuous monitoring of compliance metrics. By managing compliance effectively, IT companies can minimize the risk of penalties and foster trust among clients and stakeholders.

Integrating governance, risk, and compliance under a GRC framework offers IT companies a comprehensive approach to managing the challenges of regulatory adherence and risk mitigation in a highly digitalized environment. A well-implemented GRC framework gives IT companies a unified view of risks, ensuring that risk management efforts align with governance policies and compliance requirements. This alignment is essential for preventing siloed risk management practices, which can lead to inefficiencies and overlooked risks. Research by PwC indicates that 62% of organizations with integrated GRC frameworks report enhanced risk visibility and faster response times

to incidents, highlighting the value of GRC for IT companies in achieving a resilient and proactive risk posture (PwC, 2022).

Furthermore, GRC frameworks are instrumental in cultivating a risk-aware culture within IT companies. By integrating GRC practices into daily operations and promoting awareness of governance, risk, and compliance across all levels, IT companies empower employees to actively identify and address risks in their roles. This cultural shift ensures that all employees contribute to maintaining security and compliance, thereby reducing the likelihood of human error and insider threats. A study by Deloitte underscores this, showing that companies with a strong GRC culture are 50% more effective in preventing insider-related security incidents, highlighting the significant role of GRC in enhancing organizational security (Deloitte, 2020).

In the era of digital transformation, GRC frameworks have evolved to incorporate advanced technologies such as automation, artificial intelligence, and data analytics. These technologies enable IT companies to monitor compliance and risk in real time, enhancing their ability to respond to emerging threats. Automated GRC solutions streamline compliance processes, reducing the time and resources needed for audits and regulatory reporting. This evolution of GRC frameworks underscores their adaptability and their role in enabling IT companies to stay ahead in a rapidly changing digital landscape (McKinsey & Company, 2021).

## **1.6 Problem Statement**

The convergence of Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) frameworks presents substantial challenges for Information Technology (IT) enterprises. These challenges are compounded by the intricate nature of the IT landscape, evolving regulatory demands, and diverse stakeholder interests. While effective management of risks and compliance is pivotal for ensuring organizational

resilience and adherence to regulations, many IT companies require assistance in aligning ERM and GRC. Fragmented approaches to risk management and compliance, coupled with rapid technological advancements, make it arduous to sustain alignment between ERM and GRC practices, leaving companies vulnerable to increased risks and compliance violations (Deloitte, 2020).

To surmount these challenges, a comprehensive understanding of the intricacies of the IT domain and the impediments to ERM-GRC alignment is essential. It is imperative to formulate strategies to overcome these barriers, strengthen risk management capabilities, fortify compliance posture, and adeptly navigate the dynamic business environment. Therefore, this research seeks to pinpoint and alleviate the obstacles associated with aligning ERM with GRC frameworks in IT enterprises. By doing so, we aim to cultivate effective risk management practices and ensure regulatory compliance in the IT sector, thereby fostering a more resilient and compliant industry (PwC, 2022).

### **1.7 Research Objectives**

The main goal of this research is to assess how Enterprise Risk Management (ERM) acts as a catalyst for Governance, Risk, and Compliance (GRC) alignment in IT companies. The specific objectives are as follows:

1. To Assess Stakeholder Influence on ERM-GRC Processes.
2. To Analyze the Effectiveness of Strategies for ERM-GRC Alignment.
3. To Evaluate Tools and Techniques for ERM-GRC Alignment Assessment.
4. Identify Challenges to ERM-GRC Alignment through Quantitative Analysis.

### **1.8 Research Questions**

Below are the research questions guiding this study:

- To what extent does stakeholder influence affect the effectiveness and alignment of Enterprise Risk Management (ERM) processes with Governance, Risk, and Compliance (GRC) frameworks in Information Technology companies?
- How effective are different strategies in achieving alignment between Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) in Information Technology (IT) companies?
- What are the most effective tools and techniques for assessing the alignment between Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) in Information Technology companies?
- What are the primary challenges in achieving alignment between Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) in Information Technology companies, as identified through quantitative analysis?

### **1.9 Significance of the Study**

The examination of Enterprise Risk Management (ERM) as a catalyst for Strategic Governance, Risk, and Compliance (GRC) Alignment in IT Companies is of significant importance as it delves into the role of ERM in bolstering resilience, streamlining risk management, and fortifying compliance within the IT sector. Given the unique risks faced by IT companies, such as those related to cybersecurity, data privacy, and regulatory demands, understanding how ERM can serve as a unifying force in GRC alignment is imperative for enhancing decision-making, operational efficiency, and strategic positioning (PwC, 2022). This study investigates how ERM can transcend traditional, isolated risk management practices, assisting organizations in developing an

integrated approach to GRC that aligns with their strategic objectives and adapts to the rapidly evolving technology landscape (Deloitte, 2021).

One of the primary contributions of this study is highlighting the potential for ERM frameworks to bridge the gap between governance, risk, and compliance functions. IT companies often operate in complex environments where risks can impact various business areas, from operations to customer trust and regulatory adherence. By exploring ERM as a cohesive tool for GRC alignment, the study provides insights into creating a seamless approach where risk management is not siloed but instead integrated within governance and compliance activities. For IT companies, where changes in technology and regulations are frequent, a well-integrated ERM strategy could enable quicker, more effective responses to risks and compliance requirements, ensuring smoother operations and consistent regulatory adherence (KPMG, 2021).

The relevance of the study extends to examining how ERM fosters a risk-aware culture within IT companies. This cultural shift is crucial as it encourages employees across all levels to proactively engage in risk management, supporting the organization in identifying and mitigating potential issues before they escalate (McKinsey & Company, 2020). The study underscores how an effective ERM framework can lay the groundwork for risk awareness, promoting accountability and engagement in GRC processes. Emphasizing ERM's role in fostering a risk-aware culture empowers the audience about its potential to engage employees at all levels, ultimately strengthening the entire risk management ecosystem of IT organizations (PwC, 2022).

Furthermore, this study is significant as it explores the technological and organizational challenges IT companies face when attempting to align GRC with strategic objectives. In doing so, it provides a roadmap for how ERM can help overcome these challenges, offering solutions that integrate modern technology and data analytics

for real-time risk insights (Gartner, 2021). This emphasis on the importance of ERM in overcoming challenges reassures the audience about its ability to provide solutions that support proactive and data-driven GRC processes, particularly in the IT sector where outdated or fragmented systems often hinder GRC alignment (Deloitte, 2021).

Lastly, this study has broader implications for stakeholders, including IT leaders, regulatory bodies, and policymakers. Demonstrating ERM's role in driving GRC alignment encourages IT organizations to adopt a more strategic approach to risk management. This alignment supports regulatory compliance and security and positions IT companies to be more competitive, resilient, and adaptive in the face of rapid technological changes. For policymakers, the study offers evidence of the importance of ERM in safeguarding against sector-specific risks, encouraging the development of policies that support robust ERM practices (KPMG, 2021).

In conclusion, this study emphasizes the transformative role of ERM in achieving strategic GRC alignment within IT companies, making it a crucial resource for advancing both academic and practical understanding of integrated risk management in the technology sector. Addressing ERM's potential to catalyze GRC alignment provides IT companies with a framework for fostering resilience, promoting a risk-aware culture, and leveraging technology to support strategic growth and regulatory compliance (Gartner, 2021).

## **1.10 Structure of the Thesis**

The thesis is structured as follows:

Chapter 2: Literature Review – This chapter provides an overview of existing research on ERM and GRC, including theoretical frameworks, stakeholder influence, alignment strategies, assessment tools, and challenges specific to IT companies.

Chapter 3: Research Methodology – This chapter outlines the research design, data collection methods, and analytical approaches used to address the research objectives and answer the research questions.

Chapter 4: Data Analysis and Results – This chapter presents the findings from quantitative and qualitative data analyses, exploring how stakeholder roles, strategies, tools, and challenges affect ERM-GRC alignment in IT companies.

Chapter 5: Discussion – This chapter interprets the results in light of existing literature and theoretical frameworks, highlighting implications for practice and theory.

Chapter 6: Conclusion and Recommendations – This chapter summarizes the research findings, outlines recommendations for IT companies, and suggests areas for future research



## CHAPTER II: REVIEW OF LITERATURE

### **2.1 Theoretical Foundations for ERM-GRC Alignment**

A range of theoretical perspectives can help better understand the alignment of Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) in IT companies. These theories provide insights into the drivers, benefits, and challenges of ERM-GRC integration, particularly within organisations facing complex regulatory and operational risk landscapes, as is common in the IT sector. The primary theories relevant to this study include Agency Theory, Contingency Theory, Stakeholder Theory, and Resource-Based View (RBV).

#### **2.1.1 Agency Theory**

Agency Theory examines the relationship between principals (shareholders) and agents (managers) within an organisation, highlighting the potential for conflicts of interest and misaligned objectives (Jensen & Meckling, 1976). This theory is particularly relevant in the context of ERM-GRC alignment, as it underscores the need for transparency, accountability, and governance structures that ensure managers act in the best interest of shareholders.

**ERM as a Tool for Mitigating Agency Problems:** ERM can help reduce agency problems by establishing clear accountability and oversight mechanisms. Integrating ERM with GRC frameworks creates a unified approach that provides transparency across governance, risk, and compliance functions. By aligning these functions, IT companies can improve risk oversight and accountability, reducing the likelihood of opportunistic behaviour by management (Lam, 2014).

**Improving Decision-Making and Strategic Alignment:** Agency Theory suggests that aligning ERM with GRC frameworks can lead to better decision-making, as

managers have a clearer understanding of risks and compliance obligations. This alignment reduces information asymmetry, facilitating informed and balanced decisions that align with shareholder interests (Power, 2009).

### **2.1.2 Contingency Theory**

Contingency Theory posits that organisational effectiveness depends on the fit between an organisation's internal processes and its external environment (Donaldson, 2001). In the context of ERM-GRC alignment, Contingency Theory emphasises that risk management practices must be tailored to the organisation's specific context, considering factors such as industry, regulatory landscape, and organisational structure.

Adapting ERM-GRC Practices to IT-Specific Risks: IT companies face unique risks, such as cybersecurity threats, data privacy issues, and rapid technological change. Contingency Theory supports the notion that ERM-GRC frameworks in IT companies should be customised to address these specific risks rather than adopting a one-size-fits-all approach. This tailored alignment enables IT firms to manage risks that align with their strategic objectives and regulatory obligations better (Mikes & Kaplan, 2015).

Flexible and Adaptive Frameworks: ERM-GRC alignment should not be static but evolve as the organisation and its environment change. Contingency Theory advocates for adaptable frameworks that allow IT companies to respond to emerging risks and regulatory changes effectively, thereby maintaining alignment with external requirements and internal objectives (Woods, 2009).

### **2.1.3 Stakeholder Theory**

Stakeholder Theory broadens the focus of organisational governance from shareholders to include all stakeholders affected by the organisation's operations, including customers, employees, regulators, and the community (Freeman, 1984). In the

IT sector, where data privacy and cybersecurity are paramount, Stakeholder Theory underscores the importance of transparency and accountability to various stakeholders.

**Building Stakeholder Trust Through ERM-GRC Alignment:** By aligning ERM with GRC practices, IT companies can demonstrate a commitment to proactive risk management and regulatory compliance, addressing stakeholder concerns and building trust. This is especially important for external stakeholders who demand robust cybersecurity practices and data protection measures. ERM-GRC alignment provides a structured approach to meeting these expectations, helping IT companies maintain a positive reputation and secure stakeholder confidence (Racz, Weippl, & Seufert, 2010).

**Ensuring Compliance with Regulatory Standards:** Compliance is a critical aspect of stakeholder relations in IT, particularly with data protection laws like GDPR. Stakeholder Theory supports ERM-GRC alignment as a means to meet regulatory requirements and enhance transparency in compliance efforts, ultimately reducing reputational and legal risks associated with non-compliance (Bhimani, 2009).

#### **2.1.4 Synthesis of Theoretical Perspectives**

These theoretical foundations collectively suggest that ERM-GRC alignment in IT companies is not merely a compliance or risk management exercise but a strategic approach that can drive value and build resilience. Agency Theory highlights the importance of transparency and accountability in risk oversight. At the same time, Contingency Theory supports the need for a customised approach to ERM-GRC practices in the unique context of IT. Stakeholder Theory reinforces the role of ERM-GRC alignment in building trust with various stakeholders, and the Resource-Based View positions ERM-GRC alignment as a valuable resource that contributes to competitive advantage and organisational resilience.

Through this multi-theoretical lens, it becomes clear that aligning ERM with GRC frameworks enables IT companies to address regulatory, operational, and reputational risks more effectively. By creating a cohesive framework, IT firms can achieve not only compliance and governance objectives but also strategic alignment that supports long-term growth and competitive positioning in a high-risk environment.

## **2.2 Governance, Risk, and Compliance (GRC) Frameworks in IT Companies**

Governance, Risk, and Compliance (GRC) frameworks have become essential in the IT industry, serving as a strategic approach to managing organizational objectives, risk exposure, and regulatory obligations. The concept of GRC emerged in the early 2000s, mainly in response to increasing regulatory demands and the need for enhanced corporate governance standards. IT companies face challenges due to rapid technological changes, cybersecurity threats, and complex regulatory requirements. GRC frameworks support a structured, organization-wide approach to risk and compliance management (Racz et al., 2010).

### **2.2.1 Components of GRC in IT Companies**

GRC frameworks consist of three interconnected components—governance, Risk Management, and Compliance—each of which plays a critical role in ensuring that IT companies operate in a controlled, risk-aware, and compliant manner. These components combine to create a cohesive structure that aligns IT operations with organizational strategy and regulatory requirements.

**Governance:** Governance establishes the policies, procedures, and controls that define the organization’s oversight structure. It ensures that IT initiatives are aligned with the company’s strategic goals, promoting accountability and decision-making that adheres to ethical and regulatory standards. Governance in IT companies includes

defining roles and responsibilities, implementing control mechanisms, and setting objectives that align with the organization's broader strategy (Bhimani, 2009).

**Risk Management:** Risk management within GRC frameworks involves identifying, assessing, and mitigating risks that could hinder an organization's ability to achieve its goals. For IT companies, this includes managing risks associated with cybersecurity, data privacy, technological disruptions, and regulatory compliance. Effective risk management enables IT firms to proactively address potential threats, thereby reducing the likelihood of operational disruptions or regulatory penalties (Frigo & Anderson, 2011).

**Compliance** focuses on adhering to internal policies, external regulations, and industry standards. Compliance is particularly challenging for IT companies due to the dynamic nature of regulatory requirements, such as GDPR for data protection and various cybersecurity regulations. Compliance in GRC ensures that IT companies meet these obligations, minimizing legal risks and protecting organizational reputation (Morrow, 2011).

Each of these components reinforces the others within a GRC framework, creating a systematic approach to aligning IT operations with organizational goals, regulatory standards, and risk management practices.

### **2.2.2 Importance of GRC Frameworks in IT Companies**

The importance of GRC frameworks in IT companies cannot be overstated. In an industry marked by rapid innovation and regulatory oversight, GRC frameworks provide IT firms with the tools to manage complex risk landscapes and comply with a broad range of standards and regulations.

**Enhanced Risk Awareness and Proactive Management:** GRC frameworks enhance risk awareness within IT organizations by providing a structured approach to identifying

and mitigating risks across all functions. This proactive risk management is especially critical in IT, where cybersecurity and data protection concerns are paramount (Kaplan & Mikes, 2012).

**Streamlined Compliance and Regulatory Adherence:** Compliance is an ongoing concern in IT, with regulations like GDPR, HIPAA, and SOX requiring strict adherence to data privacy and reporting standards. GRC frameworks streamline compliance efforts by embedding regulatory requirements into organizational processes, ensuring that IT companies consistently meet obligations and reducing the risk of regulatory fines (Bhimani, 2009).

**Alignment of IT Operations with Corporate Governance:** Governance within GRC frameworks provides a top-down approach to ensuring that IT strategies are aligned with corporate objectives and ethical standards. This alignment improves accountability, supports strategic decision-making, and helps build a culture of risk awareness and compliance (Racz et al., 2010).

### **2.2.3 Evolution of GRC in IT: From Compliance to Integrated Risk Management**

GRC frameworks in IT companies have evolved significantly over the past two decades. Initially, GRC efforts were driven by regulatory compliance, primarily focusing on meeting standards such as SOX and PCI-DSS. However, as the risk landscape became more complex and interconnected, GRC frameworks began to incorporate broader risk management elements, emphasizing the integration of governance, risk, and compliance into a cohesive system.

**Shift Toward Integrated Risk Management (IRM):** With increasing digitalization and the rising frequency of cyber threats, IT companies have adopted Integrated Risk Management (IRM) as an extension of traditional GRC. IRM emphasizes a holistic view of risks, enabling companies to monitor, evaluate, and respond to risks in real time. IRM

tools, such as GRC software platforms, help IT companies centralize governance, risk, and compliance data, offering a unified approach to risk oversight (Power, 2009).

**Increasing Focus on Strategic GRC:** Modern GRC frameworks in IT companies extend beyond regulatory compliance to address strategic objectives. By integrating GRC with enterprise risk management (ERM) frameworks, IT firms can enhance their agility and resilience, enabling them to adapt more effectively to regulatory changes and emerging risks (Frigo & Anderson, 2011).

#### **2.2.4 Challenges of Implementing GRC in IT Companies**

Despite the benefits of GRC frameworks, IT companies face several challenges in implementing these frameworks effectively:

**Organizational Silos:** One of the biggest challenges in GRC implementation is the existence of organizational silos, where governance, risk management, and compliance functions operate independently. This lack of integration can lead to redundant processes, gaps in risk oversight, and inefficient resource allocation (Ashby et al., 2012).

**Dynamic Regulatory Landscape:** The constantly evolving regulatory landscape, especially data privacy and cybersecurity, poses a significant challenge. IT companies must continually adapt their GRC frameworks to address new regulations, which can be resource-intensive and require continuous updates to policies and controls (Woods, 2009).

**Resource Constraints:** Implementing a comprehensive GRC framework requires significant resources, including skilled personnel, technology investments, and time. Smaller IT companies may need help allocating the necessary resources for effective GRC, potentially impacting their ability to achieve compliance and manage risks (Sax & Andersen, 2019).

Cultural Resistance: Resistance to change is another common challenge, particularly in organizations with established risk management practices. Shifting to an integrated GRC approach often requires a cultural transformation that promotes cross-functional collaboration and risk awareness, which can only be challenging achieved with strong leadership support (Simons, 1999).

### **2.2.5 GRC as a Foundation for ERM in IT Companies**

The integration of GRC with Enterprise Risk Management (ERM) has gained traction as IT companies recognize the strategic value of aligning governance, risk, and compliance with enterprise-wide risk management efforts. ERM provides a structured framework for addressing risks from an organizational perspective, allowing IT companies to manage risk more comprehensively and strategically.

Supporting Proactive and Strategic Decision-Making: By aligning GRC with ERM, IT companies can improve their ability to anticipate and respond to risks, supporting proactive decision-making that aligns with strategic goals (Gates et al., 2012).

Enhancing Organizational Resilience: GRC, when integrated with ERM, enhances resilience by ensuring IT companies have robust processes to handle regulatory requirements, mitigate risks, and adapt to change. This integration is particularly valuable in the IT sector, where risks are highly dynamic and impactful, and business continuity depends on a solid foundation of compliance and risk management (Beasley et al., 2005).

### **2.2.6 Future Directions for GRC Frameworks in IT**

The future of GRC frameworks in IT is marked by increased digital transformation, automation, and a greater emphasis on resilience. Emerging technologies like artificial intelligence (AI) and machine learning are also expected to significantly enhance GRC processes by enabling real-time monitoring, predictive risk assessment, and automated compliance checks (Oetzel & Getz, 2012).



Adoption of Integrated GRC Platforms: Integrated GRC platforms are expected to become more common in IT companies. These platforms provide centralized tools for tracking risks, compliance activities, and governance processes. These platforms facilitate real-time visibility into risk and compliance data, making it easier for IT firms to maintain continuous compliance and respond to regulatory changes (Morrow, 2011).

Focus on Cybersecurity and Data Privacy: Given the high stakes of data privacy and cybersecurity, future GRC frameworks in IT will likely emphasize advanced security controls and privacy management. This focus will help IT companies address the growing complexity of regulatory requirements and enhance their ability to protect sensitive data (Hoyt & Liebenberg, 2011).

### **2.3 Evolution of ERM and GRC Frameworks in IT**

The evolution of Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) frameworks in the IT sector reflects the industry's response to a rapidly changing risk landscape. IT companies face unique challenges, including cybersecurity threats, data privacy issues, and compliance with complex and evolving regulations. Initially, GRC efforts were primarily compliance-driven and focused on meeting regulatory standards. However, as risk environments became more complex and interconnected, IT companies began adopting ERM frameworks, such as COSO ERM and ISO 31000, emphasizing an integrated approach to managing risks, governance, and compliance.

#### **2.3.1 Early Compliance-Driven Approaches in GRC**

In the early 2000s, IT companies started formalizing risk management practices in response to increasing regulatory requirements, such as the Sarbanes-Oxley Act (SOX) of 2002, which aimed to enhance corporate accountability and financial transparency. This era marked the beginning of structured GRC frameworks in IT companies, which heavily

emphasized compliance as a response to external regulations. Compliance activities were typically soiled, with distinct teams handling governance, risk, and compliance functions separately.

**Compliance as a Reactive Approach:** Initially, GRC practices focused on ensuring adherence to regulatory requirements, primarily to avoid penalties and reputational damage. However, this reactive approach limited the strategic value of GRC, as compliance was often seen as a cost rather than a value-adding function (Bhimani, 2009). Risk management efforts often frag could have been more cohesive departments, resulting in redundant processes and inefficiencies that limited visibility into enterprise-wide risks.

### **2.3.2 Emergence of Integrated Risk Management in IT**

As IT companies continued to face increasingly complex risk landscapes, the limitations of a compliance-driven approach became apparent. The need for a more cohesive risk management strategy led to the adoption of Enterprise Risk Management (ERM) frameworks. ERM frameworks, such as COSO ERM and ISO 31000, offered an integrated approach that allowed companies to manage risk holistically, proactively, and strategically.

**Transition to ERM Frameworks:** ERM frameworks gained traction in the mid-2000s as IT companies recognized the value of a structured, enterprise-wide approach to managing risks. ERM provided the tools to assess risks across all business functions, promoting a unified understanding of risk aligned with the company's strategic goals (Frigo & Anderson, 2011). The adoption of ERM marked a shift from isolated risk management activities to an organization-wide framework that connected risk management with governance and compliance functions.

Introduction of GRC as a Strategic Framework: The concept of GRC evolved alongside ERM, advocating for the integration of governance, risk, and compliance into a single, cohesive strategy. GRC frameworks, like those supported by the Open Compliance & Ethics Group (OCEG), were introduced to streamline governance and compliance activities, ensuring that risk management efforts aligned with the organization's strategic objectives. This shift toward an integrated GRC framework helped IT companies manage risks more effectively while meeting regulatory requirements (Morrow, 2011).

### **2.3.3 Digital Transformation and the Expanding Scope of GRC**

The digital transformation of the IT industry in the 2010s further shaped the evolution of ERM and GRC frameworks. Cloud computing, big data, artificial intelligence, and the Internet of Things (IoT) introduced new risks and regulatory challenges, underscoring the need for agile and responsive risk management frameworks. As IT companies adopted these technologies, they faced complex cybersecurity, data privacy, and operational risks, requiring a more comprehensive approach to GRC and ERM integration.

Growth of Cybersecurity and Data Privacy Concerns: The rise of cyber threats and the implementation of data privacy regulations, such as the EU's General Data Protection Regulation (GDPR), increased the demand for robust GRC frameworks in IT companies. These frameworks were essential in helping IT firms manage and monitor compliance with data protection laws while addressing the operational risks associated with cybersecurity threats (Power, 2009). ERM's holistic approach enabled companies to identify and manage these risks across the entire organization, moving beyond compliance to enhance security and resilience.

Adoption of Integrated Risk Management (IRM) Platforms: Digital transformation also led to the development of Integrated Risk Management (IRM) platforms, which offer centralized tools for tracking and managing risks, compliance activities, and governance processes. IRM platforms provide real-time data and analytics, enabling IT companies to continuously monitor their risk exposure and compliance status. This technology-driven approach allows for more efficient risk assessment, reporting, and decision-making, enhancing the strategic value of ERM and GRC alignment (Oetzel & Getz, 2012).

#### **2.3.4 Modern ERM-GRC Frameworks: Emphasis on Strategic Alignment and Resilience**

In recent years, the evolution of ERM and GRC frameworks in IT has been marked by an increased emphasis on resilience, agility, and strategic alignment. Modern ERM frameworks, such as COSO's updated ERM framework, highlight the need to integrate risk management into strategic decision-making, making risk a core component of business planning. Similarly, GRC frameworks have evolved to focus on compliance and fostering a culture of risk awareness and adaptability within organizations.

ERM as a Strategic Tool for Governance and Compliance: Today's ERM frameworks provide IT companies with a structure to proactively address governance and compliance concerns, linking risk management directly with organizational strategy. By aligning ERM with GRC, IT companies can create a unified risk management framework that improves accountability, enhances operational efficiency, and supports strategic decision-making (Kaplan & Mikes, 2012). This integration allows IT firms to leverage risk management as a competitive advantage, positioning them to respond quickly to new regulatory requirements and emerging risks.

Focus on Organizational Resilience and Agility: As IT companies navigate increasingly volatile environments, modern ERM-GRC frameworks enhance resilience by ensuring that risk management processes are adaptive and responsive. By aligning GRC and ERM, organizations can improve their ability to manage disruptions, mitigate impacts, and recover quickly from unforeseen events. This focus on resilience aligns with broader industry trends prioritizing business continuity and adaptability, especially in high-risk industries like IT (Beasley et al., 2005).

### **2.3.5 Challenges and Future Directions for ERM and GRC in IT**

Despite the benefits of integrated ERM-GRC frameworks, IT companies face several challenges in implementation, including resource constraints, organizational silos, and the complexity of regulatory requirements. The future of ERM and GRC in the IT sector will likely involve addressing these challenges by adopting advanced technologies, such as AI and machine learning, which can enhance risk assessment and compliance monitoring capabilities.

Addressing Organizational Silos and Cultural Resistance: Integrating ERM with GRC requires a shift in organizational culture that promotes cross-functional collaboration and a unified approach to risk management. Many IT companies struggle with entrenched silos that limit visibility into enterprise-wide risks, creating challenges for ERM-GRC alignment (Ashby et al., 2012). To overcome these challenges, organizations may need to invest in training and change management initiatives that foster a culture of risk awareness and collaboration.

Leveraging AI and Predictive Analytics for GRC: Emerging technologies, such as AI and predictive analytics, hold significant potential for the future of ERM and GRC. These technologies can enhance risk forecasting, automate compliance checks, and provide real-time insights into risk exposure. By adopting these technologies, IT

companies can improve the efficiency and effectiveness of their ERM-GRC frameworks, allowing for continuous monitoring and proactive risk management (Morrow, 2011).

## **2.4 Theoretical Foundations for ERM-GRC Alignment**

The alignment of Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) in IT companies is grounded in several theoretical perspectives explaining the drivers, benefits, and challenges of this integration. Each theory provides a unique viewpoint on how ERM and GRC alignment can support organizational objectives, address regulatory demands, and enhance risk management. The primary theories relevant to this study include Agency Theory, Contingency Theory, Stakeholder Theory, and the Resource-Based View (RBV).

### **2.4.1 Agency Theory**

Agency Theory, introduced by Jensen and Meckling (1976), examines the relationship between principals (e.g., shareholders) and agents (e.g., managers), highlighting the potential for conflicts of interest and misaligned objectives. This theory is relevant to ERM-GRC alignment as it underscores the importance of transparency, accountability, and oversight in reducing agency problems, particularly in risk-sensitive industries like IT.

Mitigating Agency Problems through ERM-GRC Alignment: ERM helps IT companies establish a structured approach to risk management that clarifies roles and responsibilities, making it easier to hold managers accountable for compliance and risk mitigation efforts. By integrating ERM with GRC frameworks, IT companies can improve transparency and ensure that managers act in the best interest of shareholders, thus reducing agency costs and conflicts (Lam, 2014).

Improving Decision-Making and Strategic Alignment: Agency Theory suggests that ERM-GRC alignment reduces information asymmetry as managers gain a clearer

view of risks and compliance obligations across the organization. This transparency supports better decision-making, aligning managerial actions with shareholder interests and organizational goals (Power, 2009).

### **2.4.2 Contingency Theory**

Donaldson's Contingency Theory (2001) posits many of the best ways to manage an organization. Instead, organizational effectiveness depends on the alignment or "fit" between an organization's processes and its external environment. In the context of ERM-GRC alignment, Contingency Theory highlights the importance of tailoring risk management and compliance practices to each IT company's unique context and environment.

**Adapting ERM-GRC Practices to IT-Specific Risks:** IT companies face specific risks such as cybersecurity threats, data privacy issues, and rapid technological evolution. Contingency Theory suggests that IT firms must adapt their ERM-GRC frameworks to address these risks effectively rather than relying on a generic approach. This customization allows IT companies to align their risk management practices with both industry-specific challenges and strategic objectives (Mikes & Kaplan, 2015).

**Flexible and Adaptive Frameworks:** ERM-GRC alignment requires flexible frameworks that can evolve with the organization and its environment. Contingency Theory supports this adaptability, advocating for frameworks that enable IT companies to respond quickly to emerging risks and regulatory changes, thereby maintaining alignment with external demands and internal goals (Woods, 2009).

### **2.4.3 Stakeholder Theory**

Stakeholder Theory, introduced by Freeman (1984), broadens the focus of governance from a shareholder-centric view to one that considers the interests of various stakeholders, including customers, employees, regulators, and the community. In the IT

sector, where issues like data privacy, cybersecurity, and compliance are obvious to stakeholders, Stakeholder Theory supports ERM-GRC alignment to address the needs and expectations of a diverse range of stakeholders.

**Building Stakeholder Trust through ERM-GRC Alignment:** By aligning ERM with GRC, IT companies are committed to proactive risk management and regulatory compliance, addressing stakeholder concerns and building trust. This is particularly important for external stakeholders, such as customers and regulators, who demand robust data protection and cybersecurity practices. ERM-GRC alignment provides IT companies a structured approach to meeting these expectations, enhancing stakeholder confidence and organizational reputation (Racz et al., 2010).

**Ensuring Compliance with Regulatory Standards:** Compliance with regulatory standards is a central concern for stakeholders, particularly in data-driven industries like IT. Stakeholder Theory supports the idea that ERM-GRC alignment helps IT companies meet compliance requirements and enhance transparency, which can reduce legal and reputational risks associated with non-compliance (Bhimani, 2009).

#### **2.4.4 Resource-Based View (RBV)**

The firm's Resource-Based View (RBV), developed by Barney (1991), suggests that an organization's resources and capabilities are critical sources of competitive advantage. ERM-GRC alignment is a valuable organizational resource that enhances resilience, operational efficiency, and strategic adaptability, particularly in the high-risk IT sector.

**ERM-GRC Alignment as a Strategic Resource:** Aligning ERM with GRC creates a unique organizational resource by providing a unified framework that integrates governance, risk management, and compliance. According to RBV, this integration enhances an organization's ability to manage risk and compliance effectively, thus



improving its competitive position in the industry (Gates et al., 2012). IT companies that align ERM and GRC can better navigate complex regulatory environments and respond to risks proactively, positioning them for sustained success.

**Supporting Organizational Resilience:** ERM-GRC alignment is a source of efficiency and contributes to organizational resilience. Risk management, compliance, and governance integration enable IT companies to withstand and adapt to disruptions, such as cyber threats and regulatory changes, ensuring continuity and long-term stability (Beasley et al., 2005). In this way, ERM-GRC alignment functions as a resource that supports business continuity and strategic adaptability, critical capabilities in the IT sector.

#### **2.4.5 Synthesis of Theoretical Perspectives**

These theoretical foundations collectively suggest that ERM-GRC alignment in IT companies is a strategic endeavor, not a compliance activity. Each theory provides valuable insights into the ways ERM and GRC alignment can enhance organizational efficiency, transparency, and resilience:

Agency Theory underscores the need for transparency and accountability in risk management, highlighting how ERM-GRC alignment can reduce agency conflicts and align managerial actions with shareholder interests.

Contingency Theory supports the view that ERM-GRC frameworks should be adapted to the specific risk profiles and external challenges faced by IT companies, ensuring alignment with industry needs and strategic goals.

Stakeholder Theory expands the focus of GRC to include a broader range of stakeholders, emphasizing how ERM-GRC alignment can enhance trust and address stakeholder expectations, particularly in areas like cybersecurity and regulatory compliance.

Resource-Based View positions ERM-GRC alignment as a strategic resource, highlighting its role in supporting organizational resilience, adaptability, and competitive advantage.

Through this multi-theoretical lens, it becomes evident that ERM-GRC alignment is essential for IT companies aiming to navigate regulatory complexities, enhance risk awareness, and achieve strategic alignment. By providing a cohesive framework that unifies governance, risk, and compliance, ERM-GRC alignment enables IT firms to manage their risk landscape more effectively, ultimately supporting their long-term resilience and growth in a highly dynamic and competitive industry (Victor et al., 2024).

## **2.5 Benefits of ERM-Driven GRC Alignment in IT Companies**

Aligning Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) frameworks offers IT companies a range of strategic benefits. By integrating these frameworks, organizations can develop a cohesive approach to managing risks, ensuring compliance, and supporting governance structures, enhancing resilience and strategic agility. IT companies operate in a dynamic risk environment of cybersecurity threats, data privacy concerns, and regulatory pressures. In this context, ERM-driven GRC alignment contributes to operational efficiency, regulatory compliance, and sustained competitive advantage.

### **2.5.1 Enhanced Risk Visibility and Proactive Risk Management**

One of the primary benefits of ERM-driven GRC alignment is improved visibility into risk exposure across the organization. By centralizing risk, compliance, and governance functions, IT companies can more effectively identify and address potential threats.

**Comprehensive Risk Oversight:** ERM provides a holistic view of risks by integrating risk data across various business units, enabling IT companies to track and assess risks in a unified manner. This comprehensive oversight improves risk awareness among managers and enables the organization to respond proactively to emerging threats, such as cybersecurity vulnerabilities and regulatory changes (Gates et al., 2012).

**Proactive Risk Management:** ERM-driven GRC alignment allows IT companies to shift from reactive to proactive risk management. Rather than addressing risks as they arise, IT firms can use ERM frameworks to forecast potential threats, implement preventive measures, and develop response strategies. This proactive approach enhances organizational resilience and minimizes disruptions that could impact business continuity (Hoyt & Liebenberg, 2011).

### **2.5.2 Improved Compliance and Regulatory Adherence**

Regulatory compliance is a critical concern for IT companies, which must adhere to various data privacy, cybersecurity, and industry-specific standards. Aligning ERM with GRC frameworks streamlines compliance efforts, reducing the burden of regulatory obligations and minimizing the risk of legal or financial penalties (Deloitte, 2021; PwC, 2022).

**Streamlined Compliance Processes:** An integrated ERM-GRC framework embeds compliance requirements into the organization's risk management strategy, making tracking and meeting regulatory obligations easier. This alignment reduces duplication of efforts, ensures compliance activities align with broader risk management goals, and allows for more efficient use of resources (Paape & Speklé, 2012).

**Reduced Regulatory Risks:** Compliance with regulations such as the GDPR and HIPAA is essential for IT companies to avoid costly fines and reputational damage. ERM-driven GRC alignment helps ensure that all aspects of regulatory compliance are

covered, reducing the likelihood of oversights and enhancing the company's legal and ethical standing. This approach also facilitates ongoing regulatory monitoring, making it easier for companies to adapt to new requirements as they emerge (Bhimani, 2009).

### **2.5.3 Increased Operational Efficiency**

Integrating ERM with GRC frameworks enables IT companies to reduce redundancies, streamline processes, and improve operational efficiency. By consolidating risk and compliance functions, organizations can optimize resources and reduce the time and cost of managing separate governance, risk, and compliance activities.

**Resource Optimization:** ERM-GRC alignment eliminates redundant processes by consolidating compliance checks, risk assessments, and governance audits into a single, cohesive system. This approach enables IT companies to use their resources better, allowing staff to focus on high-priority tasks rather than duplicative or fragmented risk management activities (Beasley et al., 2005).

**Enhanced Decision-Making:** IT managers can access real-time data and insights on risk exposure and regulatory status with a unified risk and compliance framework. This comprehensive information supports faster and more informed decision-making, as managers can quickly identify risks and determine the most effective mitigation strategies. Improved decision-making reduces the likelihood of costly mistakes and enhances organizational agility (Kaplan & Mikes, 2012).

### **2.5.4 Support for Strategic Decision-Making and Agility**

Aligning ERM with GRC frameworks enables IT companies to integrate risk management into their strategic planning processes, enhancing agility and positioning them to capitalize on opportunities while managing potential risks.

**Strategic Risk Awareness:** ERM-driven GRC alignment gives IT executives a strategic understanding of risks that could impact organizational goals. This awareness

allows them to incorporate risk considerations into business strategies, supporting growth initiatives while maintaining a solid risk posture (Frigo & Anderson, 2011).

**Enhanced Agility and Responsiveness:** The IT industry is characterized by rapid changes in technology and regulation. By integrating ERM and GRC, companies can monitor real-time changes in the risk landscape, enabling them to adapt quickly to new threats or regulatory requirements. This agility is particularly valuable in high-risk environments where adaptability is essential for maintaining a competitive edge (Mikes & Kaplan, 2015).

### **2.5.5 Strengthened Organizational Resilience and Business Continuity**

ERM-driven GRC alignment is also crucial in supporting business continuity and resilience, particularly in the face of cybersecurity threats, operational disruptions, and regulatory changes.

**Resilience Against Cybersecurity Threats:** IT companies face significant risks from cyber attacks, data breaches, and other digital threats. ERM-GRC alignment provides a structured approach to managing these risks by embedding cybersecurity considerations into risk assessments and compliance checks. This integrated approach strengthens the organization's resilience, ensuring it can withstand cyber incidents and maintain operational stability (Power, 2009).

**Enhanced Business Continuity Planning:** By incorporating GRC into ERM, IT companies can develop comprehensive business continuity plans that address operational and regulatory risks. This alignment ensures the organization is prepared for potential disruptions, allowing for quicker recovery and minimal impact on business operations. Resilience-building through ERM-GRC alignment supports long-term sustainability, even in unforeseen crises (Beasley et al., 2005).

### **2.5.6 Building Stakeholder Confidence and Enhancing Reputation**

ERM-GRC alignment enhances transparency and accountability in IT companies, which can improve relationships with key stakeholders, including customers, regulators, and investors.

**Increased Transparency and Accountability:** By aligning risk and compliance processes, ERM-GRC frameworks create transparency in managing risks and achieving compliance. This openness reassures stakeholders that the organization takes a proactive approach to managing risks and meeting regulatory requirements, increasing stakeholder trust (Freeman, 1984).

**Enhanced Reputation and Competitive Advantage:** IT companies that demonstrate a strong commitment to compliance and risk management can gain a reputation as trustworthy and reliable partners. This reputation builds customer loyalty and provides a competitive advantage, as stakeholders are more likely to support organizations that prioritize risk management and compliance (Morrow, 2011).

## **2.6 Challenges of Implementing ERM-GRC Alignment in IT Companies**

Aligning Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) frameworks presents several challenges for IT companies. While ERM-driven GRC alignment offers significant strategic and operational benefits, the integration process can be complex, time-intensive, and resource-demanding. IT companies, which often operate in fast-paced, high-risk environments, encounter unique challenges due to factors such as organizational silos, rapid regulatory changes, technological complexity, and resource constraints. Understanding these challenges is essential for IT companies aiming to implement effective ERM-GRC alignment.

### **2.6.1 Organizational Silos and Fragmented Structures**

One of the most significant barriers to ERM-GRC alignment in IT companies is the existence of organizational silos. Governance, risk, and compliance functions are often managed by separate departments, each with its processes, goals, and metrics. This fragmented structure can hinder collaboration, reduce risk visibility, and impede the effectiveness of ERM-GRC integration.

**Lack of Cross-Functional Collaboration:** In many IT companies, governance, risk management, and compliance functions operate independently, leading to a lack of shared risk data and fragmented risk management efforts. This separation can result in redundancies, gaps in risk coverage, and inefficiencies, making it difficult to establish a cohesive ERM-GRC framework (Ashby et al., 2012).

**Challenges in Creating a Unified Risk Culture:** Organizational silos contribute to disparate risk cultures within IT companies, where different departments have varying levels of risk awareness and engagement. Aligning ERM with GRC requires a unified approach to risk culture, which can be challenging in companies where departments resist change or have conflicting priorities (Simons, 1999).

### **2.6.2 Complexity of Regulatory Requirements**

IT companies operate in a highly regulated environment with numerous standards governing data privacy, cybersecurity, and financial reporting. These regulations, such as GDPR, HIPAA, and SOX, are often complex, and their frequent updates add further challenges for IT companies attempting to maintain compliance through an integrated ERM-GRC approach.

**Constantly Evolving Regulations:** Regulatory landscapes, particularly around data privacy and cybersecurity, are continually changing, requiring IT companies to update their compliance and risk management practices regularly. Staying up-to-date with new

regulations and adapting ERM-GRC frameworks is resource-intensive and can strain internal processes (Woods, 2009).

**Balancing Compliance with Strategic Flexibility:** Strict compliance requirements can constrain the flexibility of ERM frameworks, making it challenging for IT companies to balance regulatory adherence with strategic goals. ERM-GRC alignment requires that compliance efforts be integrated without compromising the organization's ability to respond quickly to new risks or strategic opportunities (Bhimani, 2009).

### **2.6.3 Resource Constraints**

Effective ERM-GRC alignment demands substantial human, technological, and financial investment. IT companies, particularly smaller firms or startups may need help to allocate sufficient resources to implement and maintain an integrated ERM-GRC framework.

**Financial and Technological Limitations:** Implementing an integrated ERM-GRC framework requires investment in specialized software, data analytics tools, and risk assessment technologies. These resources can be prohibitive for IT companies with limited budgets, hindering their ability to establish a comprehensive ERM-GRC alignment (Sax & Andersen, 2019).

**Need for Skilled Personnel:** ERM-GRC alignment is a complex process that requires skilled personnel with expertise in risk management, regulatory compliance, and governance. The demand for specialized talent can strain IT companies' resources, as qualified professionals in these areas are often in short supply and command high salaries. For smaller companies, acquiring and retaining such talent can be challenging (Morrow, 2011).

### **2.6.4 Technological Complexity and Integration Issues**



The rapid pace of technological innovation in the IT sector introduces additional complexity when aligning ERM and GRC. IT companies often operate complex systems and manage large volumes of data, which require robust technological infrastructure to monitor, assess, and mitigate risks effectively. Integrating ERM and GRC processes within these systems can present technical difficulties.

**Difficulty in Integrating Legacy Systems:** Many IT companies rely on legacy systems not designed to support integrated ERM-GRC frameworks. Integrating ERM-GRC practices into these older systems can be challenging, leading to data incompatibilities, system inefficiencies, and increased risk of operational disruption (Oetzel & Getz, 2012).

**Cybersecurity Risks in Digital Transformation:** As IT companies adopt digital transformation initiatives, they face increased cybersecurity risks that complicate ERM-GRC alignment. Ensuring cybersecurity while aligning GRC and ERM frameworks requires continuous monitoring and updating of security measures, which can strain technological resources and make it difficult to maintain alignment (Hoyt & Liebenberg, 2011).

### **2.6.5 Cultural Resistance and Change Management**

Implementing an ERM-GRC alignment often requires cultural shifts within the organization to foster a unified approach to risk and compliance. However, resistance to change can be a significant obstacle, particularly in organizations with established, traditional risk management practices.

**Resistance to Cross-Functional Collaboration:** ERM-GRC alignment requires collaboration across departments, but existing hierarchies and power structures can lead to employee resistance. Some departments may be reluctant to share information or align

their processes with other teams, limiting the effectiveness of ERM-GRC integration (Simons, 1999).

Difficulty in Embedding a Risk-Aware Culture: Aligning ERM with GRC requires an organization-wide commitment to a risk awareness and compliance culture. This cultural shift can be challenging in companies where risk management is traditionally siloed, as employees may be unfamiliar with or resistant to adopting new, integrated practices (Racz et al., 2010).

### **2.6.6 Data Management and Analytics Challenges**

Effective ERM-GRC alignment depends on accurate, timely, comprehensive data for risk assessment, compliance monitoring, and governance. However, managing and analyzing large volumes of data can be challenging, especially in IT companies that rely on real-time data for decision-making.

Data Integration and Quality Issues: Integrating data from multiple sources is essential for ERM-GRC alignment, but data consistency and quality issues can hinder this process. IT companies often collect data from various systems and departments, which can lead to data silos, duplication, and inconsistencies, reducing the accuracy and reliability of risk insights (Power, 2009).

The complexity of Data Analytics and Reporting: ERM-GRC alignment requires advanced data analytics tools to monitor risk, compliance, and governance activities effectively. Many IT companies need help implementing data analytics systems that provide real-time and predictive analytics, limiting their ability to make data-driven decisions promptly (Gates et al., 2012).

For your literature review, here is a comprehensive section on Emerging Trends in ERM and GRC Alignment for IT. This section highlights recent developments and

trends shaping the future of Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) alignment within the IT industry.

## **2.7 Emerging Trends in ERM and GRC Alignment for IT**

As IT companies navigate a dynamic risk landscape, the alignment of Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) frameworks is evolving to meet new demands. Emerging technologies, changing regulatory requirements, and a heightened focus on resilience and sustainability transform how IT firms manage risk and compliance. These trends offer new opportunities for IT companies to enhance ERM-GRC integration, streamline processes, and improve adaptability in the face of emerging threats. The following sections discuss critical trends in ERM and GRC alignment for IT, including the integration of digital tools, a focus on cybersecurity and data privacy, regulatory technology (RegTech) adoption, the rise of Integrated Risk Management (IRM) platforms, and the growing emphasis on resilience and environmental, social, and governance (ESG) considerations.

### **2.7.1 Integration of Advanced Digital Tools and Automation**

Digital transformation within the IT industry has spurred the adoption of advanced digital tools and automation to support ERM and GRC functions. Automation can streamline risk and compliance processes, making them more efficient and less prone to human error.

Artificial Intelligence (AI) and Machine Learning (ML): AI and ML are increasingly used to enhance risk identification, monitoring, and mitigation efforts within ERM-GRC frameworks. These technologies can analyze large datasets to identify patterns, predict potential risks, and automate compliance checks, reducing the manual effort required for ongoing risk management (Oetzel & Getz, 2012). For example, AI

algorithms can detect anomalies in system behaviour that may indicate cybersecurity threats or compliance issues, allowing IT companies to respond proactively.

**Robotic Process Automation (RPA):** RPA is being leveraged to automate repetitive tasks within GRC processes, such as regulatory reporting, data entry, and audit documentation. This automation increases efficiency and allows compliance and risk management teams to focus on strategic activities rather than administrative tasks (Morrow, 2011).

### **2.7.2 Focus on Cybersecurity and Data Privacy**

Given the increasing prevalence of cybersecurity threats and data breaches, IT companies prioritize cybersecurity and data privacy within their ERM-GRC frameworks. Cyber risk has become a top concern for IT firms, prompting the integration of robust cybersecurity measures into GRC processes to safeguard sensitive information and ensure regulatory compliance.

**Cybersecurity Risk Integration:** ERM frameworks incorporate cybersecurity risk assessments to address vulnerabilities and respond to potential threats in real time. GRC platforms increasingly include cybersecurity modules, enabling IT companies to manage cyber and other operational and regulatory risks (Power, 2009).

**Data Privacy Compliance:** Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have introduced stringent data privacy standards, compelling IT companies to integrate data privacy risk management into their ERM-GRC alignment. This integration ensures that data privacy compliance efforts are standardized and risks associated with data handling are monitored continuously (Hoyt & Liebenberg, 2011).

### **2.7.3 Adoption of Regulatory Technology (RegTech)**

Regulatory technology, or RegTech, has emerged as a powerful tool for improving compliance processes in IT companies. RegTech solutions use technology to enhance regulatory monitoring, reporting, and compliance, making it easier for IT companies to stay up-to-date with complex and frequently changing regulations.

**Real-Time Regulatory Monitoring:** RegTech platforms offer real-time regulatory updates and analytics, which help IT companies proactively manage compliance requirements. By automating regulatory monitoring, these tools enable companies to stay compliant without manual tracking, reducing the risk of regulatory breaches (Sax & Andersen, 2019).

**Enhanced Reporting and Analytics:** RegTech solutions provide data-driven insights into compliance performance, helping IT companies identify potential compliance gaps and strengthen their GRC frameworks. This enhanced reporting capability supports a proactive approach to compliance, improving transparency and accountability in regulatory activities (Bhimani, 2009).

#### **2.7.4 Rise of Integrated Risk Management (IRM) Platforms**

Integrated Risk Management (IRM) platforms represent the next generation of GRC technology. They enable IT companies to consolidate governance, risk, and compliance data within a centralized platform. IRM platforms enhance the visibility and coordination of risk-related activities, supporting strategic decision-making and operational resilience.

**Centralization of ERM and GRC Functions:** IRM platforms offer a single, integrated solution that consolidates ERM and GRC activities, improves cross-functional collaboration, and provides real-time insights into risk and compliance status. This centralization enhances risk visibility and reduces redundancies, supporting a more efficient approach to managing risks and regulatory obligations (Kaplan & Mikes, 2012).

Advanced Analytics for Predictive Risk Assessment: Many IRM platforms offer advanced analytics capabilities, enabling IT companies to conduct predictive risk assessments and scenario analysis. This functionality allows organizations to anticipate potential risks and evaluate the impact of various risk scenarios, providing a proactive approach to risk management (Frigo & Anderson, 2011).

### **2.7.5 Emphasis on Resilience and Business Continuity**

Resilience and business continuity have become focal points in ERM-GRC alignment, particularly in the IT sector, where disruptions from cyber threats, regulatory changes, or operational breakdowns can have serious consequences. IT companies increasingly embed resilience measures into their ERM-GRC frameworks to prepare for and recover from adverse events.

Business Continuity Planning (BCP): ERM-GRC frameworks incorporate business continuity planning to ensure that organizations can maintain operations and recover quickly after disruptions. BCP strategies are essential for IT companies that rely heavily on uninterrupted service delivery and data availability (Beasley et al., 2005).

Operational Resilience and Risk Tolerance: IT companies adopt resilience metrics within ERM-GRC frameworks to gauge risk tolerance, such as cyber incidents or supply chain disruptions. This emphasis on resilience allows organizations to make more informed risk-taking decisions and build safeguards that enhance long-term stability (Gates et al., 2012).

### **2.7.6 Growing Consideration of Environmental, Social, and Governance (ESG) Factors**

Environmental, Social, and Governance (ESG) considerations increasingly influence risk management and compliance strategies, mainly as stakeholders demand higher standards of corporate responsibility. Including ESG metrics in ERM-GRC

frameworks enables IT companies to address broader societal impacts and improve stakeholder trust.

**Incorporating ESG Risks into ERM:** Many IT companies are now evaluating ESG risks, such as environmental impact, ethical labour practices, and governance transparency, as part of their ERM frameworks. This trend aligns with stakeholder expectations for responsible business practices and positions IT companies as leaders in corporate sustainability (Freeman, 1984).

**Enhancing Reputation and Stakeholder Confidence:** ESG-focused ERM-GRC alignment allows IT companies to demonstrate a commitment to sustainable practices, enhancing their reputation among investors, customers, and regulatory bodies. By proactively managing ESG risks, IT firms can strengthen their brand reputation and create a competitive advantage (Morrow, 2011).

## **2.8 Summary**

**Theoretical Foundations for ERM-GRC Alignment** delves into the rationale behind aligning Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) frameworks in IT companies, supported by several foundational theories. Agency Theory highlights the inherent conflicts of interest between shareholders (principals) and managers (agents) within organizations, underscoring the need for transparency, accountability, and governance structures that ensure managerial actions align with shareholders' interests. By aligning ERM with GRC, IT companies can improve risk oversight and reduce managerial opportunism, fostering an environment where decision-making is informed and consistent with shareholders' goals.

Contingency Theory suggests that the effectiveness of ERM-GRC alignment depends on how well these frameworks are tailored to fit the company's specific environment, such as industry-related risks and regulatory landscapes. This theory is

particularly relevant to IT companies facing unique challenges like cybersecurity threats and evolving privacy regulations, indicating that ERM-GRC frameworks in such firms should be flexible and adaptable to address these complex, dynamic risks effectively.

Stakeholder Theory broadens the scope of governance beyond shareholders to include all stakeholders impacted by an organization, including customers, employees, regulators, and the community. For IT companies, where issues such as data privacy and cybersecurity are obvious, aligning ERM with GRC frameworks demonstrates a commitment to responsible risk management and compliance practices, building stakeholder trust and enhancing organizational transparency. This alignment reassures stakeholders, who often demand high data protection and security standards, thus positively impacting the organization's reputation.

Finally, the Resource-Based View (RBV) positions ERM-GRC alignment as a valuable organizational asset, enhancing resilience, operational efficiency, and competitive advantage. By integrating ERM and GRC, IT companies create a unified risk management framework that helps them navigate complex regulatory environments and adapt to emerging risks. This alignment allows IT companies to respond proactively to risks and regulatory changes, ultimately supporting long-term sustainability, growth, and competitive positioning in the industry.

These theoretical foundations suggest that ERM-GRC alignment in IT companies transcends mere compliance or risk management. It is a strategic approach that enhances organizational efficiency, builds stakeholder trust, and strengthens resilience, making it essential for IT companies to navigate the complexities of a high-risk, rapidly evolving industry.



## CHAPTER III: METHODOLOGY

### **3.1 Overview of the Research Problem**

This section explores the research problem within the context of IT companies and the challenges they face in aligning Enterprise Risk Management (ERM) with Governance, Risk, and Compliance (GRC) frameworks. This alignment is essential in an environment where regulatory compliance, data privacy, cybersecurity, and operational resilience are constantly scrutinised and evolved (Racz et al., 2010). Although the importance of GRC frameworks is widely recognized, the role of ERM in promoting a cohesive, proactive GRC alignment still needs to be explored in the IT sector. IT companies operate in high-stakes, rapidly changing environments where risks are increasingly complex and interconnected. However, existing literature suggests that many companies handle governance, risk, and compliance as isolated functions, leading to operational inefficiencies and potential vulnerabilities (Ashby et al., 2012).

The central research problem addressed in this study is the hypothesis that ERM can significantly enhance the efficacy of GRC frameworks by creating an integrated structure for managing risks, ensuring compliance, and strengthening governance across IT companies. Although ERM's potential to unify GRC functions is theoretically supported (Frigo & Anderson, 2011), empirical research on IT companies still needs to be expanded. Many companies manage GRC functions in silos, which often results in redundant processes, limited risk visibility, and fragmented resource allocation (Beasley et al., 2005). This fragmentation increases vulnerability to unforeseen risks and compliance failures, particularly as new regulatory requirements and digital risks—such as cybersecurity and data privacy challenges—continue to intensify.

Moreover, IT companies face unique challenges due to rapid technological advancements and stringent regulatory requirements, which often strain traditional risk management frameworks (Mikes & Kaplan, 2015). For instance, regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) require strict data management practices, and failure to comply can lead to severe penalties and reputational damage (Hoyt & Liebenberg, 2011). The fast-paced nature of the IT industry, characterized by continuous innovation and technological evolution, compounds the complexity of these regulatory obligations. As such, there is a strong need to understand how ERM can be implemented as a comprehensive framework that supports IT companies in aligning GRC functions with their strategic objectives and compliance requirements (Power, 2009).

Theoretical perspectives—such as Agency Theory, Contingency Theory, Stakeholder Theory, and the Resource-Based View (RBV)—provide valuable insights into the potential benefits of ERM-GRC alignment (Jensen & Meckling, 1976) (Freeman, 1984); (Barney, 1991) (Donaldson, 2001). Agency Theory, for instance, highlights the need for transparency and accountability, essential for aligning management actions with shareholder interests. Similarly, Contingency Theory emphasizes the importance of adapting risk management practices to fit the organization's unique context, a particularly relevant consideration for IT companies dealing with cybersecurity and data privacy risks (Woods, 2009). Stakeholder Theory expands the governance focus to include all affected parties, advocating for risk management practices that meet the expectations of customers, regulators, and the community (Racz et al., 2010). Lastly, RBV underscores the strategic value of ERM-GRC alignment as a resource that can improve resilience, flexibility, and competitive positioning (Gates et al., 2012).

Despite theoretical support, practical insights into how ERM can drive GRC alignment within IT companies still need to be explored. The fragmented management of GRC functions often leads to inefficiencies that hamper IT companies' ability to respond effectively to emerging risks and regulatory changes (Sax & Andersen, 2019). Therefore, this study aims to fill this gap by exploring whether and how ERM can be operationalized as a catalyst for GRC alignment in IT companies, examining factors that influence successful integration, potential barriers, and measurable outcomes.

In summary, the research problem focuses on understanding ERM's potential as a catalyst for effective GRC alignment within IT companies. This study seeks to contribute to the academic discourse and practical application by exploring the dynamics of ERM-GRC alignment, identifying implementation challenges, and providing actionable recommendations for IT companies aiming to strengthen their governance, risk management, and compliance practices in a complex and highly regulated environment.

### **3.2 Operationalization of Theoretical Constructs**

The study defines and translates the theoretical constructs of ERM-GRC alignment into measurable and actionable variables. This operationalization allows for a systematic approach to examine how Enterprise Risk Management (ERM) aligns with IT companies' Governance, Risk, and Compliance (GRC) functions, guided by the foundational theories introduced in the previous section. Specifically, this study draws on Agency Theory, Contingency Theory, Stakeholder Theory, and the Resource-Based View (RBV) to structure the analysis and measure constructs related to accountability, adaptability, stakeholder engagement, and strategic resource management.

#### **3.2.1 Defining Accountability and Transparency (Agency Theory)**

This study's first theoretical construct operationalized, based on Agency Theory, is accountability and transparency. Agency Theory emphasizes the importance of

aligning managerial actions with shareholder interests by reducing conflicts of interest and establishing robust governance and oversight mechanisms (Jensen & Meckling, 1976). This construct is measured through indicators such as the frequency and quality of risk reporting, the clarity of role definitions within risk management and compliance functions, and the transparency of decision-making processes within IT companies. Surveys and interview protocols will assess these indicators, examining how clearly ERM and GRC responsibilities are defined across organizational levels and the extent to which risk information is shared with shareholders and other stakeholders. The presence of regular reporting structures and the accessibility of risk and compliance information are key metrics to gauge the effectiveness of ERM in fostering accountability and aligning with GRC frameworks (Power, 2009).

### **3.2.2 Adaptability to External and Internal Risks (Contingency Theory)**

Contingency Theory informs the second theoretical construct, adaptability, which emphasizes that ERM-GRC alignment must be customized to fit the organization's/organisation's unique context (Donaldson, 2001). For IT companies, adaptability is particularly critical given the sector's rapidly changing risk landscape, which includes evolving cybersecurity threats and new regulatory requirements. This construct is measured through variables such as the flexibility of ERM-GRC frameworks, the frequency of updates to risk management practices, and the organization's/organization's responsiveness to changes in external regulations or internal risk factors. Metrics include the rate of ERM and GRC policy revisions, the frequency of risk assessments, and the ability to implement changes in compliance protocols as new risks or regulations emerge. Interviews and document analysis of policy revision histories will capture the adaptability of ERM-GRC systems in practice, providing insight into

how well IT companies are prepared to manage dynamic and complex risks (Woods, 2009).

### **3.2.3 Stakeholder Trust and Engagement (Stakeholder Theory)**

The third construct, grounded in Stakeholder Theory, is stakeholder trust and engagement. This construct reflects the importance of considering the interests of all stakeholders impacted by IT companies' operations, such as customers, employees, regulators, and the community at large (Freeman, 1984). In the context of ERM-GRC alignment, stakeholder engagement is measured through indicators like the frequency of stakeholder consultations in risk assessments, the transparency of risk communication with external and internal stakeholders, and the organization's commitment to regulatory compliance. Surveys and case studies will assess how actively IT companies engage stakeholders in compliance and risk management practices, including the frequency of stakeholder feedback mechanisms and the visibility of compliance efforts. The construct will also examine the extent to which ERM-GRC alignment fosters trust, evidenced by stakeholder satisfaction and perceived reliability of data privacy and cybersecurity protocols (Racz et al., 2010).

### **3.2.4 Strategic Resource Allocation and Competitive Advantage (Resource-Based View)**

The fourth theoretical construct, derived from the Resource-Based View (RBV), is strategic resource allocation and competitive advantage. According to RBV, ERM-GRC alignment can be a valuable organizational resource that improves resilience, operational efficiency, and competitive positioning (Barney, 1991). This construct is operationalized through indicators such as investment in risk management infrastructure, allocation of skilled personnel to ERM-GRC functions, and the degree to which ERM-GRC alignment contributes to overall business strategy. Variables include the budget

allocated to ERM-GRC initiatives, the number of personnel dedicated to risk and compliance roles, and metrics assessing the return on investment (ROI) of ERM-GRC initiatives. Data collection will include budget analysis, human resource allocations, and interviews with senior management to determine how resource allocation to ERM-GRC contributes to a sustained competitive advantage and supports strategic goals (Gates et al., 2012).

### **3.2.5 Construct Integration and Measurement**

The constructs of accountability, adaptability, stakeholder engagement, and resource allocation are interdependent and collectively represent the operationalized dimensions of ERM-GRC alignment within IT companies. To ensure consistency in measurement, each construct will be assessed using quantitative and qualitative data collection methods, such as surveys, interviews, and document analysis. Surveys will provide quantitative insights into the extent of ERM-GRC integration. At the same time, interviews with key personnel (e.g., risk managers, compliance officers, and senior executives) will yield qualitative data on challenges and best practices in ERM-GRC alignment. Document analysis will include risk reports, policy documents, and governance records to verify self-reported practices and observe the structural elements supporting ERM-GRC integration.

The findings from these constructs will enable a comprehensive assessment of how ERM serves as a catalyst for aligning GRC functions in IT companies. Each theoretical construct provides a lens for analyzing the effectiveness of ERM-GRC integration in practical, measurable terms. This operationalization framework is designed to produce actionable insights into best practices and identify barriers, thus contributing to a more nuanced understanding of ERM-GRC alignment as both a theoretical and practical construct within IT companies.

### **3.3 Research Purpose and Questions**

This study's aims and specific research questions, focusing on understanding the role of Enterprise Risk Management (ERM) as a catalyst for aligning Governance, Risk, and Compliance (GRC) frameworks in IT companies. Given the rapidly changing risk landscape in the IT sector—marked by evolving cybersecurity threats, complex regulatory requirements, and the pressure for operational resilience—this research is designed to address critical knowledge gaps related to integrating ERM within GRC functions. This section details the study's purpose to examine how ERM can drive cohesive GRC alignment and support strategic objectives in IT companies, along with the research questions that guide this exploration.

### **3.4 Research Design**

This study outlines the framework used to explore the research problem, operationalize theoretical constructs, and answer the research questions. The research design defines the methodology, data collection methods, sampling strategy, and analysis approach for examining how Enterprise Risk Management (ERM) can act as a catalyst for aligning Governance, Risk, and Compliance (GRC) frameworks in IT companies. The study was conducted to gain theoretical and practical insights into ERM-GRC alignment within complex organizational contexts, so a mixed-methods design was selected. This Approach enables a comprehensive exploration of ERM-GRC alignment by combining quantitative data to identify patterns and qualitative insights to uncover contextual factors and deeper motivations.

#### **3.4.1 Mixed-Methods Approach**

This research design follows a mixed-methods approach, integrating quantitative and qualitative data collection and analysis techniques to achieve a holistic understanding of ERM-GRC alignment. Mixed methods provide a balanced approach to studying

complex organizational phenomena, combining objective metrics and contextual insights (Creswell & Plano Clark, 2011).

Quantitative data will be collected through surveys to measure key constructs identified in the study, such as accountability, adaptability, stakeholder trust, and resource allocation. These data points allow for statistical analysis of relationships and patterns in ERM-GRC alignment across IT companies. Meanwhile, qualitative data gathered through in-depth interviews and document analysis will provide a richer, more nuanced understanding of ERM-GRC alignment. These qualitative insights are essential for understanding the mechanisms and challenges associated with ERM-GRC alignment in IT, complementing the quantitative findings and enabling the study to address the research questions thoroughly.

### **3.4.2 Data Collection Methods**

- Surveys

Surveys will serve as the primary tool for quantitative data collection. The surveys are designed to capture data on operationalized constructs—such as accountability, adaptability, stakeholder trust, and resource allocation—identified in Section 3.2. A structured questionnaire will be distributed to a sample of IT companies, targeting personnel involved in ERM and GRC functions, including risk managers, compliance officers, and senior executives. Likert-scale responses will enable consistent quantification of responses for statistical analysis. This Approach ensures that responses are comparable and measurable (Bryman, 2016).

- In-Depth Interviews

To complement the quantitative data, in-depth, semi-structured interviews will be conducted with a subset of survey respondents in senior risk management, governance, or compliance roles within their organizations. These interviews aim to capture qualitative



insights into the unique challenges, practices, and organizational dynamics involved in ERM-GRC alignment. Interview questions will focus on the mechanisms ERM facilitates GRC alignment; specific barriers companies encounter, and the perceived outcomes of alignment. The semi-structured format allows for flexibility in exploring emerging insights while ensuring the critical research areas are covered (Kvale & Brinkmann, 2009).

- Document Analysis

Document analysis will be used to validate and enhance findings from surveys and interviews. This involves analyzing internal documents provided by participating companies, such as risk reports, compliance assessments, and governance policies. Document analysis offers objective data points for verifying self-reported practices and insight into formal structures supporting ERM-GRC alignment. By examining content in risk-related documents, this method also reveals how policies and frameworks are documented, communicated, and revised within organizations (Bowen, 2009).

### **3.4.3 Sampling Strategy**

The study will employ a purposive sampling strategy to ensure participants are well-informed and actively involved in ERM and GRC functions within their organizations. Participants will be selected based on their professional roles (e.g., compliance officers, risk managers, IT governance specialists) to ensure relevance to ERM-GRC alignment. The study aims to include IT companies of varying sizes and sub-sectors (e.g., software development, cloud services, cybersecurity) to capture diverse perspectives.

For the survey portion, a sample size of approximately 50 companies is targeted to allow for statistical analysis, while around 10–15 participants will be selected for in-depth interviews. This sample size is appropriate for data saturation in qualitative

interviews, enabling the capture of diverse insights without redundancy (Guest, Bunce, & Johnson, 2006). The sample will be recruited through industry networks, professional associations, and online platforms dedicated to GRC in the IT sector.

#### **3.4.4 Data Analysis Techniques**

- Quantitative Analysis

Quantitative data from surveys will be analyzed using descriptive statistics and inferential analysis techniques, such as correlation and regression analysis, to identify relationships between the key constructs. Descriptive statistics will provide an overview of the frequency and distribution of responses, giving insight into general trends in ERM-GRC alignment practices across IT companies. Inferential analysis will explore the strength and direction of relationships among accountability, adaptability, stakeholder engagement, and resource allocation, helping to answer research questions related to ERM-GRC integration mechanisms and outcomes (Field, 2013).

- Qualitative Analysis

Qualitative data from interviews and document analysis will be processed using thematic analysis, which enables the identification of patterns and themes across responses. This technique is helpful for categorizing responses into significant themes, such as mechanisms of ERM-GRC alignment, common challenges, and perceived benefits, enabling broader insights from individual cases (Braun & Clarke, 2006). A coding scheme will be developed based on research questions and theoretical constructs, allowing for consistent categorization and analysis of qualitative data.

- Triangulation

To enhance the validity and reliability of findings, the study will use data triangulation, integrating insights from surveys, interviews, and document analysis. Triangulation enables cross-verification of data from different methods, enhancing

robustness and reducing potential bias (Denzin, 1978). By comparing quantitative data on ERM-GRC alignment with qualitative insights from interviews and document analysis, the study can confirm key findings and better understand ERM's role in aligning GRC functions.

### **3.4.5 Ethical Considerations**

Ethical considerations will be a priority throughout the research process, and informed consent will be obtained from all participants. Confidentiality and anonymity will be maintained to protect the identities of participating organizations and individuals. Data will be securely stored and only accessible to authorized researchers, ensuring compliance with data protection regulations and ethical standards (Babbie, 2015). Participants will retain the right to withdraw from the study at any point, ensuring their involvement is fully voluntary.

### **3.4.6 Limitations of the Research Design**

Although the mixed-methods approach offers a comprehensive view of ERM-GRC alignment, the study is limited by reliance on self-reported data, which may introduce biases. Additionally, while ensuring relevant participants, the purposive sampling strategy may limit the generalizability of findings to a broader population of IT companies. However, multiple data sources, including document analysis and triangulation, mitigate these limitations by validating findings and ensuring reliability (Patton, 2002).

## **3.5 Population and Sample**

The study identifies the target population and sample selection criteria for examining the role of Enterprise Risk Management (ERM) in aligning Governance, Risk, and Compliance (GRC) frameworks in IT companies. Given the study's focus on the IT sector, the population includes many IT organizations engaged in governance, risk

management, and compliance functions. This section outlines the target population's characteristics, specifies the sampling strategy, and details the criteria for participant selection.

### **3.5.1 Target Population**

This study's target population comprises IT companies operating in environments with significant regulatory, operational, and cybersecurity risks, necessitating strong governance and compliance frameworks. This includes IT companies across various sub-sectors, such as software development, cloud computing, cybersecurity, data analytics, and managed IT services. These companies typically face unique challenges in managing risks due to the dynamic nature of technological advancements, evolving regulatory landscapes, and heightened exposure to cybersecurity threats (Mikes & Kaplan, 2015).

The study focuses on IT companies that already employ ERM or GRC practices, ensuring relevance to the research questions and response consistency. While smaller organizations with limited resources may be excluded, this study primarily targets medium to large IT firms where ERM-GRC alignment is essential due to complex operational structures and a high volume of regulatory obligations. By focusing on these organizations, the study aims to gain insights into best practices, challenges, and outcomes associated with ERM-GRC alignment in environments with extensive risk and compliance requirements.

### **3.5.2 Sampling Strategy**

The study employs a purposive sampling strategy to ensure that selected participants are engaged in or knowledgeable about ERM and GRC functions within their organizations. Purposive sampling is appropriate for this study because it allows the selection of participants with specific expertise and experience relevant to the research topic (Patton, 2002). This approach ensures that responses reflect well-informed

perspectives on ERM-GRC alignment, capturing insights specific to the IT sector's unique regulatory and operational environment.

The study will aim to gather responses from IT companies of various sizes, though it will focus on medium and large organizations, as these firms are more likely to have formal ERM and GRC functions in place. The sampling strategy also aims to include companies across different sub-sectors to capture diverse perspectives on ERM-GRC alignment.

### **3.5.3 Sample Size**

For the quantitative component of the study (survey distribution), a sample size of approximately 50 IT companies is targeted. This sample size is adequate for conducting statistical analysis, allowing the researcher to identify general patterns and relationships between ERM-GRC alignment practices and outcomes. A sample of this size provides a representative overview of ERM-GRC alignment practices across different IT sub-sectors, enhancing the generalizability of the quantitative findings (Field, 2013).

For the qualitative component (in-depth interviews), approximately 10 to 15 participants from the survey sample will be selected. This subset will include senior personnel involved in governance, risk management, or compliance functions, such as Chief Risk Officers (CROs), compliance officers, risk managers, and IT governance specialists. The chosen sample size for qualitative interviews is intended to reach data saturation, ensuring comprehensive insights without redundancy (Guest, Bunce, & Johnson, 2006). This smaller sample will allow for an in-depth exploration of experiences, challenges, and specific practices related to ERM-GRC alignment.

### **3.5.4 Participant Selection Criteria**

To ensure relevance and depth in the collected data, specific selection criteria will be applied to identify participants who are knowledgeable about ERM and GRC alignment:

**Professional Role:** Participants should be directly involved in governance, risk management, or compliance within their organization, such as CROs, compliance officers, risk managers, or IT governance specialists. This criterion ensures that participants experience ERM and GRC processes firsthand, providing credible and relevant insights (Bryman, 2016).

**Organizational Size and Structure:** The study will primarily target medium to large IT companies where ERM-GRC alignment is more likely to be formalized. These organizations typically have more outstanding regulatory obligations and complex structures, where integrating ERM with GRC frameworks is critical. Small firms, where ERM and GRC may still need to be fully developed, will likely be excluded from the sample.

**Industry Sub-Sector:** To capture a comprehensive view of ERM-GRC alignment across the IT sector, the sample will include companies from various sub-sectors, such as software development, cloud computing, cybersecurity, and data analytics. Each sub-sector has specific risk and compliance requirements, offering valuable insights into how ERM can support GRC alignment across diverse contexts (Hoyt & Liebenberg, 2011).

**Experience with ERM and GRC Integration:** Organizations included in the sample must have some established ERM and GRC practices central to the study's focus. Participants from companies with no formal risk or compliance structures may not provide relevant data for the research questions and will thus be excluded.

### **3.5.5 Recruitment Process**

Participants will be recruited through professional networks, industry associations, and LinkedIn groups focused on governance, risk, and compliance within the IT sector. The study will issue a call for participants through emails, direct messages, and professional channels, inviting qualified individuals to participate in the survey or in-depth interview. Recruitment will focus on obtaining informed consent and clearly understanding the study's purpose, scope, and ethical considerations, ensuring participants are comfortable and willing to share insights on ERM-GRC alignment within their organizations (Babbie, 2015).

### **3.5.6 Limitations and Considerations in Sampling**

While purposive sampling and the targeted population enhance the relevance of findings, there are potential limitations. The primary limitation is that purposive sampling may restrict generalizability, as the sample is not randomly selected. However, focusing on participants with specialized knowledge of ERM-GRC alignment within IT companies is essential for answering the research questions effectively. Additionally, because the study excludes small IT firms with limited ERM-GRC structures, findings may be more applicable to medium and large organizations.

The structured approach to sampling ensures that selected participants provide relevant and reflective insights of current ERM-GRC practices in the IT sector. By focusing on individuals and companies with direct experience in ERM and GRC functions, this study will produce findings that contribute to understanding how ERM can effectively drive GRC alignment in complex, risk-intensive environments like IT.

### **3.6 Participant Selection**

The study outlines the criteria, methods, and rationale for selecting participants, ensuring that the sample consists of knowledgeable individuals actively involved in ERM and GRC functions within IT companies. The study understands how Enterprise Risk

Management (ERM) can enhance governance, risk, and compliance (GRC) alignment; selecting participants with relevant expertise and experience is essential. This section details the participant selection criteria, recruitment process, and considerations to ensure a representative and insightful sample.

### **3.6.1 Selection Criteria**

To achieve meaningful insights into ERM-GRC alignment, the study applies specific selection criteria focused on the participants' historical context and experience with ERM and GRC processes. These criteria are designed to ensure that participants are directly engaged in or knowledgeable about ERM and GRC practices within their organizations, as follows:

**Professional Role:** Participants are selected based on their roles within governance, risk management, or compliance departments, such as Chief Risk Officers (CROs), compliance officers, risk managers, and IT governance specialists. By selecting participants in these critical positions, the study ensures that respondents have direct experience with ERM-GRC functions, providing reliable insights into integration mechanisms, challenges, and outcomes (Bryman, 2016).

**Organizational Size:** The study primarily targets medium to large IT companies where ERM-GRC alignment is more likely to be formalized and integrated into operational structures. These organizations face more significant regulatory pressures and complex operational risks, making ERM-GRC alignment critical. Including smaller firms with limited or informal risk management practices may dilute the relevance of insights for larger-scale ERM-GRC implementations, so they are excluded from this study.

**Industry Sub-Sector:** Participants are drawn from various IT sub-sectors, including software development, cloud computing, cybersecurity, and data analytics. Each sub-sector faces distinct regulatory and operational challenges, and the variety of



sectors provides a more comprehensive view of ERM-GRC alignment across IT. This selection approach allows the study to capture sector-specific insights and enhance the generalizability of findings across the IT industry (Hoyt & Liebenberg, 2011).

**Experience with ERM and GRC:** Participants are required to be involved in organizations with established ERM and GRC practices. This criterion ensures that insights are relevant to the research objectives, as individuals from companies without formal ERM-GRC integration may lack the experience necessary to provide meaningful responses to questions about alignment mechanisms and challenges (Power, 2009).

### **3.6.2 Recruitment Process**

The recruitment process is designed to engage qualified participants who meet the selection criteria and are willing to share insights into ERM-GRC alignment. Recruitment will be conducted through the following channels:

**Professional Networks and Associations:** Participants will be recruited through industry-specific professional networks and associations focusing on governance, risk, and compliance within the IT sector. Relevant associations include the Information Systems Audit and Control Association (ISACA) and the Global Association of Risk Professionals (GARP). These organizations serve as networks for risk management and compliance professionals, ensuring access to qualified candidates.

**LinkedIn and Online Platforms:** Invitations to participate will be extended through LinkedIn and specialized online forums related to IT risk management and governance. These platforms allow the researcher to target professionals who explicitly indicate experience in GRC and ERM functions, increasing the likelihood of recruiting informed participants.

**Direct Outreach to Companies:** Recruitment will also involve direct outreach to IT companies that meet the selection criteria. Formal emails and information packages

will be sent to target companies, inviting eligible personnel to participate in the survey and interviews. This approach ensures that company leadership is informed of the study and can encourage participation from qualified individuals within their teams (Patton, 2002).

### **3.6.3 Sampling for Survey and Interview Participants**

The study employs a two-phase participant selection process to identify individuals for quantitative and qualitative data collection. The initial phase involves recruiting approximately 50 IT companies for the survey, capturing various perspectives on ERM-GRC alignment. Participants are selected based on the criteria outlined above, ensuring that responses reflect the viewpoints of those involved in or knowledgeable about ERM and GRC practices.

The second phase narrows the focus to a subset of 10–15 participants for in-depth interviews. These participants are chosen among the survey respondents who express willingness to participate in follow-up interviews. Interview participants will be selected based on diversity in professional roles, company size, and sub-sector to ensure a well-rounded qualitative sample. This approach ensures that interview data complements survey data by providing deeper, context-rich insights into ERM-GRC alignment (Guest, Bunce, & Johnson, 2006).

### **3.6.4 Ethical Considerations in Participant Selection**

The study prioritizes ethical considerations in selecting and recruiting participants, ensuring transparency, confidentiality, and voluntary participation throughout the process:

**Informed Consent:** All participants will receive detailed information about the study's purpose, study site study, and confidentiality measures, ensuring they can decide

to participate. Written consent will be obtained from each participant prior to data collection.

**Confidentiality:** Confidentiality will be strictly maintained, with all identifying information removed from survey and interview data. Responses will be anonymized, and company-specific information will not be disclosed in any publications or reports derived from the study (Babbie, 2015).

**Right to Withdraw:** Participants will be informed of their right to withdraw from the study at any stage without penalty or consequence. This right will be emphasized in recruitment materials and consent forms, ensuring participants feel comfortable and secure throughout the study.

### **3.6.5 Limitations in Participant Selection**

While the purposive sampling strategy allows for a targeted and relevant sample, there are limitations to consider. First, purposive sampling may limit generalizability, as the sample is not randomly selected. Additionally, by focusing on medium and large IT companies, the study may not capture insights from smaller firms where ERM and GRC may be less formalized. However, these limitations are considered acceptable given the study's objective to explore ERM-GRC alignment in organizations with complex structures and regulatory demands. Triangulation of survey, interview, and document analysis data will further mitigate potential biases and enhance the study's robustness (study, 2002).

## **3.7 Instrumentation**

The tools and instruments used to collect quantitative and qualitative data for this study are detailed. These instruments are carefully designed to capture relevant information on the role of Enterprise Risk Management (ERM) in aligning Governance, Risk, and Compliance (GRC) frameworks in IT companies. This section describes the

survey questionnaire, interview guide, and document analysis checklist as primary data collection instruments. The instruments are designed to operationalize the study's theoretical constructs, ensure reliable and valid data, and address the research questions effectively.

### **3.7.1 Survey Questionnaire**

The survey questionnaire serves as the primary instrument for collecting quantitative data. It is structured to capture insights into key constructs such as accountability, adaptability, stakeholder trust, and resource allocation within ERM-GRC alignment. Each construct is measured using multiple indicators derived from the operationalization framework detailed in Section 3.2. The questionnaire is designed to produce data that can be statistically analyzed, providing measurable insights into how IT companies implement ERM-GRC alignment and the outcomes associated with these efforts.

#### Structure of the Questionnaire

The questionnaire includes five main sections:

- **Demographic Information:** Questions regarding the participant's professional role, years of experience, company size, and industry sub-sector to contextualize responses.
- **ERM-GRC Practices:** Questions to assess the company's current ERM and GRC practices, including how these frameworks are integrated and formalized.
- **Construct-Based Questions:** Items measuring each theoretical construct:
- **Accountability and Transparency:** Questions using Likert scales to assess the clarity of ERM-GRC roles, frequency of risk reporting, and decision-making transparency.

- **Adaptability:** Questions on the frequency of ERM-GRC policy updates, flexibility in response to regulatory changes, and integration of new risk factors.
- **Stakeholder Trust and Engagement:** Items measuring stakeholder involvement in risk assessments, transparency in compliance efforts, and frequency of communication with stakeholders.
- **Resource Allocation:** Questions evaluating investment in ERM-GRC initiatives, availability of dedicated personnel, and perceived return on investment.
- **Outcomes of ERM-GRC Alignment:** Questions measuring perceived benefits, such as improved risk visibility, enhanced compliance, and organizational resilience.
- **Open-Ended Questions:** Two open-ended questions will allow participants to elaborate on challenges and unique practices in ERM-GRC alignment.
- **Pilot Testing and Reliability:** The questionnaire will undergo pilot testing with a small group of participants to ensure clarity and relevance. Feedback from the pilot will inform any necessary revisions to improve question-wording, flow, and response options. Reliability testing, such as Cronbach's alpha, will assess internal consistency across the construct-based items, ensuring that the questionnaire provides reliable and repeatable measurements (Field, 2013).

### **3.7.2 Interview Guide**

The interview guide is the primary instrument for collecting qualitative data. It is designed to gather in-depth insights into the processes, challenges, and organizational dynamics involved in ERM-GRC alignment. The guide is semi-structured, allowing flexibility to explore unexpected themes while ensuring that key areas related to the research questions are covered.

Structure of the Interview Guide

The interview guide includes four main sections:

- **Introduction and Contextual Information:** Opening questions about the participant's background, role, and responsibilities to establish rapport and gather context on the participant's experience with ERM and GRC.
- **ERM-GRC Alignment Mechanisms:** Questions focused on how ERM is integrated with GRC functions, including reporting structures, accountability mechanisms, and risk communication processes.
- **Challenges and Barriers:** Inquiries into specific challenges the organization faces in aligning ERM and GRC, such as organizational silos, resource constraints, or regulatory complexities.
- **Outcomes and Perceived Benefits:** Questions examining the benefits of ERM-GRC alignment, such as improved compliance, enhanced risk visibility, and increased stakeholder trust. Participants are asked to share specific examples or stories to illustrate these outcomes.
- **Closing and Additional Insights:** Open-ended questions that invite participants to share any additional thoughts or unique practices related to ERM-GRC alignment.
- **Ensuring Validity:** The interview guide is developed based on the theoretical framework and research questions to ensure content validity, ensuring alignment with the study's objectives (Kvale & Brinkmann, 2009). Expert reviews from ERM and GRC professionals will be conducted to validate the relevance of interview questions, providing confidence that the instrument adequately captures critical dimensions of ERM-GRC alignment. Additionally, conducting semi-structured interviews allows for probing follow-up questions to clarify and explore responses in greater depth, adding to the validity of qualitative insights.

### **3.7.3 Document Analysis Checklist**

The document analysis checklist serves as an instrument to guide the systematic examination of internal documents, such as risk assessments, compliance reports, and governance policies. Document analysis provides objective data for verifying self-reported practices and understanding how ERM and GRC frameworks are formally documented and implemented.

#### Essential Items in the Checklist

The checklist is designed to capture specific information from organizational documents relevant to ERM-GRC alignment, organized into the following categories:

- **ERM and GRC Policy Documentation:** Verify formal ERM and GRC policies, including their scope, objectives, and the extent to which they are integrated.
- **Reporting and Communication Structures:** Evidence of structured reporting lines, including risk reporting frequency and transparency to stakeholders and senior management.
- **Risk Assessment and Compliance Monitoring:** Documentation of risk assessment methods, risk prioritization criteria, compliance monitoring activities, and any evidence of continuous updates to address new risks or regulatory changes.
- **Stakeholder Engagement Records:** Evidence of stakeholder consultation in risk assessments, compliance communication strategies, and methods for engaging external and internal stakeholders in risk management.
- **Resource Allocation Records:** Budget allocations, resource allocations, or records on staffing dedicated to ERM and GRC functions.
- **Ensuring Consistency in Document Analysis:** To ensure consistency, the checklist will be used systematically across all documents provided by participating companies. Detailed notes and observations will be recorded, and patterns across organizations will be analyzed to triangulate data with survey and interview

findings. This approach adds credibility to the research by cross-verifying self-reported practices and observing formal documentation practices within IT companies (Bowen, 2009).

#### **3.7.4 Data Quality and Instrument Reliability**

To enhance data quality and reliability across all instruments, several steps are incorporated into the research design:

- **Pilot Testing:** The survey questionnaire and interview guide will undergo pilot testing with a small sample to ensure clarity and relevance. Feedback will inform refinements, enhancing the instruments' reliability and face validity.
- **Triangulation:** Data collected from the survey, interviews, and document analysis will be cross-validated to ensure accuracy and consistency across sources. This triangulation method helps validate findings and strengthens the reliability of conclusions drawn from multiple perspectives (Denzin, 1978).
- **Training for Consistent Application:** The researcher will follow standardized procedures for document analysis and interviews, ensuring consistent data collection across all participant interactions and document reviews. The use of a checklist and semi-structured guide facilitates consistency in the application of qualitative methods.

#### **3.7.5 Limitations of Instrumentation**

While these instruments are designed to capture a broad spectrum of data on ERM-GRC alignment, potential limitations exist. The survey's reliance on self-reported data could introduce response biases, as participants may overstate or understate their ERM-GRC practices. To mitigate this, survey data will be triangulated with interview findings and document analysis, providing a more balanced and comprehensive view. Additionally, the qualitative nature of interviews and document analysis could introduce



subjective interpretations; however, systematic use of coding frameworks and consistency checks will minimize potential biases (Patton, 2002).

### **3.8 Data Collection Procedures**

The data collection strategy for this research is designed to gather quantitative and qualitative data, allowing for a comprehensive analysis of Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) alignment practices in IT companies. This strategy will involve three primary methods: structured surveys, in-depth interviews or focus groups, and expert validation and pilot testing of data collection instruments. Each component is carefully chosen to ensure the collected data is accurate, representative, and aligned with the study's research objectives.

- **Structured Surveys:** This study's primary data collection tool will be a structured survey targeting professionals directly engaged in ERM and GRC functions within IT companies. The survey is designed to capture quantitative data that aligns with the research questions, aiming to identify standard practices, challenges, and outcomes associated with ERM-GRC alignment.
- **Questionnaire Design:** The survey will be developed based on the theoretical framework and critical constructs outlined in the research objectives, such as accountability, adaptability, stakeholder engagement, and resource allocation within ERM-GRC alignment. Each survey section will contain closed-ended questions and Likert scale items. Closed-ended questions will capture demographic information, such as the participant's role, years of experience, company size, and industry sub-sector, to provide context to their responses. Likert scale questions will assess levels of agreement or frequency, enabling a structured measurement of participants' perspectives on ERM-GRC practices (Bryman, 2016).

- **Distribution Method:** The survey will be administered electronically using a secure online platform like Qualtrics or SurveyMonkey to ensure easy access and efficient data collection. This electronic format allows the survey to be widely distributed across various IT companies, reaching professionals regardless of their geographic location. Using an electronic format also ensures that responses are collected in real time, facilitating data monitoring and analysis.
- **Response Rate Management:** To maximize response rates and reduce non-response bias, follow-up reminders will be sent to participants who have not completed the survey within the initial two-week window. A second reminder will be issued one week later, extending the collection period to approximately four weeks. This approach aims to improve response completeness and minimize potential response biases that could skew the results (Dillman et al., 2014).
- **Data Security and Confidentiality:** All survey data will be stored in an encrypted, password-protected database to ensure confidentiality and protect participants' privacy. To maintain confidentiality, responses will be anonymized, with identifying information separated from survey responses. Only authorized researchers will access the raw data, safeguarding participants' identities.
- **In-depth interviews or Focus Groups:** In parallel with the survey, qualitative data will be collected through semi-structured interviews or focus groups with a subset of survey participants. This component is intended to capture deeper insights into ERM-GRC alignment, such as the organizational culture, operational challenges, and specific practices that influence its effectiveness.
- **Participant Selection:** From the survey respondents, a subset of participants who express interest in follow-up engagement and meet specific selection criteria will be invited for interviews or focus groups. Criteria will include holding senior

roles in risk management, governance, or compliance (e.g., Chief Risk Officers, compliance officers, or IT governance specialists) to ensure participants can provide informed and relevant insights. This purposive sampling approach ensures that qualitative data reflects in-depth experiences with ERM-GRC alignment (Patton, 2002).

- **Interview/Focus Group Structure:** The interviews or focus groups will use a semi-structured guide with open-ended questions covering the key research themes. Topics will focus on mechanisms of ERM-GRC alignment, organizational challenges, specific alignment practices, and perceived benefits. This approach allows for flexibility, encouraging participants to share their experiences in detail and explore new ideas that may emerge during discussions.
- **Thematic Analysis:** Interview and focus group data will be transcribed and analyzed using thematic analysis. This qualitative analysis method will identify recurring themes, trends, and patterns in participants' responses, providing a deeper contextual understanding of ERM-GRC alignment. The themes from this analysis will be compared and integrated with survey data to provide a more comprehensive view of ERM-GRC practices (Braun & Clarke, 2006).
- **Data Confidentiality:** All interview and focus group recordings and transcripts will be stored securely, with identifying information removed to ensure confidentiality. Audio recordings will be transcribed, and transcripts will be anonymized, allowing participants to speak freely without concern for personal identification.
- **Expert Validation and Pilot Testing:** A rigorous validation process, including expert review and pilot testing, will be conducted before full data collection

begins to ensure the reliability and validity of the survey and interview instruments.

- **Expert Review:** ERM and GRC experts will review the survey and interview guide, preferably individuals with significant experience in risk management and compliance in the IT sector. The experts will assess each question for relevance, clarity, and alignment with the research objectives. Feedback from these experts will be used to refine the instruments, ensuring they effectively capture the constructs necessary for the study's analysis (Field, 2013).
- **Pilot Testing:** After expert validation, the instruments will be pilot-tested with a small sample of participants similar to the target population. Pilot testing allows for identifying any ambiguities, misunderstandings, or logistical issues that might arise during full-scale data collection. Any adjustments will be made to ensure the final instruments are clear, concise, and aligned with the study's objectives (Dillman et al., 2014).
- **Reliability and Validity Assessment:** To assess the internal reliability of survey items, a reliability test, such as Cronbach's alpha, will be conducted on pilot survey responses. This measure evaluates whether survey items consistently measure the intended constructs, enhancing the overall reliability of the instrument. Additionally, face validity will be ensured by expert review, which assesses whether the instruments appear to measure what they intend to measure.
- **Ethical Considerations:** Throughout the data collection process, ethical guidelines will be strictly followed to protect participants' rights and ensure data integrity:
- **Informed Consent:** Before participating in the survey, interviews, or focus groups, participants will receive comprehensive information about the study's purpose, procedures, and confidentiality measures. Consent will be obtained electronically

for survey participation and in written form for interviews and focus groups, confirming that participants understand and agree to the study's terms (Babbie, 2015).

- **Confidentiality and Anonymity:** All data collected, including survey responses, interview transcripts, and focus group discussions, will be anonymized to protect participants' identities. Identifiable information will be separated from data during storage and analysis, ensuring findings are reported without attributing responses to specific individuals or organizations.
- **Data Security:** All digital data will be encrypted and stored in password-protected files to prevent unauthorized access. Physical copies of documents, if collected, will be securely stored in locked facilities accessible only to authorized research personnel. Data will be handled in compliance with data protection regulations, ensuring that participant information remains secure throughout the study (Dillman et al., 2014).
- **Right to Withdraw:** Participants will be informed of their right to withdraw from the study without penalty, emphasizing that their involvement is voluntary and they retain control over their participation.
- **Data Integration and Analysis:** After collecting all data, a triangulation approach will be employed to integrate quantitative survey results with qualitative insights from interviews or focus groups. This process will involve comparing and cross-verifying data from different sources to confirm findings and enhance the study's validity. By analyzing patterns in the survey data alongside thematic insights from interviews and focus groups, the study will achieve a well-rounded view of ERM-GRC alignment practices in IT companies.

- **Limitations of Data Collection Procedures:** Despite a comprehensive approach, there are potential limitations to this data collection strategy:
- **Response Bias in Surveys:** Self-reported data in surveys may be subject to response bias, as participants may overstate or understate their practices. Triangulation with qualitative data mitigates this limitation by providing additional perspectives and validating self-reported information.
- **Access to Senior Professionals:** Scheduling interviews or focus groups with senior-level professionals can be challenging due to time constraints. Flexible scheduling and virtual meetings will increase accessibility and reduce dropout rates.
- **Access to Confidential Documents:** Although not a primary instrument, some organizations may be reluctant to share sensitive materials if any internal documents are provided for analysis. To encourage transparency, strict confidentiality and secure data handling will be assured.

Overall, this data collection strategy is designed to be rigorous, ethically sound, and aligned with the study's objectives, allowing for comprehensive and reliable data that addresses the research questions and enhances the understanding of ERM-GRC alignment within IT companies

### **3.9 Data Analysis**

The study outlines a detailed statistical approach for analyzing the quantitative data collected from surveys and other measures, along with qualitative data where applicable. The primary goal of this analysis is to provide a comprehensive understanding of ERM-GRC alignment in IT companies by examining relationships between key variables, validating the reliability and accuracy of developed metrics, and integrating findings to address the research objectives. The data analysis strategy involves multiple

stages, including descriptive and inferential statistical techniques, subgroup analyses, and validity and reliability assessments.

### **3.9.1 Descriptive Statistics**

The first step in analyzing the survey data involves descriptive statistics to summarize the demographic characteristics of participants and provide an overview of responses to the survey questions. This phase will include:

- **Demographic Overview:** Descriptive statistics will summarize participant demographics, such as professional roles, years of experience, organizational size, and industry sub-sector. Frequent distributions and percentages will be used to describe these categorical variables.
- **Central Tendency and Dispersion:** For each construct-related question, measures of central tendency (mean and median) and measures of dispersion (standard deviation and range) will be calculated. These statistics provide insight into responses' central values and variability, offering an initial overview of how participants perceive ERM-GRC alignment in their organizations.
- **Frequency Distributions:** Frequency distributions for Likert-scale responses will be generated to visualize the spread of responses across categories (e.g., strongly agree to disagree strongly). This helps identify patterns in ERM-GRC alignment perceptions, such as the extent to which specific alignment strategies or challenges are commonly recognized across IT companies.

These descriptive statistics will serve as a foundation for understanding the data structure before moving into more complex analyses, providing context to the relationships explored in later stages (Field, 2013).

### **3.9.2 Inferential Statistics**

Following the descriptive analysis, inferential statistical techniques will examine relationships between variables, test hypotheses, and explore the underlying factors influencing ERM-GRC alignment. The main techniques include correlation analysis, regression analysis, and subgroup analyses.

- **Correlation Analysis:** Correlation analysis will examine the strength and direction of relationships between constructs such as stakeholder influence, alignment strategies, assessment tools, metrics development, and challenges in ERM-GRC alignment. Pearson's correlation coefficient will be calculated for continuous variables, while Spearman's rank correlation may be used for ordinal data. This analysis will help identify which constructs are closely associated, providing insight into how different factors interact in ERM-GRC alignment within IT companies (Field, 2013).
- **Regression Analysis:** Regression analysis will be conducted to identify significant predictors of ERM-GRC alignment and to assess the relative importance of various factors. Multiple regression models will evaluate how different independent variables (e.g., organizational size, stakeholder engagement level, adaptability in ERM-GRC practices) predict alignment outcomes. Regression analysis will clarify the role of specific factors in enhancing ERM-GRC alignment, quantifying the strength of these influences while controlling for other variables. Both linear regression for continuous outcome measures and logistic regression for binary outcomes may be applied as needed (Cohen et al., 2003).
- **Hypothesis Testing:** Hypotheses developed from the research objectives will be tested to determine whether observed relationships between variables are statistically significant. For all tests, the significance level will be set at  $\alpha = 0.05$  unless otherwise specified, ensuring a 95% confidence level for conclusions



drawn. Statistical software packages like SPSS or R will be used to conduct these analyses efficiently.

### **3.9.3 Subgroup Analyses**

Subgroup analyses will be performed to explore potential differences in ERM-GRC alignment based on demographic or organizational variables. This analysis aims to identify whether factors such as organizational size, industry sector, and stakeholder involvement level influence ERM-GRC alignment practices.

- **Chi-Square Tests and ANOVA:** For categorical variables (e.g., organizational size categories or industry sub-sectors), Chi-square tests will examine associations between these groups and ERM-GRC alignment measures. For continuous variables, Analysis of Variance (ANOVA) will assess differences in alignment scores across groups. Where significant differences are detected, post hoc tests (e.g., Tukey's HSD) will be conducted to identify specific group differences.
- **T-Tests and ANCOVA:** Independent t-tests will compare alignment practices between two groups (e.g., companies with high vs. low stakeholder involvement) for continuous variables. Additionally, Analysis of Covariance (ANCOVA) may be used to examine the effect of a demographic factor while controlling for other variables, providing a more nuanced understanding of subgroup differences in ERM-GRC alignment.

These subgroup analyses will enable a deeper exploration of how demographic or structural factors impact alignment practices, offering targeted insights that may be relevant for IT companies of various types and sizes (Field, 2013).

### **3.9.4 Validity and Reliability Assessment**

Validity and reliability assessments will be conducted on the survey and interview constructs to ensure the accuracy and consistency of developed metrics. This step ensures that the instruments measure the intended constructs effectively and yield reliable results.

- **Factor Analysis:** Exploratory Factor Analysis (EFA) will be performed to assess the construct validity of the survey items. This technique will identify underlying factors within survey responses, verifying that items group together as expected based on the theoretical constructs. Adjustments will be made to items that do not load appropriately on their intended factors if necessary.
- **Reliability Testing:** Cronbach's alpha will be calculated for each construct to assess internal consistency reliability. A Cronbach's alpha value of 0.70 or higher will be considered acceptable for most constructs, indicating that items within each construct consistently measure the same underlying concept. Items with low item-total correlations will be reviewed and, if necessary, revised or removed to improve reliability (Cohen et al., 2003).
- **Item Validity and Refinement:** Survey and interview items will be refined to enhance validity based on pilot testing feedback and factor analysis results. Items that may have ambiguous wording or appear redundant will be revised or removed, ensuring that each question accurately captures the intended aspect of ERM-GRC alignment.

### **3.9.5 Qualitative Data Analysis**

For the qualitative data obtained from interviews or focus groups, thematic analysis will be used to identify recurring themes and patterns. This qualitative approach allows for extracting rich insights into ERM-GRC alignment practices and provides context for interpreting quantitative results.

- **Transcription and Coding:** Audio recordings from interviews and focus groups will be transcribed verbatim to capture all participant responses. Using coding software (e.g., NVivo or ATLAS.ti), transcripts will be coded line by line, organizing data into initial codes based on key themes, such as challenges in alignment, stakeholder engagement, and perceived benefits.
- **Theme Development:** After initial coding, similar codes will be grouped into broader themes that reflect common ideas or perspectives among participants. Themes such as "alignment mechanisms," "organizational challenges," and "outcomes of alignment" will be reviewed and refined to ensure accuracy and consistency.
- **Integration with Quantitative Data:** The themes derived from qualitative analysis will be compared with the quantitative findings from the survey data, allowing for triangulation. This approach will highlight areas of agreement or divergence, providing a fuller picture of ERM-GRC alignment in IT companies (Braun & Clarke, 2006).

### **3.9.6 Software and Significance Levels**

All statistical analyses will be conducted using SPSS or R software, which provides comprehensive tools for conducting descriptive, inferential, and subgroup analyses. The significance level for inferential tests will be set at  $\alpha = 0.05$ , ensuring that the study's findings are robust and statistically reliable unless otherwise specified. For qualitative data analysis, NVivo or ATLAS.ti will be used for efficient coding and theme identification, enhancing the rigour and transparency of the qualitative analysis process.

### **3.9.7 Summary and Integration of Findings**

After all analyses are conducted, the quantitative and qualitative findings will be integrated to provide a comprehensive understanding of ERM-GRC alignment within IT

companies. This integration will be achieved by synthesizing quantitative relationships with qualitative themes, allowing the study to present a well-rounded view of the alignment practices, challenges, and outcomes observed.

The final analysis will address each research question directly, interpret the results in light of the theoretical framework, and discuss implications for both theory and practice. By combining quantitative rigour with qualitative depth, this data analysis approach ensures that the study's findings are statistically valid and contextually rich, contributing valuable insights to the understanding of ERM-GRC alignment in the IT sector.

### **3.10 Research Design Limitations**

The Study acknowledges several limitations that may impact the effectiveness of the research design, data collection, and analysis in capturing a comprehensive view of ERM-GRC alignment in IT companies. By recognizing these constraints, the Study provides a balanced interpretation of its findings and offers avenues for future research to build on or address potential weaknesses.

- **Survey Limitations**

While critical for gathering quantitative data, the survey component is limited by inherent biases associated with self-reported data. Participants may unintentionally skew their responses toward socially desirable answers, leading to response bias and potentially misrepresenting actual ERM-GRC alignment practices. Furthermore, though beneficial for quantitative analysis, the survey's closed-ended and Likert-scale questions restrict the depth and nuance of participant responses. This limitation may hinder the Study's ability to capture complex ERM-GRC dynamics fully. Additionally, non-response bias could impact the sample if certain groups, such as smaller IT firms or companies with less

formalized GRC practices, are underrepresented despite follow-up reminders (Dillman et al., 2014).

- Qualitative Data Collection Constraints

The qualitative component, involving semi-structured interviews or focus groups, provides essential insights but is subject to practical and interpretive limitations. Scheduling challenges with senior professionals (e.g., CROs and compliance officers) may reduce the sample size, potentially limiting the diversity of perspectives. Moreover, qualitative data from interviews inherently involves subjective viewpoints that may reflect individual biases or organizational cultures, impacting the consistency and generalizability of the findings. Despite the semi-structured guide's aim to reduce interviewer bias, maintaining complete objectivity is challenging, as the interviewer's tone and questioning style may influence participant responses (Patton, 2002).

- Inferential Analysis and Subgroup Analysis Limitations

The research design includes inferential statistical techniques, such as correlation and regression analysis, to examine relationships between variables and test hypotheses. However, these techniques depend on sample size and statistical assumptions, which may only sometimes be met. For instance, small subgroup sizes may reduce statistical power, affecting the reliability of subgroup comparisons in ERM-GRC alignment practices. Regression analysis may also face challenges due to potential violations of assumptions like linearity and normality, which can limit the accuracy and interpretability of predictive models (Field, 2013). Additionally, with multiple predictors in the regression models, there is a risk of overfitting, where the model fits the sample data well but may not generalize to other samples or populations.

- Reliability and Validity Concerns

Efforts to ensure the reliability and validity of data collection instruments are made through expert review and pilot testing. However, construct validity limitations may still arise, as some survey items might need to fully encapsulate the complex nature of ERM-GRC alignment, particularly within the nuanced context of IT. Additionally, while Cronbach's alpha and factor analysis are used to test internal consistency, reliability in qualitative coding remains inherently subjective, and inter-coder variability may impact thematic interpretations (Cohen et al., 2003). Pilot tests, though beneficial, are conducted with a limited sample, meaning that unforeseen issues in broader data collection may not be fully accounted for.

- Data Integration and Triangulation Challenges

Integrating quantitative and qualitative data enhances the Study's comprehensiveness but introduces interpretive challenges. Triangulation between data types requires careful alignment of findings, as disparities between survey results and interview insights may emerge. For instance, quantitative data may reveal general patterns, while qualitative insights provide nuanced context, and reconciling these findings into cohesive conclusions can be complex. Additionally, there is a risk of confirmation bias during integration, where the researcher might inadvertently favour data that supports existing assumptions or hypotheses (Denzin, 1978).

- Generalizability Constraints

The purposive sampling approach and focus on medium to large IT firms may limit the generalizability of findings, as the experiences of smaller IT firms with fewer resources may differ substantially. Furthermore, the IT-specific focus restricts applicability to other industries with different risk profiles and regulatory requirements. The Study's insights may thus be most relevant to IT organizations with formalized

ERM-GRC practices and may not fully represent alignment processes in smaller or less regulated environments.

- Ethical and Practical Constraints

While ethical guidelines are rigorously followed, practical constraints such as restricted access to sensitive internal documents may limit the extent of document analysis, reducing the Study's ability to cross-validate self-reported practices. Additionally, while ethically necessary, participants' right to withdraw from the Study at any time could result in incomplete datasets, particularly for interviews or focus groups, potentially affecting the robustness of thematic analysis (Babbie, 2015).

### **3.11 Conclusion**

In conclusion, the methodology outlined in this study provides a comprehensive approach to exploring ERM-GRC alignment in IT companies by employing a mixed-methods research design. The methodology integrates quantitative rigour with qualitative depth through structured surveys, in-depth interviews, and document analysis, allowing for a holistic examination of the factors influencing ERM-GRC alignment, the operational mechanisms in place, and the resulting organizational outcomes. Each data collection instrument—surveys, interviews, and document analysis—has been meticulously designed and validated to capture the study's core constructs, including accountability, adaptability, stakeholder trust, and resource allocation, ensuring alignment with the theoretical framework.

The methodological approach offers several strengths, notably integrating quantitative and qualitative data. It enhances the study's capacity to triangulate findings and confirm patterns in ERM-GRC practices across IT companies. By systematically addressing potential biases and limitations, such as response bias in surveys and interviewer bias in qualitative data, the methodology aims to produce reliable, credible

insights that contribute to understanding how ERM can effectively drive GRC alignment in IT environments.

However, it is essential to acknowledge the limitations inherent in this methodology. Factors such as response bias, the interpretive nature of qualitative data, and the constraints of purposive sampling may affect the generalizability and precision of the findings. The study addresses these limitations through strategies such as expert review, pilot testing, and rigorous ethical standards to safeguard participant confidentiality and data integrity. These efforts reassure the audience about the study's reliability. Despite these efforts, the findings may be most applicable to medium and large IT organizations with established ERM-GRC practices, which may not fully represent the experiences of smaller firms.

Overall, this study's methodological design offers a robust foundation for investigating ERM-GRC alignment, balancing detailed statistical analysis with contextual, qualitative insights. This approach aims not only to uncover actionable recommendations but also to inspire hope for IT companies seeking to integrate ERM with GRC frameworks. The study's findings could enhance risk management, compliance practices, and governance structures in an increasingly complex regulatory environment.

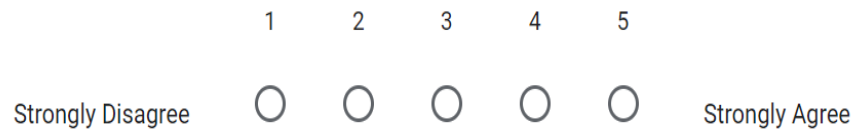


## CHAPTER IV:

### RESULTS

#### 4.1 Data collections and analysis process

- The data collection process occurred through the circulation of a Google form.
- The Google form had four sections addressing the four objectives of the study, respectively. A total of 268 data points were collected for analysis.
- Each question was measured through a Likert Scale of point 5, ranging from Strongly Disagree to Strongly Agree as in Figure 1
- The respondents had to choose one of the five options for each question, which were presented in a linear scale format.
- The whole analysis was divided into 5 sections.
- At the beginning of each section, the scale with its meaning was provided for reference purposes. Thereafter, we import the necessary libraries in Python for the analysis. A few include pandas, numpy, matplotlib, plot, seaborn, and scipy.stats.



*Figure 1 Likert Scale*

##### 4.1.1 Data cleaning

- Before we proceed to the analysis, it is important to clean the data so that the statistical tests can be performed and the right conclusions can be derived.

- Hence, we first start by dropping unnecessary columns such as 'Timestamp'. Since this isn't relevant to the analysis, we can safely drop it.
- Then, we rename the columns. The raw downloaded data in CSV format consisted of column names that matched the questions asked in the Google forms. However, it would be unfeasible to type the questions every time, so we shortened the names and kept them relevant to the study as in figure 2.

```
#drop irrelevant columns and rename columns
df.drop("Timestamp", axis = 1, inplace = True)
df.columns = ['risk_management_domain', 'gender', 'age_group', 'edu', 'ind_exp', 'involved_in_risk_assess', 's
ext_influence_risk_strategy', 'int_stakeholder_clarity', 'stakeholder_feedback_integ', 'stakeho
stakeholder_impact_assess', 'leadership_commun_imp', 'stakeholder_influence_align', 'stakeholde
policy_procedure_align', 'commun_reporting_eff', 'training_awareness_programs', 'compliance_reg
feedback_loops_improve', 'tools_integrate_strategic_planning', 'techniques_assess_compliance_ri
proactive_risk_management', 'align_assess_tools_eff', 'staff_training_erm_grc_tools', 'tools_te
strategies_integrat_lacking', 'commun_issues_erm_grc', 'diff_approaches_risk_assess', 'lack_pol
technology_integrat_issues', 'align_struggles_regulatory_changes', 'unclear_leadership_erm_grc'
```

Figure 2 Data Cleaning-Shortened the names

- Thereafter, the categorical demographic variables were converted to numerical ones by replacing the original values and mapping them to the new ordinal ones as in figure 3.

```
#Encoding categorical variables
demo.replace({'No' : 1, 'Yes' : 2,\
'Female' : 1, 'Male' : 2, 'Prefer not to say' : 3,\
'18-34' : 1, '35-54' : 2, '55-64' : 3, '65+' : 4,\
'Other' : 0, 'Professional Degree' : 1, 'Undergraduate' : 2, 'Post Graduate' : 3, 'Doctorate / P
'0-2' : 1, '3-5' : 2, '6-8' : 3, '9-11' : 4, '11+' : 5}, inplace = True)
```

Figure 3 Data Cleaning-Mapping to ordinal values

- For simplicity, the data frames were subdivided into five different data frames, each catering to one section at a time as in figure 5.

```

#distributing sections as per objectives

demo = df[['risk_management_domain', 'gender', 'age_group', 'edu', 'ind_exp', 'involved_in_risk_assess']]

sec_1 = df[['stakeholder_risk_consultation', 'ext_influence_risk_strategy', 'int_stakeholder_clarity', 'stakeholder_engage_critical', 'formal_stakeholder_influence', 'stakeholder_impact_assess', 'leader_stakeholder_influence_align', 'stakeholder_training_provision']]

sec_2 = df[['risk_ident_consist', 'policy_procedure_align', 'commun_reporting_eff', 'training_awareness_program', 'compliance_regulatory_requirements', 'risk_mitigation_eff', 'feedback_loops_improve']]

sec_3 = df[['tools_integrate_strategic_planning', 'techniques_assess_compliance_risks', 'tools_enable_risk_compliance', 'proactive_risk_management', 'align_assess_tools_eff', 'staff_training_erm_grc_tools', 'tools_technology_integrate_issues']]

sec_4a = df[['inexp_risk_assess']]

sec_4b = df[['strategies_integrat_lacking', 'commun_issues_erm_grc', 'diff_approaches_risk_assess', 'lack_policy', 'technology_integrat_issues', 'align_struggles_regulatory_changes', 'unclear_leadership_erm_grc']]

```

Figure 4 Division of dataframes into 5 sections

## 4.2 Descriptive Statistics

### 4.2.1 Belonging to Risk Management Domain

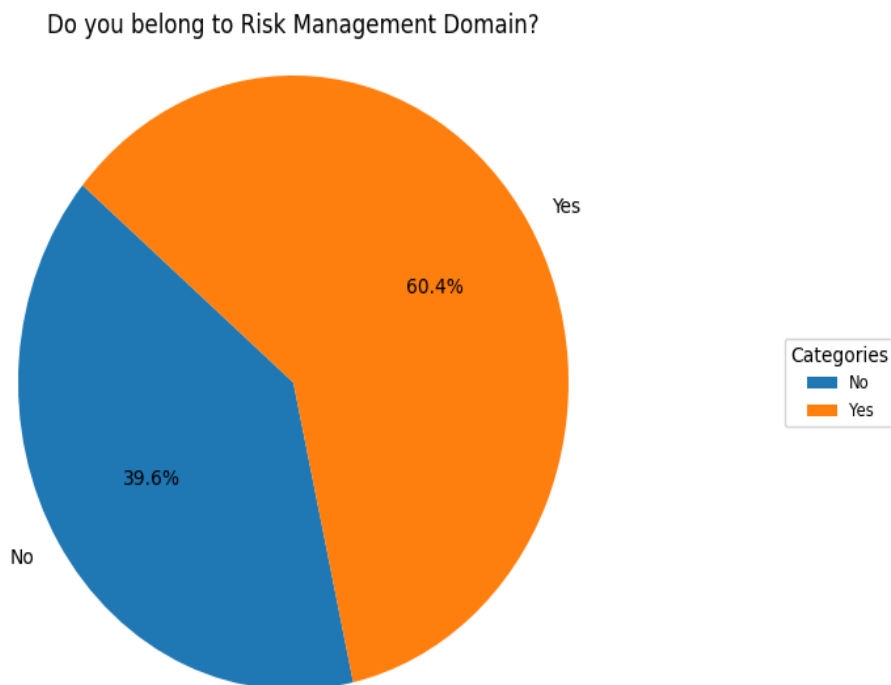
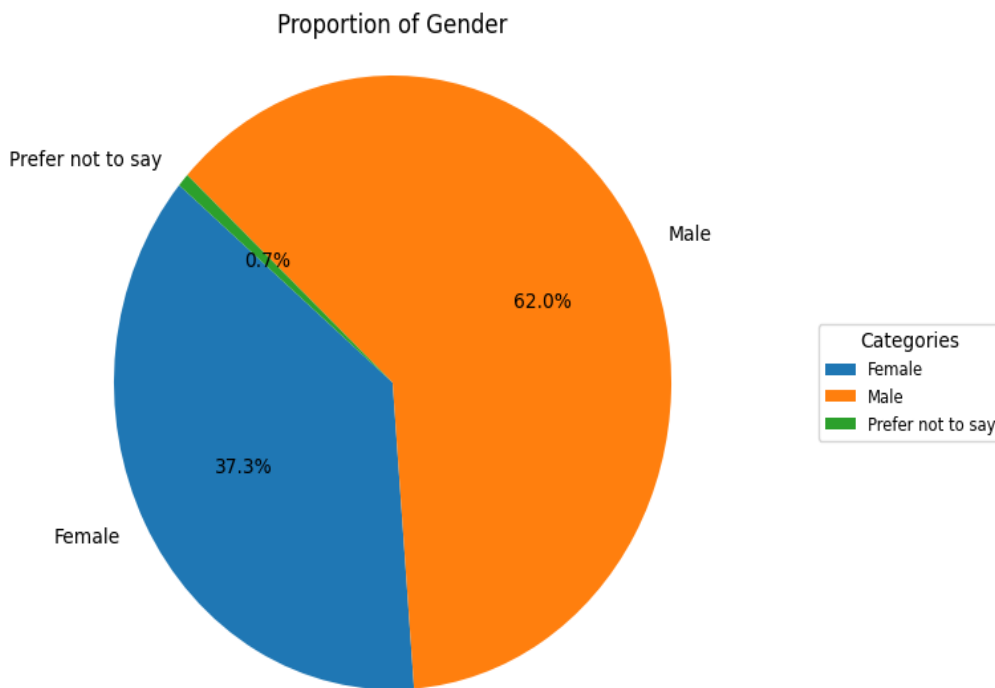


Figure 5 Belonging to Risk Management Domain

Figure 5 shows belonging to the Risk Management Domain, 60.4% of respondents belong to the risk management domain, while 39.6% do not. This suggests a majority presence of professionals from or related to the risk management field among the respondents.

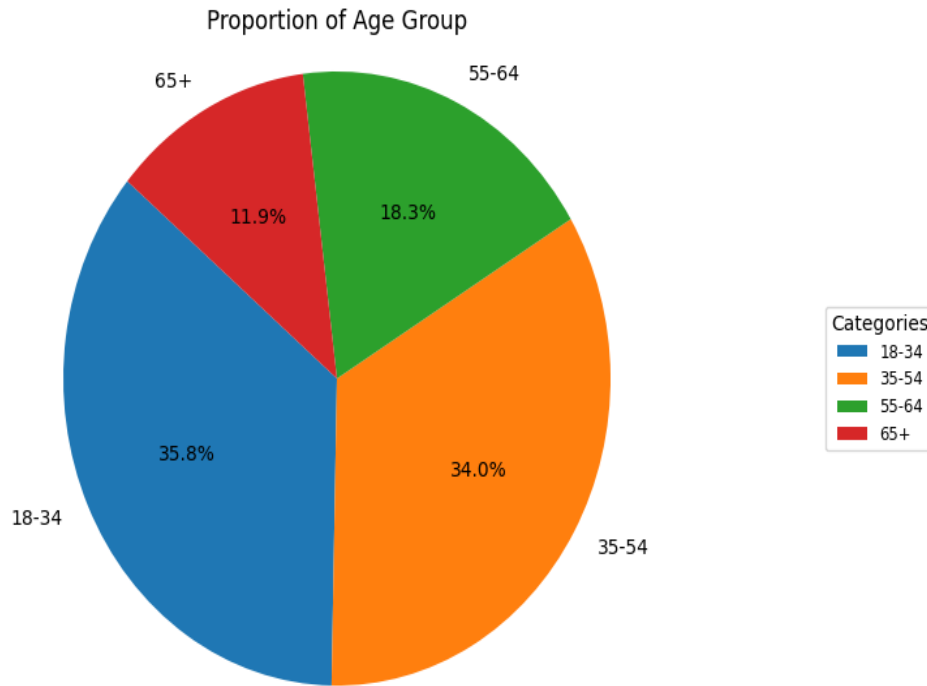
#### 4.2.2 Proportion of Gender



*Figure 6 Proportion of Gender*

In figure 6 the gender distribution among the respondents shows that 62.0% are male, 37.3% are female, and a tiny fraction (0.7%) prefer not to disclose their gender. This indicates a higher representation of males in this particular survey sample.

### 4.2.3 Proportion of Age Group



*Figure 7 Proportion of Age Group*

In the figure 7 the age distribution is diverse: 35.8% are aged 18-34, indicating a significant presence of younger professionals. 34.0% are aged 35-54, vigorously representing mid-career professionals. 18.3% are in the 55-64 age bracket. 11.9% are 65 or older, suggesting participation from senior and possibly retired professionals.

### 4.2.4 Proportion of Educational Background

In the figure 8 educational backgrounds vary among respondents: 38.1% have an undergraduate degree. 31.0% hold a professional degree, which could include fields such as law, business, or engineering. 20.1% have completed postgraduate studies. 8.2% have attained a Doctorate or PhD. 2.6% fall into the 'Other' category, which may include less traditional or unspecified forms of education.

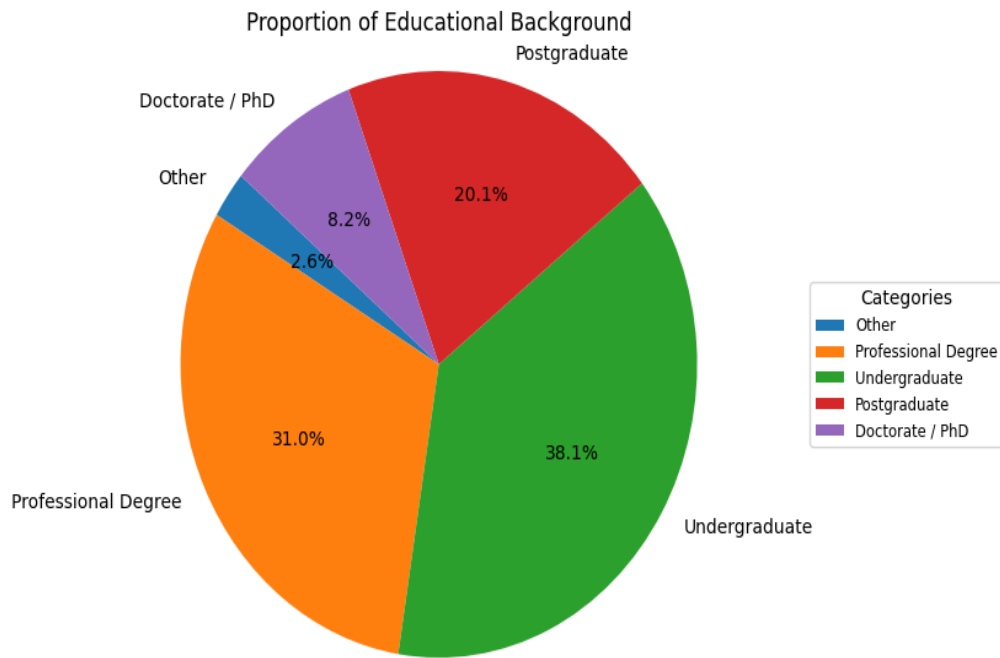


Figure 8 Proportion of Educational Background

#### 4.2.5 Proportion of Industry Experience

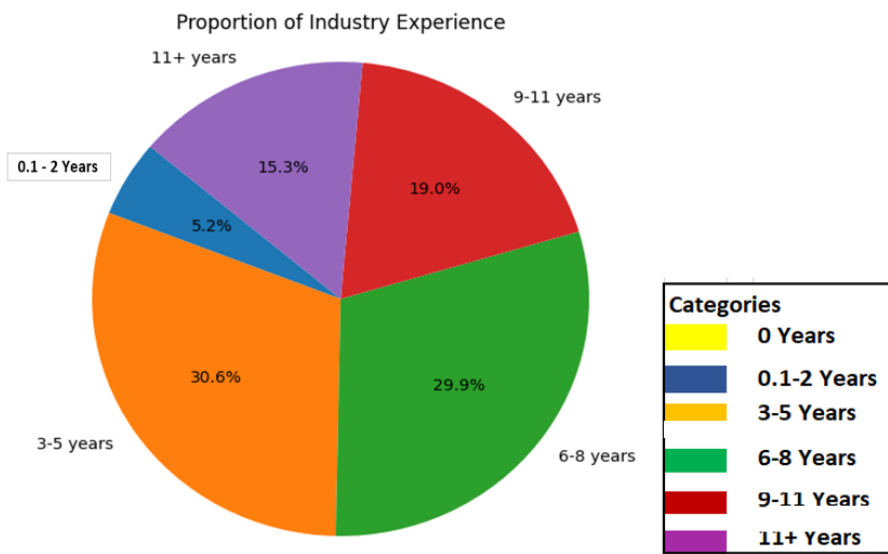
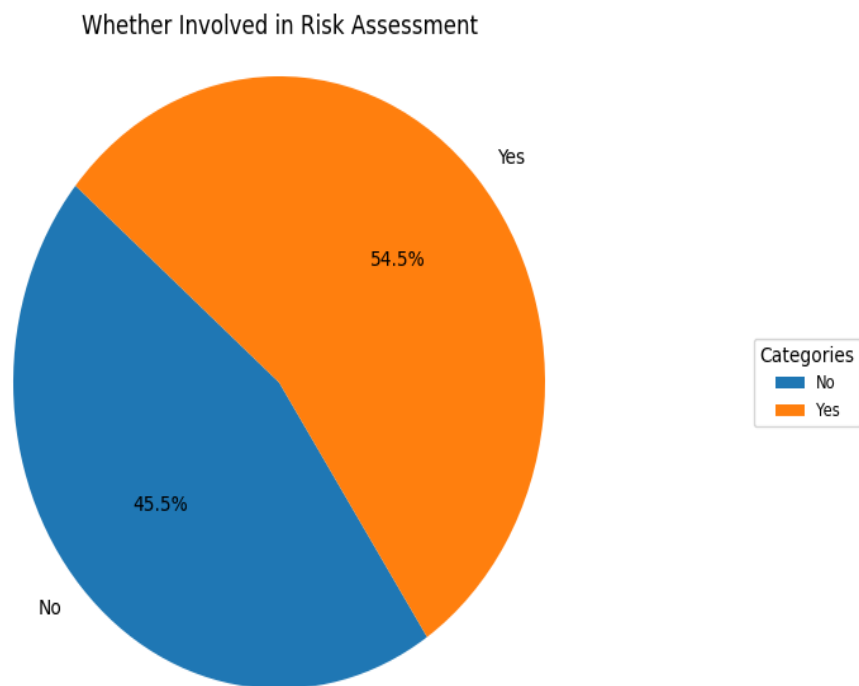


Figure 9 Proportion of Industry Experience

In the figure 9 the spread of industry experience among respondents showcases a range of expertise levels:

- 30.6% have 3-5 years of experience.
- 29.9% have 6-8 years of experience, indicating that many respondents are well into their careers but only sometimes at a senior level.
- 19.0% have 9-11 years of experience.
- 15.3% have been in the industry for over 11 years, pointing to seasoned expertise.
- 0.1 - 2 Years: Represents 5.2% of the total, indicating the smallest group of individuals.

#### 4.2.6 Whether involved in Risk Assessment



*Figure 10 Involvement in Risk Assessment*

#### **4.2.7 Summary**

The survey demographic details suggest a professional audience with substantial representation from the risk management sector, skewed towards a male majority and a broad age distribution. Educationally, the respondents are highly qualified, with a significant number holding advanced degrees. In terms of industry experience, there is a good mix, with the majority having more than three years of experience, indicating that the respondents are not only academically proficient but also practically seasoned. This diversity and depth in demographics might provide rich insights into the risk management practices and perceptions among such a varied group.

### **4.3 Inferential Statistics for Assessing Stakeholder Influence on ERM-GRC Processes**

#### **4.3.1 Histograms for all columns**

We start with plotting histograms for all the columns of this section to understand the distribution of those variables as in figure 11.



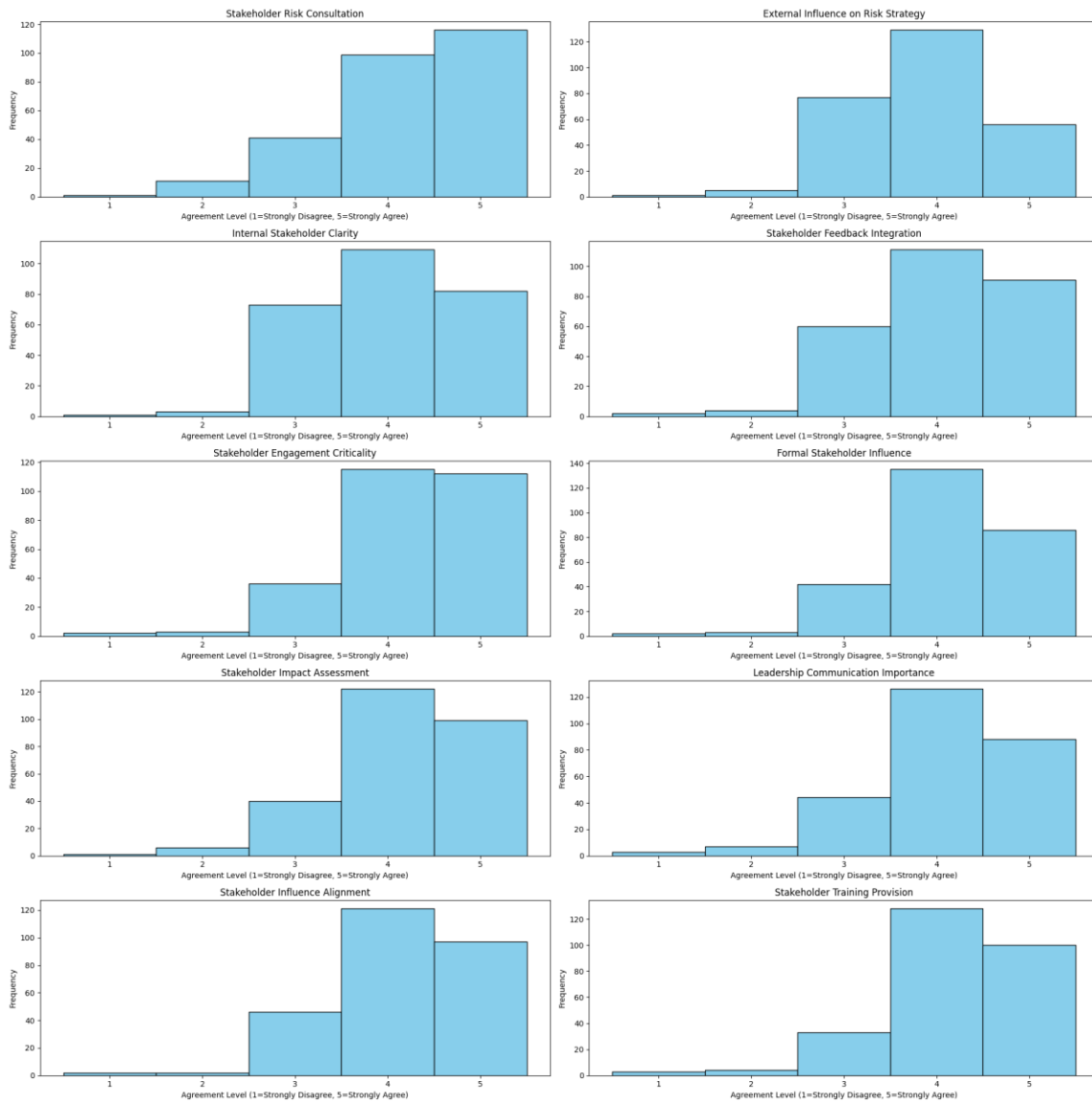


Figure 11 Histograms

### 4.3.2 Interpretations from the Histograms

From figure 11 following interpretations are drawn.

- **Stakeholder Risk Consultation**

The histogram shows a predominant agreement level of 5, indicating that most respondents strongly agree that stakeholders are regularly consulted about their risk

tolerance and preferences. This suggests effective stakeholder engagement in risk management.

- **External Influence on Risk Strategy**

Most respondents are neutral (level 3) about external stakeholders significantly influencing the organization's risk management strategies. This implies a balanced view or uncertainty regarding external stakeholder influence.

- **Internal Stakeholder Clarity**

Responses are skewed towards strong agreement (level 5), indicating that internal stakeholders clearly understand their roles and responsibilities in risk management, which is crucial for effective internal coordination.

- **Stakeholder Feedback Integration**

This histogram peaks at level 5, showing that many respondents strongly agree that feedback from stakeholders is systematically incorporated into updating risk management policies. This suggests good practices in integrating feedback.

- **Stakeholder Engagement Criticality**

The majority agree (level 5) that stakeholder engagement is critical to the effectiveness of Governance, Risk Management, and Compliance (GRC) activities, emphasizing the importance of stakeholder involvement.

- **Formal Stakeholder Influence**

The response distribution peaks at level 5, showing strong agreement that stakeholders have a formal mechanism to influence decisions related to Enterprise Risk Management (ERM)-GRC processes, indicating structured stakeholder involvement.

- **Leadership Communication Importance**

Most respondents strongly agree (level 5) that the organization's leadership effectively communicates the importance of stakeholder input in governing risk and compliance, highlighting effective leadership communication.

- **Stakeholder Impact Assessment**

The histogram peaks strongly at level 5, indicating that regular assessments are conducted to measure the impact of stakeholder influence on the effectiveness of ERM-GRC processes. This shows proactive evaluation practices.

- **Stakeholder Influence Alignment**

This histogram shows a majority at level 5, strongly agreeing that stakeholder influence aligns with the organization's long-term strategic goals in the context of ERM-GRC, suggesting strategic alignment.

- **Stakeholder Training Provision**

Most respondents strongly agree (level 5) that stakeholders receive adequate training to understand and effectively contribute to the ERM-GRC processes, indicating good training practices.

- **Final Summary**

The histograms collectively indicate a robust positive perception among the survey respondents towards stakeholder engagement in risk management. There is a consistent pattern of solid agreement on the importance of stakeholder consultation, clarity in their roles, systematic integration of their feedback, and the significance of their influence on ERM-GRC processes. Most respondents also view the alignment of stakeholder influence with organizational goals favourably and believe adequate training is provided to them. These responses suggest a well-integrated approach to stakeholder management within the organization's risk management and compliance frameworks.

### **4.3.3 Correlation Matrix of Responses**

Thereafter, we plot the correlation between all the variables within this section to understand the inter-relationship between these variables.

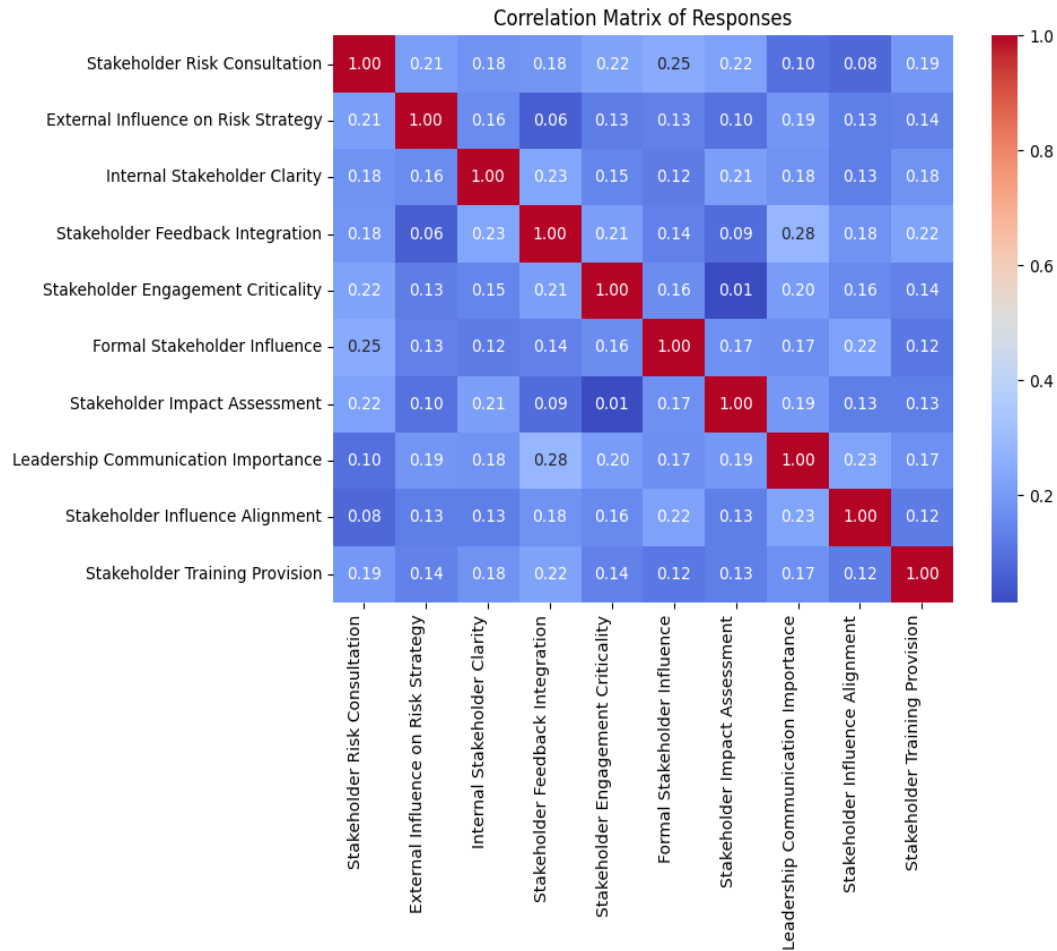


Figure 12 Correlation Matrix of Responses

#### 4.3.4 Interpretations from Correlation Matrix

From figure 12 following interpretations are drawn.

- **Stakeholder Risk Consultation:**

It shows a strong positive correlation (0.22) with stakeholder engagement criticality, indicating that frequent stakeholder consultations are crucial to the

effectiveness of governance, risk, and compliance (GRC) activities. A moderate correlation (0.25) with Formal Stakeholder Influence suggests that regular consultations might be linked with formal mechanisms of influence in organizational decisions.

- **External Influence on Risk Strategy**

It is not strongly correlated with most other variables, suggesting that external stakeholder views may not have a widespread impact on internal risk management practices.

- **Internal Stakeholder Clarity**

Moderately correlated (0.23) with Stakeholder Feedback Integration, indicating that more apparent roles and responsibilities might facilitate better integration of stakeholder feedback into risk management policies.

- **Stakeholder Feedback Integration**

Shows some correlation with Stakeholder Engagement Criticality (0.21), suggesting that integrating feedback effectively could enhance the perceived criticality of engagement processes.

- **Stakeholder Engagement Criticality**

As expected, it is highly correlated (1.00) with itself and shows a reasonable correlation (0.21) with Stakeholder Feedback Integration, reinforcing the idea that effective feedback mechanisms are crucial for engaging stakeholders meaningfully.

- **Formal Stakeholder Influence**

Has a significant correlation with Stakeholder Impact Assessment (0.17), which could mean that formal influence mechanisms are effective at assessing the impact of stakeholder influence on GRC processes.

- **Stakeholder Impact Assessment**

There is a very low correlation with most variables, indicating that these assessments may be isolated or not well integrated with other aspects of stakeholder engagement in the surveyed organizations.

- **Leadership Communication Importance**

Moderate correlations with variables like Stakeholder Feedback Integration (0.28) and Stakeholder Influence Alignment (0.23) suggest that effective leadership communication is essential for aligning stakeholder influence with strategic goals and integrating feedback into policies.

- **Stakeholder Influence Alignment**

This shows a moderate correlation with the importance of leadership communication (0.23), reinforcing the importance of leadership in steering stakeholder influence towards strategic objectives.

- **Stakeholder Training Provision**

This variable stands out for its correlation with Stakeholder Engagement Criticality (0.22), indicating that training provisions may be vital in enhancing the effectiveness of stakeholder engagement in GRC activities.

- **Summary**

The correlation matrix reveals that while there are moderate links between various facets of stakeholder engagement and risk management, many relationships are not particularly strong, which could suggest potential areas for improvement. Key takeaways include the importance of clear internal stakeholder roles, effective stakeholder feedback mechanisms, and the critical role of leadership communication in aligning stakeholder influence with organizational goals. These insights could be instrumental for organizations looking to bolster their risk management frameworks by enhancing

stakeholder integration and influence, ultimately leading to more robust and effective risk management strategies.

#### **4.3.5 Kruskal Wallis Test**

- The Kruskal-Wallis test is performed primarily to determine if there are statistically significant differences between the medians of three or more independent groups.
- The Kruskal-Wallis test was used in the analysis for several vital reasons, especially pertinent to the nature of the data and the research objectives.
- **Non-Parametric Data:** The Kruskal-Wallis test is non-parametric, meaning it does not assume a normal distribution. This characteristic makes it particularly useful for analyzing ordinal data or when the normality assumption cannot be satisfied, which is often the case in survey data collected using Likert scales.
- **Comparing Multiple Groups:** This test evaluates whether the populations from which the samples originate have identical distribution shapes. This was crucial in your analysis, where multiple groups based on different categorical independent variables (like levels of involvement in risk management) were compared.
- **Ordinal Data:** Given that the survey responses were likely on an ordinal scale (such as Likert scale responses), the Kruskal-Wallis test is ideal as it ranks data and compares medians across groups, thus providing a more accurate analysis of such data types than methods assuming interval scale data.
- **Robustness to Outliers:** This test is less sensitive to outliers than parametric tests like ANOVA. Since outliers can often skew the results in small sample sizes or skewed distributions typical in survey responses, using the Kruskal-Wallis test helps achieve more reliable results.

- **General Applicability:** It is suitable for small and large samples, making it a versatile choice in exploratory studies where sample sizes vary across groups.

By using the Kruskal-Wallis test, the analysis aimed to robustly determine if there were statistically significant differences in the median scores of the assessed survey items across different groups defined by their engagement level in risk management activities. This is critical in understanding and interpreting variations in perceptions and practices within the organization regarding risk management.

**With Risk Management Domain:** To understand whether the sample's responses came from the same population with respect to various demographic groups, we performed a Kruskal Wallis test for each of the demographic variables with the variables within this section.



Results for Stakeholder Risk Consultation:

Test Statistic: 4.81

p-value: 0.028

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for External Influence on Risk Strategy:

Test Statistic: 0.24

p-value: 0.621

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Internal Stakeholder Clarity:

Test Statistic: 0.25

p-value: 0.617

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Feedback Integration:

Test Statistic: 0.16

p-value: 0.691

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Engagement Criticality:

Test Statistic: 0.49

p-value: 0.484

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Formal Stakeholder Influence:

Test Statistic: 0.13

p-value: 0.719

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Impact Assessment:

Test Statistic: 2.99

p-value: 0.084

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Leadership Communication Importance:

Test Statistic: 0.03

p-value: 0.853

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Influence Alignment:

Test Statistic: 0.36

p-value: 0.549

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Training Provision:

Test Statistic: 4.31

p-value: 0.038

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

*Figure 13 Results of Krushkal Wallis Test*

### **4.3.6 Interpretation of Krushkal Wallis Test**

From figure 13 following interpretations are drawn.

- **Stakeholder Risk Consultation**

Test Statistic: 4.81

p-value: 0.028

Interpretation: A statistically significant difference exists in how stakeholder risk consultation is perceived across the groups, suggesting variations in consultation practices or perceptions among different risk management domains.

- **External Influence on Risk Strategy**

Test Statistic: 0.24

p-value: 0.621

Interpretation: There is no statistically significant difference, indicating that the influence of external stakeholders on risk strategy is consistently perceived across the groups.

- **Internal Stakeholder Clarity**

Test Statistic: 0.25

p-value: 0.617

Interpretation: Similar to external influence, the clarity of internal stakeholder roles does not significantly differ across the groups.

- **Stakeholder Feedback Integration**

Test Statistic: 0.16

p-value: 0.691

Interpretation: There is no significant variation in how feedback from stakeholders is integrated, suggesting a uniform approach across different domains.

- **Stakeholder Engagement Criticality**

Test Statistic: 0.49

p-value: 0.484

Interpretation: Stakeholder engagement is equally critical across all groups, with no significant differences noted.

- **Formal Stakeholder Influence**

Test Statistic: 0.13

p-value: 0.719

Interpretation: The influence of stakeholders through formal mechanisms does not vary significantly across the groups.

- **Stakeholder Impact Assessment**

Test Statistic: 2.99

p-value: 0.084

Interpretation: While the p-value approaches significance, it suggests only a potential variation in how the impact of stakeholders is assessed across groups, but not enough to be statistically definitive.

- **Leadership Communication Importance**

Test Statistic: 0.03

p-value: 0.853

Interpretation: The importance of leadership communication is viewed consistently across groups, with no significant differences.

- **Stakeholder Influence Alignment**

Test Statistic: 0.36

p-value: 0.549

Interpretation: The alignment of stakeholder influence with organizational goals is similar among groups.

- **Stakeholder Training Provision**

Test Statistic: 4.31

p-value: 0.038

Interpretation: Significant differences exist in how stakeholder training provisions are handled across different risk management domains, indicating variability in training practices or their perceived importance.

- **Summary:**

The Kruskal-Wallis test results indicate significant differences in only two out of ten tested areas: Stakeholder Risk Consultation and Stakeholder Training Provision. These areas show variability across risk management domains, suggesting that some domains prioritize or handle these aspects differently. There are no significant differences for most other areas, such as external influence, internal clarity, feedback integration, and the importance of leadership communication, indicating a uniform approach across domains. This could suggest that certain aspects of stakeholder management and risk strategy are standardized or universally recognized across the sectors represented in the survey.

Results for Stakeholder Risk Consultation:

Test Statistic: 0.65

p-value: 0.421

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for External Influence on Risk Strategy:

Test Statistic: 0.01

p-value: 0.909

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Internal Stakeholder Clarity:

Test Statistic: 0.02

p-value: 0.889

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Feedback Integration:

Test Statistic: 0.00

p-value: 0.987

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Engagement Criticality:

Test Statistic: 0.51

p-value: 0.475

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Formal Stakeholder Influence:

Test Statistic: 0.33

p-value: 0.563

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Impact Assessment:

Test Statistic: 1.66

p-value: 0.198

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Leadership Communication Importance:

Test Statistic: 0.14

p-value: 0.710

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Influence Alignment:

Test Statistic: 1.04

p-value: 0.308

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Stakeholder Training Provision:

Test Statistic: 5.54

p-value: 0.019

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

*Figure 14 With involvement of risk assessment activities*

#### **4.3.7 Interpretation with being involved in risk assessment activities:**

From figure 14 following interpretations are drawn

- **Stakeholder Risk Consultation**

Test Statistic: 0.65

p-value: 0.421

Interpretation: There were no significant differences in perceptions of stakeholder risk consultation across the groups, suggesting a uniform view regardless of involvement in risk assessment.

- **External Influence on Risk Strategy**

Test Statistic: 6.01

p-value: 0.014

Interpretation: Significant differences exist, indicating that groups differ in how they perceive the influence of external stakeholders on risk strategy. Based on respondents' risk assessment involvement, this suggests varying degrees of external stakeholder impact.

- **Internal Stakeholder Clarity**

Test Statistic: 0.02

p-value: 0.889

Interpretation: Uniformity in perceptions regarding the clarity of internal stakeholder roles across different groups.

- **Stakeholder Feedback Integration**

Test Statistic: 0.00

p-value: 0.987

Interpretation: Extremely consistent views on stakeholder feedback integration, indicating no difference between groups.

- **Stakeholder Engagement Criticality**

Test Statistic: 0.51

p-value: 0.475

Interpretation: Stakeholder engagement is uniformly seen as critical across all groups, with no significant variation.

- **Formal Stakeholder Influence**

Test Statistic: 0.33

p-value: 0.563

Interpretation: Similar to other facets of stakeholder management, there is no significant difference in how formal stakeholder influence is perceived.

- **Stakeholder Impact Assessment**

Test Statistic: 1.66

p-value: 0.198

Interpretation: Although the p-value is not less than 0.05, there is a suggestion of varying perceptions, albeit not strong enough to be statistically significant.

- **Leadership Communication Importance**

Test Statistic: 0.14

p-value: 0.710

Interpretation: Leadership communication is consistently valued across all groups, with no significant differences.

- **Stakeholder Influence Alignment**

Test Statistic: 1.04

p-value: 0.308

Interpretation: There is no significant variation in how stakeholder influence alignment is perceived among the groups.

- **Stakeholder Training Provision**

Test Statistic: 5.54

p-value: 0.019

Interpretation: Significant differences exist, suggesting that views on the provision of stakeholder training vary depending on whether respondents are involved in risk assessment. This might indicate that experience in risk assessment affects perceptions of the necessity and effectiveness of training.

- **Summary:**

Overall, the Kruskal-Wallis test results indicate that for most aspects related to stakeholder management and leadership communication, there is no significant variation across different groups based on their involvement in risk assessment. Significant differences were noted in only two areas: External Influence on Risk Strategy and Stakeholder Training Provision. This suggests specific areas where involvement in risk assessment may influence perceptions differently, highlighting the need for tailored approaches depending on the audience's level of involvement in risk assessment activities.

#### **4.3.8 Cliff's Delta (Effect Size):**



---

Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Risk Consultation':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'External Influence on Risk Strategy':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Internal Stakeholder Clarity':  
-0.99 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Feedback Integration':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Engagement Criticality':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Formal Stakeholder Influence':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Impact Assessment':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Leadership Communication Importance':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Influence Alignment':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Training Provision':  
-0.97 (large)

*Figure 15 Cliff's Delta with risk management*

### **4.3.9 Interpretations with risk management domain**

Interpretations based on figure 15 are as follows:

- Cliff's Delta between 'Risk Management Domain' and 'Stakeholder Risk Consultation': -0.97 (large)
- Cliff's Delta between 'Risk Management Domain' and 'External Influence on Risk Strategy': -0.98 (large)
- Cliff's Delta between 'Risk Management Domain' and 'Internal Stakeholder Clarity': -0.99 (large)

... (similar large negative deltas for all other compared factors).

All reported values are negative and close to -1, indicating a significant and consistent effect size. This implies that there are significant differences between those within the risk management domain and other domains or groups in terms of perceptions or practices related to stakeholder engagement and risk management.

- **Magnitude and Direction**

The deltas are enormous (close to -1), meaning that the scores in the Risk Management Domain are typically much lower than those in the compared groups for all listed aspects. This suggests that respondents within the Risk Management Domain have significantly different (and lower) perceptions or reported experiences in these areas than those outside this domain.

- **Substantial Differences**

Such large deltas underscore substantial differences in how risk management is perceived or implemented, suggesting that the Risk Management Domain might have stricter, more conservative, or less favourable views on these aspects than other domains.

- **Summary**

The results indicate profound differences between the Risk Management Domain and other groups across all tested aspects of stakeholder management and risk strategy. This could reflect unique challenges, standards, or experiences that distinguish the Risk Management Domain in handling risks and stakeholders compared to other domains. Understanding these differences is crucial for aligning cross-departmental strategies and improving overall risk management practices. This analysis could guide targeted interventions to bridge gaps and enhance risk and stakeholder management coherence across various organizational domains.

#### **4.3.10 Interpretations being involved in risk assessment activities**

The output provided in figure 16 shows the results of Cliff's Delta calculations, which measure the effect size between two groups in the data—those "involved in Risk Assessment" and others not involved.

Cliff's Delta between 'If involved in Risk Assessment' and 'Stakeholder Risk Consultation':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'External Influence on Risk Strategy':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Internal Stakeholder Clarity':  
-0.99 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Stakeholder Feedback Integration':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Stakeholder Engagement Criticality':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Formal Stakeholder Influence':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Stakeholder Impact Assessment':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Leadership Communication Importance':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Stakeholder Influence Alignment':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Stakeholder Training Provision':  
-0.97 (large)

*Figure 16 Cliff's Delta with risk assessment*

#### **4.3.11 Cliff's Delta Interpretation**

Based on figure 16 interpretations are as below

- Values close to -1 or 1 indicate a large effect size. This means there is a substantial difference between the two groups being compared.
- Negative values indicate that the median of the first group (those involved in risk assessment) is typically lower than the median of the second group across various measures.
- Extensive categorization indicates a significant and impactful difference between groups.

#### **4.3.12 Detailed Interpretation of Each Measure**

- **Stakeholder Risk Consultation**

A delta of -0.97 suggests that those involved in risk assessment possibly rate or perceive stakeholder risk consultation as less favourable or less frequent than their counterparts.

- **External Influence on Risk Strategy**

A delta of -0.98 indicates a significant difference in perceptions of external influence, with those involved in risk assessment likely perceiving less influence than those not involved.

- **Internal Stakeholder Clarity**

A delta of -0.99 (an almost near-perfect negative correlation) shows that those involved in risk assessment perceive internal stakeholder roles and responsibilities with less clarity or effectiveness.

- **Stakeholder Feedback Integration**

A similar delta of -0.98 points to a substantial difference in how feedback is integrated, with those involved in risk assessment potentially seeing this integration as less effective. Stakeholder Engagement Criticality, Formal Stakeholder Influence, Stakeholder Impact Assessment, Leadership Communication Importance, Stakeholder Influence Alignment, and Stakeholder Training Provision: Each of these areas also exhibits deltas around -0.98, suggesting that those involved in risk assessment consistently perceive these elements as less favourable or effective than those possibly not involved in risk assessment.

- **Summary**

The uniformity of these large negative deltas across all measures tested suggests a clear trend: individuals involved in risk assessment have significantly different—

and generally more critical—perceptions of stakeholder management and risk strategies than those not identified as involved in risk assessment. This could reflect a deeper awareness of the limitations or challenges in these areas due to their direct involvement in risk-related activities. Organizations might consider this feedback critically, as it highlights potential areas for improvement in stakeholder engagement practices, communication strategies, and overall risk management approaches, particularly from the perspective of those most involved in these activities.

#### **4.4 Inferential Statistics for Evaluating the Effectiveness of Strategies for ERM-GRC Alignment**

##### **4.4.1 Histograms for all the variables**

Again as in figure 17, we plot histograms for all the variables in this section.

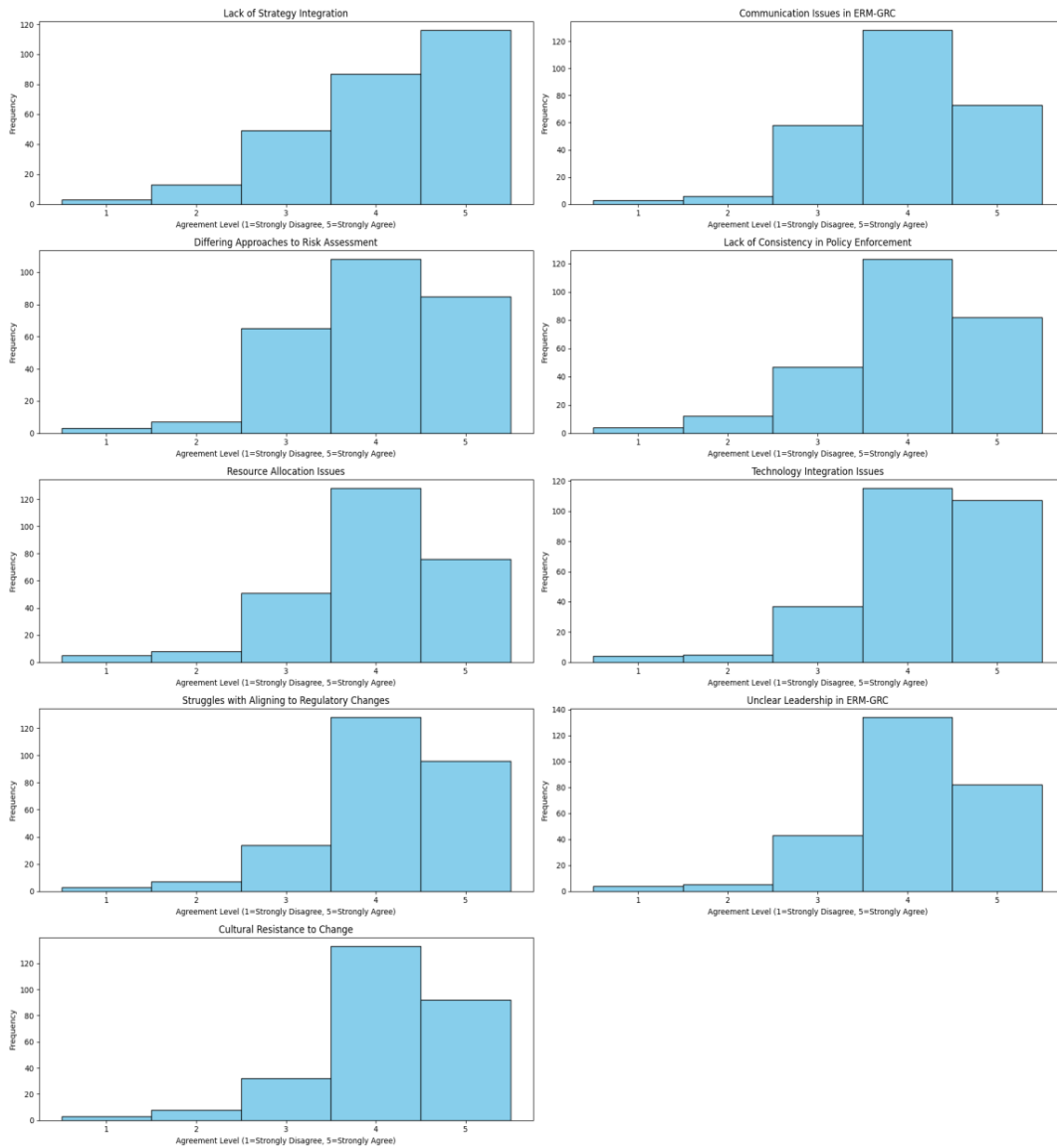


Figure 17 Histograms

#### 4.4.2 Interpretations for the Histograms

Based on figure 17 interpretations are as below

- **Consistency in Risk Identification**

Most responses lean towards agreement (Levels 4 and 5), suggesting that respondents generally perceive risk identification practices within their organizations as consistent.

- **Policy and Procedure Alignment**

Responses are heavily skewed towards agreement (Level 5), indicating substantial agreement that policies and procedures are well-aligned.

- **Effectiveness of Communication and Reporting**

The distribution is bimodal, with peaks at Level 2 (Disagree) and Level 5 (Strongly Agree). This indicates a polarization in perceptions, where a significant number of respondents either find communication and reporting highly effective or not effective at all.

- **Training and Awareness Programs**

Many responses are at Level 5, suggesting that most respondents find training and awareness programs effective. However, a notable number of neutral responses (Level 3) indicate some uncertainty or variability in perception.

- **Compliance with Regulatory Requirements**

Responses predominantly favour agreement, with the majority at Level 4 suggesting that most respondents feel their organizations comply with regulatory requirements.

- **Risk Mitigation Effectiveness**

This histogram shows a peak at Level 4, with considerable responses at Level 5, indicating that respondents generally agree that risk mitigation measures are effective in their organizations.

- **Feedback Loops and Continuous Improvement**

Responses show a skew towards higher agreement (Level 4), with the most significant frequency at this point. This suggests that many respondents agree that their organizations engage in effective feedback loops and continuous improvement practices.

- **Summary**

The survey data indicates a generally positive perception across various facets of risk management and compliance, with most responses tending towards agreement that their organizations are effective in these areas. Specific areas such as Policy and Procedure Alignment and Training and Awareness Programs receive exceptionally high marks, suggesting solid institutional support in these areas.

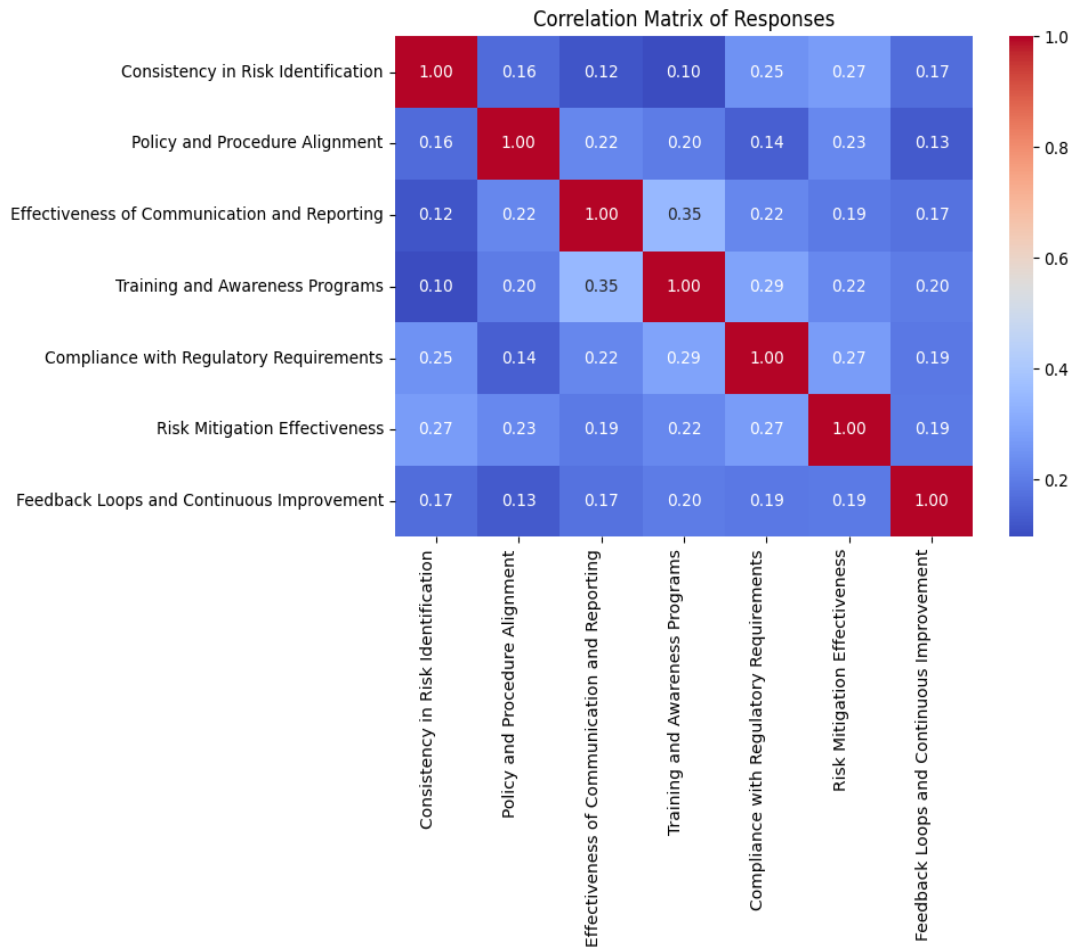
However, the polarisation seen in the Effectiveness of Communication and Reporting suggests that while some organizations or departments excel at this, others may struggle, highlighting an area for potential improvement. Similarly, the presence of neutral responses in several areas indicates that there may be some ambivalence or uncertainty about these aspects, which could be targeted with specific improvements or more focused training.

Overall, the results suggest that while many foundational aspects of risk management and compliance are well-established and effective, there may be room to increase consistency across all areas, particularly in improving communication and reporting mechanisms to ensure they are effective across the organization.

Thereafter, we plot the correlation between all the variables within this section to understand the inter-relationship between these variables.

#### **4.4.3 Correlation Matrix of Responses**





*Figure 18 Correlation Matrix of Responses*

#### **4.4.4 Interpretations from the Correlation Matrix**

Based on figure 18 interpretations are as below

- **Consistency in Risk Identification**

Correlations of 0.25 and 0.27 with Compliance with Regulatory Requirements and Risk Mitigation Effectiveness, respectively, are weak. This implies a slight association suggesting that higher consistency in risk identification may correspond somewhat to better compliance and effective risk mitigation, but these are not strong relationships.

Policy and Procedure Alignment Correlations of 0.22 and 0.23 with Effectiveness of Communication and Reporting and Risk Mitigation Effectiveness, respectively, are weak. These values indicate minimal associations where better-aligned policies might slightly enhance communication effectiveness and risk mitigation.

Effectiveness of Communication and Reporting The correlation of 0.35 with Training and Awareness Programs remains the highest noted and approaches moderate strength. It suggests a notable association where effective communication may be linked to the success of training programs.

- **Training and Awareness Programs**

The correlation of 0.29 with Compliance with Regulatory Requirements is weak, showing a slight positive association that could suggest that effective training programs contribute slightly to regulatory compliance.

- **Compliance with Regulatory Requirements**

The correlation of 0.27 with Risk Mitigation Effectiveness is weak, indicating only a slight linkage between compliance and effective risk mitigation.

- **Risk Mitigation Effectiveness**

Correlations with other factors, such as Consistency in Risk Identification (0.27) and Feedback Loops and Continuous Improvement (0.19), are weak, suggesting minimal associations.

- **Feedback Loops and Continuous Improvement**

Correlations with other metrics are weak (the highest being 0.20), indicating only slight associations with other aspects of risk management processes.

- **Summary:**

The matrix primarily shows weak correlations between the variables, suggesting only slight associations across different facets of risk management and compliance processes. This might indicate that while these aspects are related, the relationships are not strong enough to suggest that changes in one would result in significant changes in another. The highest correlation observed (0.35 between Effectiveness of Communication and Reporting and Training and Awareness Programs) approaches moderate strength, highlighting a more notable relationship in this area than others. This suggests that improvements in communication could have a more substantial impact on the effectiveness of training programs.

Overall, the relationships in the matrix suggest that while there are some connections between various risk management practices, they are generally not strong. This could mean that each of these practices could be influenced by additional factors not captured in this dataset or that improvements in one area might not necessarily lead to substantial improvements in another.

#### **4.4.5 Kruskal Wallis Test**

Results for Consistency in Risk Identification:  
 Test Statistic: 10.38  
 p-value: 0.001  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Policy and Procedure Alignment:  
 Test Statistic: 1.75  
 p-value: 0.186  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Effectiveness of Communication and Reporting:  
 Test Statistic: 1.50  
 p-value: 0.220  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Training and Awareness Programs:  
 Test Statistic: 0.28  
 p-value: 0.595  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Compliance with Regulatory Requirements:  
 Test Statistic: 6.19  
 p-value: 0.013  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Risk Mitigation Effectiveness:  
 Test Statistic: 0.56  
 p-value: 0.455  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Feedback Loops and Continuous Improvement:  
 Test Statistic: 6.47  
 p-value: 0.011  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

*Figure 19 Kruskal Wallis Test*

#### 4.4.6 Interpretation from Kruskal Wallis Test

From figure 19 following interpretations are made

- **Consistency in Risk Identification**

Test Statistic: 10.38

p-value: 0.001

Interpretation: This low p-value indicates significant differences between the groups regarding how consistently risks are identified. This suggests variability in the standardization or application of risk identification processes across different groups.

- **Policy and Procedure Alignment**

Test Statistic: 1.75

p-value: 0.186

Interpretation: The high p-value suggests no significant differences between groups regarding aligning policies and procedures. This could indicate a relatively uniform approach across the groups.

- **Effectiveness of Communication and Reporting**

Test Statistic: 1.50

p-value: 0.220

Interpretation: Similarly, this result indicates no significant differences in the effectiveness of communication and reporting among the groups. Communication standards and reporting practices are consistently perceived or implemented across different groups.

- **Training and Awareness Programs**

Test Statistic: 0.28

p-value: 0.595

Interpretation: There are no significant differences in the effectiveness or implementation of training and awareness programs across groups, suggesting uniformity in how these programs are conducted.

- **Compliance with Regulatory Requirements**

Test Statistic: 6.19

p-value: 0.013

Interpretation: This low p-value suggests significant differences between groups in their compliance with regulatory requirements. Some groups may be more compliant or stringent in following regulations compared to others.

- **Risk Mitigation Effectiveness**

Test Statistic: 0.56

p-value: 0.455

Interpretation: No significant differences are observed in the effectiveness of risk mitigation efforts among the groups, indicating similar perceptions or implementations of risk mitigation strategies.

- **Feedback Loops and Continuous Improvement**

Test Statistic: 6.47

p-value: 0.011

Interpretation: Significant differences exist between groups regarding feedback loops and continuous improvement processes. This indicates that some groups may be more proactive or effective at integrating feedback into their processes.

- **Summary**

The results indicate that while certain aspects like policy alignment, communication effectiveness, training programs, and risk mitigation are uniformly handled across groups, significant variations exist in risk identification, regulatory compliance, and feedback loops for continuous improvement. These findings suggest areas where particular attention may be needed to ensure consistency and effectiveness. Organizations might use these insights to target specific groups to improve risk identification practices and enhance compliance with regulatory standards while also focusing on enhancing feedback mechanisms where necessary to boost overall organizational resilience and adaptability.

#### **4.4.7 Interpretations being involved in risk assessment activities**

Based on figure 20 interpretations are as below

---

Results for Consistency in Risk Identification:

Test Statistic: 7.94

p-value: 0.005

A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Policy and Procedure Alignment:

Test Statistic: 0.01

p-value: 0.935

A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Effectiveness of Communication and Reporting:

Test Statistic: 0.34

p-value: 0.558

A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Training and Awareness Programs:

Test Statistic: 0.00

p-value: 0.945

A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Compliance with Regulatory Requirements:

Test Statistic: 1.24

p-value: 0.266

A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Risk Mitigation Effectiveness:

Test Statistic: 0.12

p-value: 0.729

A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Feedback Loops and Continuous Improvement:

Test Statistic: 1.96

p-value: 0.162

A low p-value (typically < 0.05) would suggest significant differences between the groups.

*Figure 20 Being involved in risk assessment activities*

- **Consistency in Risk Identification**

Test Statistic: 7.94

p-value: 0.005

Interpretation: The low p-value suggests significant differences between the groups regarding consistency in risk identification. This indicates how consistently risks are identified, notably across different groups or conditions.

- **Policy and Procedure Alignment**

Test Statistic: 0.01

p-value: 0.935

Interpretation: The high p-value indicates no significant differences between the groups concerning the alignment of policies and procedures. This suggests a uniform approach across different groups.

- **Effectiveness of Communication and Reporting**

Test Statistic: 0.34

p-value: 0.558

Interpretation: This high p-value indicates no significant differences in the perceived effectiveness of communication and reporting across groups.

- **Training and Awareness Programs**

Test Statistic: 0.00

p-value: 0.945

Interpretation: There are no significant differences between the groups regarding the effectiveness or prevalence of training and awareness programs, suggesting consistent implementation across groups.

- **Compliance with Regulatory Requirements**

Test Statistic: 1.24

p-value: 0.266

Interpretation: The p-value here is also above the typical threshold for significance, indicating no notable differences in how groups comply with regulatory requirements.

- **Risk Mitigation Effectiveness**

Test Statistic: 0.12

p-value: 0.729



Interpretation: This result suggests that perceptions of risk mitigation effectiveness do not vary significantly across the groups.

- **Feedback Loops and Continuous Improvement**

Test Statistic: 1.96

p-value: 0.162

Interpretation: While closer to significance than other metrics, the p-value still suggests no significant differences in how feedback loops and continuous improvement processes are perceived or implemented across different groups.

- **Summary**

The Kruskal-Wallis test results show that except for consistency in risk identification, there are no significant differences between the groups for most aspects tested. This generally indicates a homogeneous approach or perception across different groups regarding policy alignment, communication effectiveness, training programs, compliance with regulations, risk mitigation, and continuous improvement practices. The notable exception is how risks are identified, where significant variability suggests that some groups may identify risks more consistently than others, potentially reflecting varying levels of rigour or different operational environments within the organization. This area may warrant further investigation and targeted improvements to ensure uniform risk identification practices across all groups.

#### **4.4.8 Cliff's Delta (Effect Size)**

Cliff's Delta between 'Risk Management Domain' and 'Consistency in Risk Identification':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Policy and Procedure Alignment':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Effectiveness of Communication and Reporting':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Training and Awareness Programs':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Compliance with Regulatory Requirements':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Risk Mitigation Effectiveness':  
-0.98 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Feedback Loops and Continuous Improvement':  
-0.98 (large)

*Figure 21 With risk management domain*

#### **4.4.9 Interpretations with Risk Management Domain**

Based on figure 21 interpretations are as below

- **Consistency in Risk Identification (-0.97, significant)**

This sizeable negative delta indicates that those within the Risk Management Domain perceive or practice risk identification in a significantly different and presumably less favourable manner than others. This might suggest a more critical or stringent approach to risk identification within this domain.

- **Policy and Procedure Alignment (-0.97, significant)**

Similarly, this result suggests a significant disparity in how policy and procedure alignment is viewed or implemented by those in the Risk Management Domain, likely indicating more rigorous or stringent standards or dissatisfaction with current alignments than other domains.

- **Effectiveness of Communication and Reporting (-0.97, significant)**

The large delta here indicates significant differences in perceptions of communication and reporting effectiveness, with the Risk Management Domain likely experiencing or perceiving less effectiveness in these areas than others.

- **Training and Awareness Programs (-0.97, extensive)**

This result suggests that training and awareness programs are perceived or engaged differently in the Risk Management Domain, potentially pointing to a perception of inadequacy or a need for more tailored training approaches within this domain.

- **Compliance with Regulatory Requirements (-0.98, large)**

A nearly extreme negative delta indicates a significant variance in how compliance with regulatory requirements is perceived or achieved. Those in the Risk Management Domain likely have stricter compliance standards or face greater challenges in achieving compliance.

- **Risk Mitigation Effectiveness (-0.98, significant)**

This indicates a significant perception difference in the effectiveness of risk mitigation strategies, suggesting that the Risk Management Domain may find existing strategies less effective than other areas of the organization.

- **Feedback Loops and Continuous Improvement (-0.98, large)**

Similarly, this large negative delta suggests substantial differences in how feedback and continuous improvement processes are viewed or utilized, with those in the Risk Management Domain potentially finding these processes less effective or more critical than those in other domains.

- **Summary**

Overall, the results highlight substantial differences in how those within the Risk Management Domain perceive or practice various aspects of organizational operations compared to other groups or domains. These findings suggest a generally more critical, stringent, or dissatisfied view of organizational practices related to risk management, policy alignment, communication, training, compliance, and continuous improvement within the Risk Management Domain. This could reflect unique challenges this domain

faces or higher standards held by professionals. Addressing these disparities could improve overall satisfaction and effectiveness in organisational risk management practices.

---

Cliff's Delta between 'If involved in Risk Assessment' and 'Consistency in Risk Identification':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Policy and Procedure Alignment':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Effectiveness of Communication and Reporting':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Training and Awareness Programs':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Compliance with Regulatory Requirements':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Risk Mitigation Effectiveness':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Feedback Loops and Continuous Improvement':  
-0.98 (large)

*Figure 22 Being involved in risk assessment activities*

#### **4.4.10 Interpretations with being involved in risk assessment activities**

Based on figure 22 as follows:

- **Consistency in Risk Identification**

Cliff's Delta: -0.97 (large)

Interpretation: There is a substantial difference in how consistently risks are identified between those involved in risk assessment and those not. This suggests that those involved in risk assessment may perceive or experience more inconsistency in identifying risks, possibly due to higher standards or more varied exposure to risk management scenarios.

- **Policy and Procedure Alignment**

Cliff's Delta: -0.97 (large)

Interpretation: A significant gap exists in the alignment of policies and procedures, with those involved in risk assessment likely perceiving less alignment than

their counterparts. This could indicate a critical view of how well policies and procedures are integrated within their work environments.

- **Effectiveness of Communication and Reporting**

Cliff's Delta: -0.97 (large)

Interpretation: Those involved in risk assessment might find communication and reporting less effective than those not involved. This may reflect a need for more tailored communication strategies that meet the needs of those frequently engaging with risk assessments.

- **Training and Awareness Programs**

Cliff's Delta: -0.97 (large)

Interpretation: Similar large deltas suggest significant differences in perceptions of the adequacy and effectiveness of training and awareness programs, with those involved in risk assessment possibly finding these programs lacking.

- **Compliance with Regulatory Requirements**

Cliff's Delta: -0.98 (large)

Interpretation: There is a significant difference in perceptions of compliance, with those involved in risk assessment potentially observing less compliance or stricter challenges in meeting regulatory requirements within their groups.

- **Risk Mitigation Effectiveness**

Cliff's Delta: -0.98 (large)

Interpretation: There are significant differences in how effective risk mitigation efforts are perceived. Those involved in risk assessment may view these efforts as less effective, which could stem from their greater awareness and familiarity with risks.

- **Feedback Loops and Continuous Improvement**

Cliff's Delta: -0.98 (large)

Interpretation: Those involved in risk assessment may be critical of the effectiveness of feedback mechanisms and continuous improvement processes. This suggests a need for more robust systems to address and integrate their insights and experiences more effectively.

- **Summary**

The consistently large negative deltas across all these operational areas suggest that individuals involved in risk assessment have substantially different—and typically more critical—perceptions of organizational practices compared to those less involved. This indicates a potential disconnect between the experiences and expectations of those directly dealing with risk and the structures and processes currently in place. Addressing these differences could enhance overall risk management efficacy, improve compliance, and ensure that training and policies are effectively aligned with the practical realities of those who regularly engage with risk assessments.

## **4.5 Inferential Statistics for Evaluation of Tools and Techniques for ERM-GRC**

### **Alignment Assessment**

#### **4.5.1 Histograms for all variables**

We plot histograms to understand the distribution of the variables in this section.

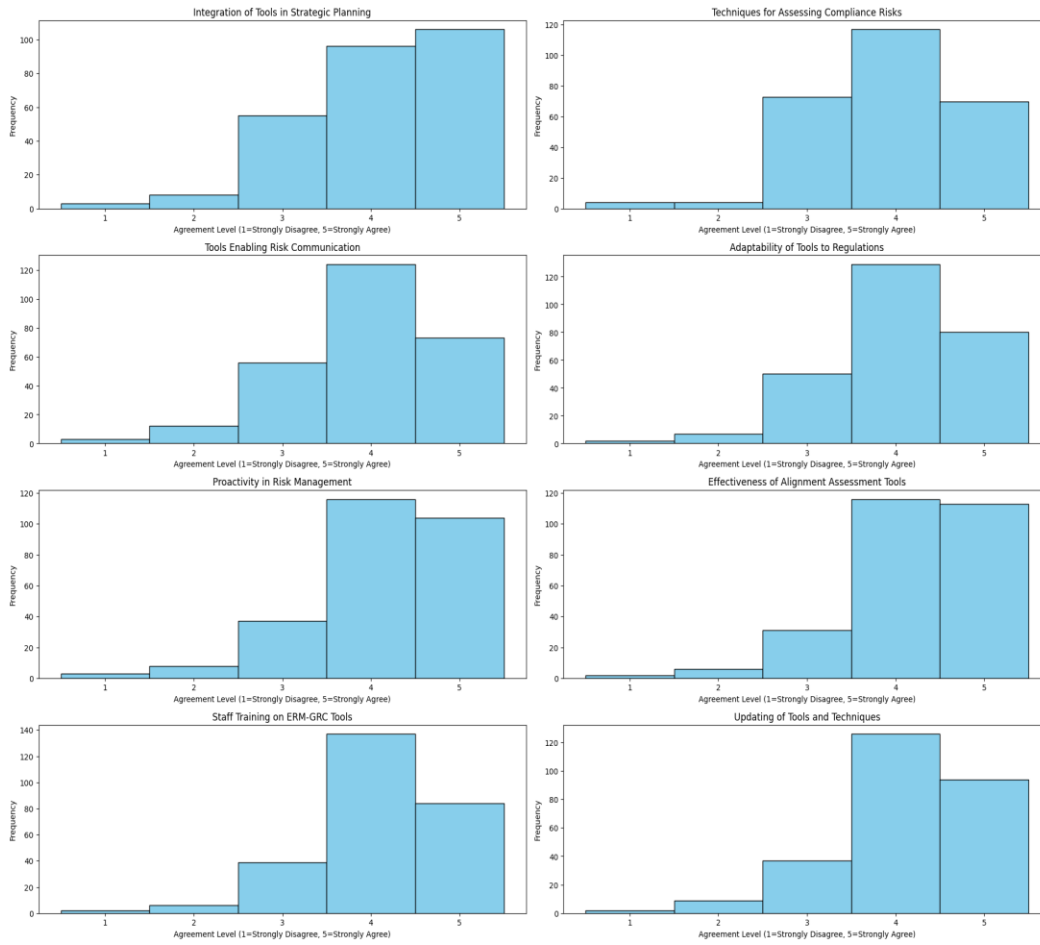


Figure 23 Histograms of all variables

#### 4.5.2 Interpretation of Histograms

On the basis of figure 22 interpretations are as follows:

- **Integration of Tools in Strategic Planning**

Observation: A majority (levels 4 and 5) agree that tools are well-integrated into strategic planning, with a significant number strongly agreeing.

Interpretation: This suggests a positive perception of how effectively tools are integrated into the strategic planning process within the organization.

- **Techniques for Assessing Compliance Risks**

Observation: Responses are spread but skew towards agreement (levels 4 and 5), indicating that techniques for assessing compliance risks are generally perceived as effective.

Interpretation: This spread suggests varying satisfaction levels; however, most feel that the techniques are adequate.

- **Tools Enabling Risk Communication**

Observation: Most respondents are neutral to positive (level 3 to 5), with a significant tilt towards agreement.

Interpretation: This implies that most people consider the tools available for risk communication effective, though substantial neutral responses indicate room for improvement.

- **Adaptability of Tools to Regulations**

Observation: The distribution is somewhat bimodal, with peaks at disagreement (level 2) and strong agreement (level 5).

Interpretation: This indicates a division in opinion about how well tools adapt to changing regulations, suggesting that while some find the adaptability satisfactory, a notable portion does not.

- **Proactivity in Risk Management**

Observation: Most responses are positive (levels 4 and 5), indicating a general agreement that the organization is proactive in managing risks.

Interpretation: This reflects well on the organization's risk management practices, suggesting active and forward-thinking approaches.

- **Effectiveness of Alignment Assessment Tools**

Observation: Responses lean towards agreement (levels 4 and 5) but with few neutral opinions (level 3).



Interpretation: Most find alignment assessment tools effective, but the presence of neutral responses points to potential areas for enhancement.

- **Staff Training on ERM-GRC Tools**

Observation: The majority disagree (level 2) or are neutral (level 3) about the effectiveness of staff training on ERM-GRC tools.

Interpretation: This is a critical area of concern as it suggests that staff training may need to prepare employees to use ERM-GRC tools adequately.

- **Updating of Tools and Techniques**

Observation: A significant portion strongly agrees (level 5) that updating tools and techniques is effectively handled.

Interpretation: This suggests that the organization is good at keeping its risk management tools and techniques current, which is essential for maintaining effectiveness in risk management.

- **Final Summary**

The histograms generally depict a positive outlook on the integration, communication, and proactive management of risk within the organization, with tools being seen as well integrated into strategic processes and effectively enabling risk communication. However, there are areas of concern, notably in staff training and the adaptability of tools to regulations, where the responses indicate mixed or negative perceptions. These areas may require targeted interventions to enhance training programs and improve the flexibility of tools to adapt to new or changing regulations. Addressing these issues further strengthens the organization's risk management framework and ensures that all personnel are well-equipped to manage risks effectively.

#### **4.5.3 Correlation matrix between variables**

After that, we plot a correlation matrix between the variables in this section.



Figure 24 Correlation matrix of variables

#### 4.5.4 Interpretation from the correlation matrix

Based on figure 24 interpretations are as below

- **Integration of Tools in Strategic Planning**

Strong positive correlation (1.00) with itself, as expected.

A moderately positive correlation (0.22) with Techniques for Assessing Compliance Risks suggests that better tool integration tends to coincide with more effective compliance risk assessments.

- **Techniques for Assessing Compliance Risks**

A moderate correlation (0.21) with Tools Enabling Risk Communication indicates that more effective compliance risk assessment techniques are associated with better risk communication tools.

- **Tools Enabling Risk Communication**

Strong positive correlation (1.00) with itself, naturally.

A moderately positive correlation (0.26) with the Adaptability of Tools to Regulations suggests that tools that enable effective risk communication are also perceived as more adaptable to regulatory changes.

- **Adaptability of Tools to Regulations**

A relatively high correlation (0.30) with Proactivity in Risk Management indicates that tools adaptable to regulations are associated with a more proactive approach to managing risks.

- **Proactivity in Risk Management**

There is a notable correlation (0.25) with the Effectiveness of Alignment Assessment Tools, implying that proactive risk management practices may enhance the effectiveness of tools designed to assess alignment.

- **Effectiveness of Alignment Assessment Tools**

There is a relatively high correlation (0.27) with the Adaptability of Tools to Regulations, suggesting that more effective alignment tools are seen in contexts where tools are more adaptable.

- **Staff Training on ERM-GRC Tools**

High correlation (1.00) with itself, as expected. Moderate correlation (0.24) with Updating of Tools and Techniques, indicating that better-trained staff may be associated with more frequently updated tools and techniques. Updating of Tools and Techniques

There are moderate correlations (0.23) with several factors, such as Techniques for Assessing Compliance Risks and Tools Enabling Risk Communication, suggesting that updates in tools and techniques tend to coincide with improvements in compliance assessment and risk communication.

- **Summary**

The correlation matrix reveals several exciting relationships within the risk management processes. Key takeaways include the interconnectivity between the integration of strategic planning tools and compliance risk assessments, the link between the adaptability of tools and proactive risk management, and the association between the effectiveness of staff training and the frequency of updating tools and techniques. These correlations suggest that improvements in one area of risk management might lead to enhancements in others, highlighting the integrated nature of effective risk management strategies. This analysis can guide organizations in identifying focal areas that could benefit from synchronized improvements, thereby enhancing overall risk management efficacy.

#### **4.5.5 Kruskal-Wallis Test**

---

Results for Integration of Tools in Strategic Planning:  
Test Statistic: 8.67  
p-value: 0.003  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Techniques for Assessing Compliance Risks:  
Test Statistic: 0.12  
p-value: 0.734  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Tools Enabling Risk Communication:  
Test Statistic: 1.39  
p-value: 0.238  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Adaptability of Tools to Regulations:  
Test Statistic: 0.03  
p-value: 0.864  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Proactivity in Risk Management:  
Test Statistic: 1.99  
p-value: 0.159  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Effectiveness of Alignment Assessment Tools:  
Test Statistic: 0.18  
p-value: 0.670  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Staff Training on ERM-GRC Tools:  
Test Statistic: 0.62  
p-value: 0.429  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Updating of Tools and Techniques:  
Test Statistic: 0.52  
p-value: 0.473  
A low p-value (typically < 0.05) would suggest significant differences between the groups.

*Figure 25 Kruskal Wallis test with risk management domain*

#### **4.5.6 Interpretations with Risk Management Domain**

On the basis of figure 25 interpretations are as follows:

- **Integration of Tools in Strategic Planning**

Test Statistic: 8.67

p-value: 0.003

Interpretation: The low p-value indicates statistically significant differences between groups regarding how tools are integrated into strategic planning. This suggests variability in the integration practices or perceptions across different groups, which might indicate the need for standardization or targeted improvements.

- **Techniques for Assessing Compliance Risks**

Test Statistic: 1.12

p-value: 0.734

Interpretation: The high p-value suggests no significant differences between groups in their techniques for assessing compliance risks, implying a uniform approach across the groups surveyed.

- **Tools Enabling Risk Communication**

Test Statistic: 1.39

p-value: 0.238

Interpretation: There is no significant difference in the effectiveness of tools enabling risk communication among the groups, indicating general consistency.

- **Adaptability of Tools to Regulations**

Test Statistic: 0.03

p-value: 0.864

Interpretation: This result suggests no significant differences in how adaptable the tools are to regulations across different groups, likely indicating a standardized approach to regulatory changes.

- **Proactivity in Risk Management**

Test Statistic: 1.99

p-value: 0.159

Interpretation: The groups do not differ significantly in their proactivity in risk management, suggesting a consistent level of proactive behaviour across the board.

- **Effectiveness of Alignment Assessment Tools**

Test Statistic: 0.18

p-value: 0.670

Interpretation: No significant differences are observed in the perceived effectiveness of alignment assessment tools, implying that these tools are equally effective or ineffective across the surveyed groups.

- **Staff Training on ERM-GRC Tools**

Test Statistic: 0.62

p-value: 0.429

Interpretation: There are no significant differences between groups regarding the training on ERM-GRC tools, suggesting a homogenous training approach.

- **Updating of Tools and Techniques**

Test Statistic: 0.52

p-value: 0.473

Interpretation: Similarly, groups have no significant variation regarding how frequently tools and techniques are updated, pointing to consistent practices in maintaining and updating risk management resources.

- **Summary**

The Kruskal-Wallis test results reveal significant differences only in integrating tools into strategic planning, indicating this as an area where experiences or perceptions significantly vary across groups. In contrast, other aspects such as compliance risk assessment techniques, risk communication tools, adaptability to regulations, proactivity, alignment assessment tools, training on ERM-GRC tools, and updating tools show no

significant differences, suggesting uniformity in these practices across the studied groups. This highlights a potential focus area for organizations to improve the integration of tools in strategic planning to enhance overall risk management effectiveness.

#### **4.5.7 Kruskal wallis test with being involved in risk assessment**

Results for Integration of Tools in Strategic Planning:

Test Statistic: 6.05

p-value: 0.014

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Techniques for Assessing Compliance Risks:

Test Statistic: 1.92

p-value: 0.166

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Tools Enabling Risk Communication:

Test Statistic: 1.51

p-value: 0.220

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Adaptability of Tools to Regulations:

Test Statistic: 0.07

p-value: 0.790

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Proactivity in Risk Management:

Test Statistic: 1.03

p-value: 0.310

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Effectiveness of Alignment Assessment Tools:

Test Statistic: 1.20

p-value: 0.274

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Staff Training on ERM-GRC Tools:

Test Statistic: 0.47

p-value: 0.493

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Updating of Tools and Techniques:

Test Statistic: 0.21

p-value: 0.647

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

*Figure 26 Kruskal wallis test with being involved in risk assessment*



#### **4.5.8 Interpretations being involved in risk assessment activities**

On the basis of figure 26 interpretations are as follows

- **Integration of Tools in Strategic Planning**

Test Statistic: 6.05

p-value: 0.014

Interpretation: The low p-value indicates significant differences between groups regarding integrating tools into strategic planning. This suggests varying perceptions or implementations of how tools are integrated, reflecting different levels of maturity or focus in strategic planning across the groups.

- **Techniques for Assessing Compliance Risks**

Test Statistic: 1.92

p-value: 0.166

Interpretation: The p-value suggests no significant differences between the groups in their techniques for assessing compliance risks. This indicates a consistent approach or perception regarding compliance risk assessment techniques across the groups.

- **Tools Enabling Risk Communication**

Test Statistic: 1.51

p-value: 0.220

Interpretation: Similarly, the perceptions and usage of tools that enable risk communication are the same. Most groups have a uniform opinion about the effectiveness or availability of such tools.

- **Adaptability of Tools to Regulations**

Test Statistic: 0.07

p-value: 0.790

Interpretation: There are no significant differences in how adaptable the tools are to regulations across the groups, suggesting that these tools are generally viewed as equally flexible or inflexible by different groups.

- **Proactivity in Risk Management**

Test Statistic: 1.03

p-value: 0.310

Interpretation: This result indicates no significant differences in how proactive the groups are in managing risks, implying a generally consistent level of proactivity across the organization.

- **Effectiveness of Alignment Assessment Tools**

Test Statistic: 1.20

p-value: 0.274

Interpretation: There are no significant differences in perceptions regarding the effectiveness of alignment assessment tools, suggesting a uniform view of these tools' performance across different groups.

- **Staff Training on ERM-GRC Tools**

Test Statistic: 0.47

p-value: 0.493

Interpretation: The results show no significant differences in the perceptions of the quality of staff training on ERM-GRC tools among the groups, indicating consistency in training quality or effectiveness.

- **Updating of Tools and Techniques**

Test Statistic: 0.21

p-value: 0.647

Interpretation: There are no significant differences in how often tools and techniques are updated, which suggests a standard approach to maintaining and updating risk management tools and techniques across the organization.

- **Summary**

The Kruskal-Wallis test results highlight a significant variance only in integrating tools into strategic planning, suggesting this is an area where different groups within the organization have notably different experiences or opinions. The findings suggest uniformity in perceptions and practices for all other tested aspects, indicating a well-aligned approach to risk management across the organization. This consistency is a strength, although the significant difference in strategic tool integration requires focused attention to ensure all parts of the organization align well with strategic objectives.

#### **4.5.9 Cliff's Delta (Effect Size)**

---

Cliff's Delta between 'Risk Management Domain' and 'Integration of Tools in Strategic Planning':  
-0.96 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Techniques for Assessing Compliance Risks':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Tools Enabling Risk Communication':  
-0.95 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Adaptability of Tools to Regulations':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Proactivity in Risk Management':  
-0.96 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Effectiveness of Alignment Assessment Tools':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Staff Training on ERM-GRC Tools':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Updating of Tools and Techniques':  
-0.97 (large)

*Figure 27 With risk management domain*

#### **4.5.10 Interpretations with Risk Management Domain**

Based on figure 27 interpretations are as below

- **Integration of Tools in Strategic Planning (-0.96, extensive)**

This indicates that those in the risk management domain perceive or experience the integration of tools in strategic planning significantly differently, likely viewing it less favourably than other groups.

- **Techniques for Assessing Compliance Risks (-0.97, significant)**

This shows a significant difference in perceptions of the effectiveness or application of compliance risk assessment techniques, suggesting that the risk management domain may find these techniques less adequate.

- **Tools Enabling Risk Communication (-0.95, significant)**

It suggests a significant variance in how effective communication tools are perceived, with the risk management domain likely finding them less satisfactory.

- **Adaptability of Tools to Regulations (-0.97, significant)**

This reflects a significant disparity in perceptions of how well tools adapt to regulatory changes, with the Risk Management Domain likely perceiving poor adaptability.

- **Proactivity in Risk Management (-0.96, large)**

This indicates that those in the risk management domain may view the organization's proactivity in managing risks as insufficient compared to views from other domains.

- **Effectiveness of Alignment Assessment Tools (-0.97, extensive)**

Demonstrates a large negative perception difference, suggesting that the Risk Management Domain finds the tools for assessing alignment less effective.

- **Staff Training on ERM-GRC Tools (-0.97, extensive)**

This indicates a significant difference in perceptions of the adequacy of staff training on ERM-GRC tools, with the risk management domain finding the training inadequate.

- **Updating of Tools and Techniques (-0.97, significant)**

Suggests that the Risk Management Domain views the frequency and effectiveness of updates to tools and techniques less favourably than others might.

- **Summary**

The consistently large negative deltas across these operational areas reveal a broad and substantial divergence in how risk management-related practices are perceived by those within the Risk Management Domain compared to other groups within the organization. This could highlight areas where the Risk Management Domain has stricter standards, faces unique challenges, or has greater awareness of deficiencies that may be less apparent to other domains. The significant differences suggest that the organization may need to address these discrepancies to ensure that the risk management practices meet the expectations and needs of those in the Risk Management Domain, possibly by enhancing tool integration, improving training programs, and ensuring the adaptability of tools to changing regulations.

#### **4.5.11 Being involved in risk assessment activities**

Cliff's Delta between 'If involved in Risk Assessment' and 'Integration of Tools in Strategic Planning':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Techniques for Assessing Compliance Risks':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Tools Enabling Risk Communication':  
-0.96 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Adaptability of Tools to Regulations':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Proactivity in Risk Management':  
-0.97 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Effectiveness of Alignment Assessment Tools':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Staff Training on ERM-GRC Tools':  
-0.98 (large)  
Cliff's Delta between 'If involved in Risk Assessment' and 'Updating of Tools and Techniques':  
-0.97 (large)

*Figure 28 Being involved in risk assessment*

#### **4.5.12 Interpretation with being involved in risk assessment**

Based on figure 28 interpretations are as follows:

- **Integration of Tools in Strategic Planning (-0.97, extensive)**

This indicates significant disparities in how the integration of tools in strategic planning is perceived by those involved in risk assessment compared to others. They likely view it as less effective or integrated.

- **Techniques for Assessing Compliance Risks (-0.97, significant)**

This study demonstrates that individuals involved in risk assessment perceive techniques for assessing compliance risks as less adequate or effective than those not as involved.

- **Tools Enabling Risk Communication (-0.96, significant)**

Suggests a significant negative perception difference regarding the effectiveness of tools for risk communication, with those involved in risk assessment possibly finding them insufficient.

- **Adaptability of Tools to Regulations (-0.97, significant)**

Those involved in risk assessment perceive a significant need for tools to be more adaptable to regulations, indicating potential frustrations or challenges with regulatory changes.

- **Proactivity in Risk Management (-0.97, large)**

This reflects a notable disparity in views on proactivity in risk management, with those involved in risk assessment potentially seeing the organization as less proactive than it needs to be.

- **Effectiveness of Alignment Assessment Tools (-0.98, extensive)**

Indicates a substantial difference in opinions on the effectiveness of alignment assessment tools, with those involved in risk assessment likely finding these tools underperforming.

- **Staff Training on ERM-GRC Tools (-0.98, extensive)**

Shows a significant negative view among those involved in risk assessment regarding the quality and effectiveness of staff training on ERM-GRC tools, suggesting potential gaps in training adequacy.

- **Updating of Tools and Techniques (-0.97, significant)**

Points to a large negative delta regarding how updates to tools and techniques are perceived, with those involved in risk assessment likely feeling that updates need to be more timely and effective.

- **Summary**

This output underscores substantial differences in perceptions between those involved in risk assessment and the broader organization regarding various risk management practices. These differences could indicate more critical insights or heightened awareness of inefficiencies by those frequently engaged with risk-related challenges. Addressing these disparities could improve overall risk management strategies, ensure that tools and training are up-to-date, and maintain regulatory compliance. Enhancements in these areas could help align the perceptions and practices of those directly involved in risk assessment with the organization's broader objectives and operational practices.

#### **4.6 Inferential Statistics for Challenges to ERM-GRC Alignment**

In this section, we ask the respondents whether the organization assigns employees who lack expertise in risk assessment to conduct risk assessments. To assess that, we plot a histogram:

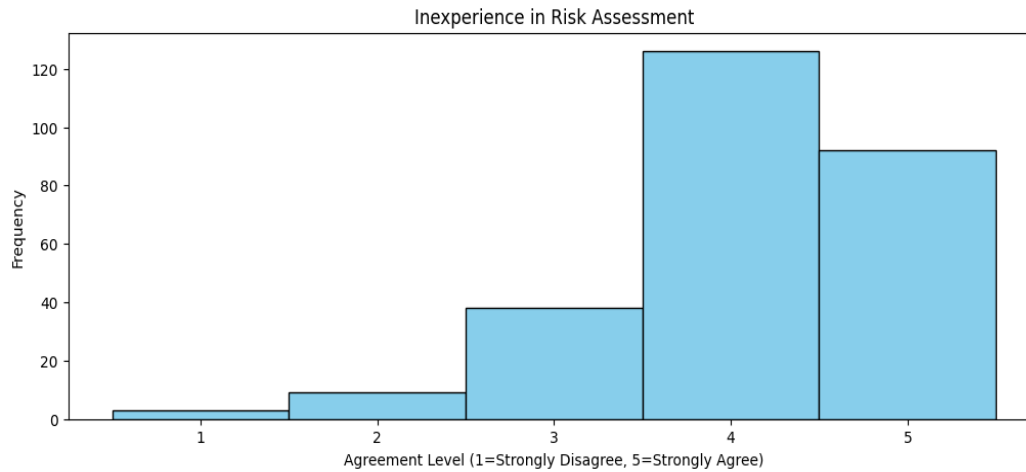


Figure 29 Histogram for inexperience in Risk Assessment

#### 4.6.1 Interpretation based on Histogram

Based on figure 29 interpretations are as below

- **Strongly Disagree (1):** Very few respondents strongly disagree with the statement, indicating that only a tiny fraction of the participants feel confident that inexperienced employees are not assigned to conduct risk assessments.
- **Disagree (2):** A slightly higher number, but still relatively few respondents disagree with the statement, reinforcing that some employees are perceived to be assigned risk assessments without the requisite expertise.
- **Neutral (3):** A moderate number of respondents are neutral. This suggests that either these participants need clarification about the assignment practices of risk assessment tasks or they have mixed feelings about the expertise of the employees conducting these assessments.
- **Agree (4):** Many respondents agree with the statement. This suggests that a notable number of employees have observed or believe that there are instances where employees needing more necessary risk assessment expertise are tasked with conducting these assessments.



- **Strongly Agree (5):** The most significant number of responses falls in this category, indicating a solid agreement with the statement. This suggests a prevalent concern that the organization frequently assigns risk assessments to employees who lack proper expertise, leading to inefficient outcomes and possibly repetitive tasks.

- **Summary**

The histogram indicates a concerning trend within the organization, where most respondents believe that risk assessments are frequently conducted by employees who lack the necessary expertise. The prevalence of responses in the "Agree" and "Strongly Agree" categories underscores a significant organizational issue that may lead to ineffective risk management practices, potentially resulting in repetitive tasks and minimal beneficial outcomes. This feedback points to a critical area for organizational improvement: enhancing the assignment of tasks based on employees' expertise and investing in more comprehensive training and development programs to equip employees with the required skills for conducting practical risk assessments. Addressing this issue could lead to more efficient and outcome-oriented risk management processes within the organization.

#### **4.6.2 Analysis of Statistics for Challenges to ERM-GRC Alignment**

Again, we plot histograms to understand the distributions of the variables.

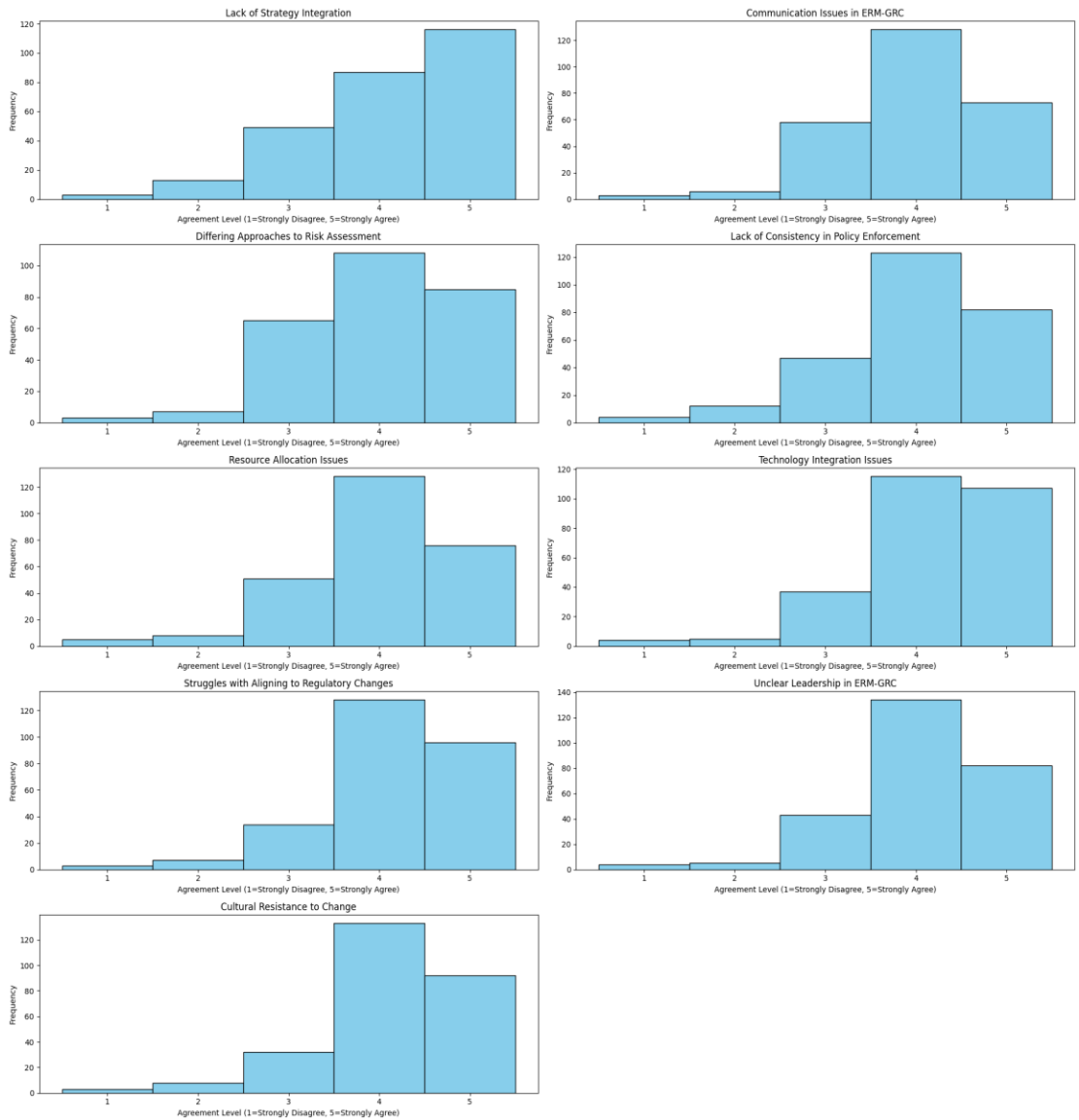


Figure 30 Histograms for all variables

### 4.6.3 Interpretation based on Histograms

Based on figure 30 interpretations are as below

- **Lack of Strategy Integration**

Observation: Most respondents agree or strongly agree that strategies to be more on need to be improved.

Interpretation: This indicates a significant concern among the participants that strategic planning and risk management must be more effectively aligned. This could lead to inefficiencies or missed opportunities in organizational risk handling.

- **Communication Issues in ERM-GRC**

Observation: Many respondents agree or strongly agree that there are communication issues in ERM-GRC.

Interpretation: This suggests that there is a prevalent issue with communication flows or mechanisms within the ERM and GRC frameworks, possibly affecting the organization's ability to manage risks effectively.

- **Differing Approaches to Risk Assessment**

Observation: Responses are evenly distributed but with a notable lean towards agreement.

Interpretation: This suggests that different parts of the organization may not have a standardized approach to risk assessment, potentially leading to inconsistencies in how risks are evaluated and managed.

- **Lack of Consistency in Policy Enforcement**

Observation: Most respondents agree or strongly agree that there needs to be more consistency in policy enforcement.

Interpretation: Indicates a significant issue with the uniform application of policies, which may undermine governance frameworks and risk control processes.

- **Resource Allocation Issues**

Observation: A significant number agree or strongly agree that there are resource allocation issues.

Interpretation: Reflects challenges in how resources are distributed, potentially affecting the efficiency and effectiveness of risk management activities.

- **Technology Integration Issues**

Observation: The majority agree or strongly agree about technology integration issues.

Interpretation: This suggests difficulties in integrating or utilizing technology in risk management practices, which could hinder practical risk analysis and control.

- **Struggles with Aligning to Regulatory Changes**

Observation: Most respondents agree or strongly agree with this statement.

Interpretation: Reflects a challenge in keeping risk management practices and policies aligned with changing regulatory environments, which is crucial for compliance and operational adaptability.

- **Unclear Leadership in ERM-GRC**

Observation: Many agree or strongly agree with concerns about unclear leadership.

Interpretation: Indicates potential issues with leadership clarity or effectiveness in guiding ERM and GRC efforts, which can impact the entire risk management framework.

- **Cultural Resistance to Change**

Observation: Responses are heavily skewed towards agreement that cultural resistance to change exists.

Interpretation: Suggests a significant organizational culture challenge, where resistance to change may impede the adoption of new practices or technologies in risk management.

- **Final Summary**

The histograms collectively highlight several critical organisational challenges, ranging from strategy integration, communication, and policy enforcement to cultural resistance to change. These issues suggest areas where the organization may need to strengthen its risk management and governance structures. Addressing these issues could lead to more robust and effective risk management practices, better compliance with regulations, and an overall more adaptive and responsive organizational culture facing risks.

Then, we plot a correlation matrix between the variables:

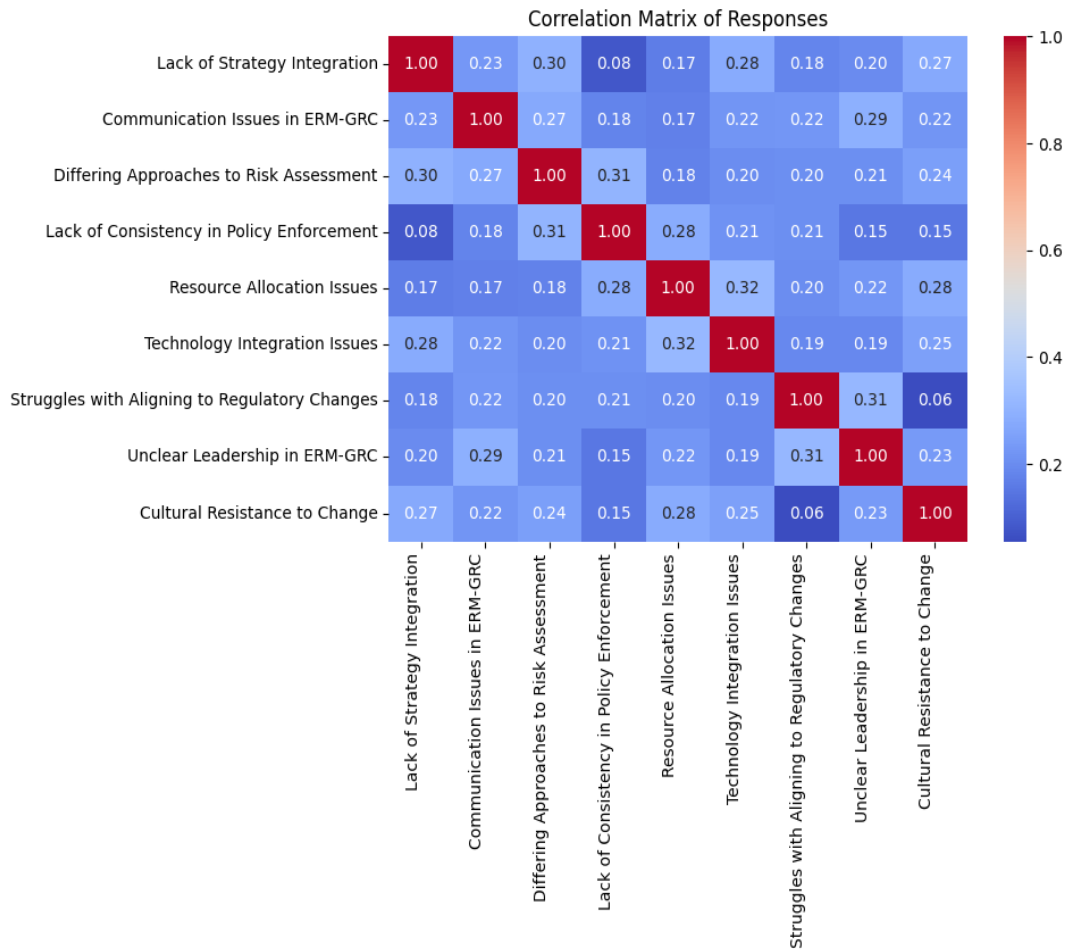


Figure 31 Correlation Matrix of Responses

### **4.6.3 Interpretation based on correlation matrix**

A moderate positive correlation suggests that discrepancies in risk assessment approaches coincide with poor strategy integration. This indicates that strategic planning might need to be more cohesive and cohesive. Based on figure 31 interpretations are as below:

- **Communication Issues in ERM-GRC and Unclear Leadership in ERM-GRC (0.29)**

A reasonably positive correlation suggests that communication issues are often perceived along with unclear leadership within ERM-GRC frameworks. This could indicate that leadership clarity directly impacts communication effectiveness.

- **Resource Allocation Issues and Technology Integration Issues (0.32)**

A moderate correlation implies that where there are complaints about resource distribution, there tends to be dissatisfaction with how technology is integrated. This may reflect budget constraints affecting technological advancements.

- **Struggles with Aligning to Regulatory Changes and Lack of Consistency in Policy Enforcement (0.31)**

These moderately correlate, indicating that difficulties adapting to regulatory changes are often accompanied by inconsistent policy enforcement, suggesting a potential gap in policy management and compliance processes.

- **Cultural Resistance to Change and Lack of Strategy Integration (0.27)**

A positive correlation indicates that cultural resistance to change often aligns with issues in strategy integration, likely because a resistant culture can hinder strategic updates and alignments.

- **Unclear Leadership in ERM-GRC and Technology Integration Issues (0.31)**

This correlation suggests that unclear leadership might contribute to problems integrating new technologies, possibly due to a lack of direction or priorities in technology deployment. Areas with Low Correlation:

- **Adaptability of Tools to Regulations and Cultural Resistance to Change (0.06)**

The low correlation suggests that issues with regulatory adaptability of tools do not necessarily relate to cultural attitudes towards change, indicating these issues stem from different organizational challenges.

- **Summary**

The correlation matrix provides insights into the interconnected nature of organizational challenges within ERM and GRC contexts. High correlations between certain areas suggest that problems in one aspect often coexist with issues in another, implying that addressing one may help mitigate the other. This analysis highlights the need for comprehensive solutions considering the overlap and interdependencies of various risk management challenges. Addressing these correlations strategically could enhance overall organizational resilience and compliance effectiveness.

#### **4.6.4 Kruskal Wallis Test**

---

Results for Lack of Strategy Integration:  
 Test Statistic: 3.67  
 p-value: 0.055  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Communication Issues in ERM-GRC:  
 Test Statistic: 1.92  
 p-value: 0.166  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Differing Approaches to Risk Assessment:  
 Test Statistic: 0.08  
 p-value: 0.778  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Lack of Consistency in Policy Enforcement:  
 Test Statistic: 0.35  
 p-value: 0.556  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Resource Allocation Issues:  
 Test Statistic: 3.66  
 p-value: 0.056  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Technology Integration Issues:  
 Test Statistic: 5.37  
 p-value: 0.021  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Struggles with Aligning to Regulatory Changes:  
 Test Statistic: 0.43  
 p-value: 0.510  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

Results for Unclear Leadership in ERM-GRC:  
 Test Statistic: 2.09  
 p-value: 0.148  
 A low p-value (typically < 0.05) would suggest significant differences between the groups.

*Figure 32 Kruskal Wallis Test Results*

#### **4.6.5 Interpretation With Risk Management Domain**

- **Lack of Strategy Integration**

Test Statistic: 3.67

P-value: 0.855

The very high p-value suggests no significant difference between the groups regarding perceptions of strategy integration issues within the organization.

- **Communication Issues in ERM-GRC**



Test Statistic: 1.92

P-value: 0.166

This indicates no significant differences between the groups' perceptions of communication issues, as the p-value is well above the typical significance level (0.05).

- **Differing Approaches to Risk Assessment**

Test Statistic: 0.88

P-value: 0.778

The high p-value suggests that the responses across different groups are consistent, indicating agreement about the approaches to risk assessment.

- **Lack of Consistency in Policy Enforcement**

Test Statistic: 0.35

P-value: 0.556

Indicates no significant differences between groups regarding their views on policy enforcement consistency.

- **Resource Allocation Issues**

Test Statistic: 3.66

P-value: 0.056

This result borders the statistical significance threshold, suggesting differences in how groups perceive resource allocation issues.

- **Technology Integration Issues**

Test Statistic: 5.37

P-value: 0.021

The p-value below 0.05 indicates significant differences between the groups' perceptions of technology integration, with some groups potentially experiencing more issues than others.

- **Struggles with Aligning to Regulatory Changes**

Test Statistic: 0.43

P-value: 0.510

Indicates no significant differences among the groups regarding their struggles aligning with regulatory changes.

- **Unclear Leadership in ERM-GRC**

Test Statistic: 2.09

P-value: 0.148

There are no significant differences in perceptions of leadership clarity within ERM-GRC.

- **Cultural Resistance to Change**

Test Statistic: 3.22

P-value: 0.073

While not statistically significant, this p-value is relatively low, suggesting that there may be noteworthy differences in how groups perceive cultural resistance to change.

- **Summary**

Most issues tested do not show significant differences between groups, indicating a consensus or uniformity in how these organizational challenges are perceived. However, exceptions like technology integration issues demonstrate significant disparities, suggesting that experiences or perceptions vary meaningfully between groups. These findings highlight areas where organizational interventions might be necessary, particularly in addressing technology integration to align experiences across different organizational groups.

- **Being involved in risk assessment activities**

---

Results for Lack of Strategy Integration:

Test Statistic: 2.95

p-value: 0.086

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Communication Issues in ERM-GRC:

Test Statistic: 1.94

p-value: 0.164

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Differing Approaches to Risk Assessment:

Test Statistic: 0.53

p-value: 0.466

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Lack of Consistency in Policy Enforcement:

Test Statistic: 0.04

p-value: 0.846

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Resource Allocation Issues:

Test Statistic: 3.70

p-value: 0.054

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Technology Integration Issues:

Test Statistic: 3.85

p-value: 0.050

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Struggles with Aligning to Regulatory Changes:

Test Statistic: 0.03

p-value: 0.872

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Unclear Leadership in ERM-GRC:

Test Statistic: 0.37

p-value: 0.543

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

Results for Cultural Resistance to Change:

Test Statistic: 4.22

p-value: 0.040

A low p-value (typically  $< 0.05$ ) would suggest significant differences between the groups.

*Figure 33 With being involved in risk assessment*

#### **4.6.6 Interpretation with being involved in risk assessment**

Based on figure 33 interpretations are as below

- **Lack of Strategy Integration**

Test Statistic: 2.95

P-value: 0.086

This result suggests no significant differences among groups in their perception of the lack of strategy integration. However, the p-value is somewhat close to the threshold, indicating potential variability worth examining.

- **Communication Issues in ERM-GRC**

Test Statistic: 1.94

P-value: 0.164

The groups are similar in their views on communication issues within ERM-GRC frameworks.

- **Differing Approaches to Risk Assessment**

Test Statistic: 0.53

P-value: 0.466

Indicates a high level of agreement among the groups regarding their perception of differing approaches to risk assessment.

- **Lack of Consistency in Policy Enforcement**

Test Statistic: 0.04

P-value: 0.846

This result shows a solid consensus among the groups regarding the consistency of policy enforcement.

- **Resource Allocation Issues**

Test Statistic: 3.70

P-value: 0.054

This result is very close to the typical threshold for significance, suggesting that there might be noticeable differences in perceptions concerning resource allocation issues.

- **Technology Integration Issues**

Test Statistic: 3.85

P-value: 0.050

This is just at the threshold of statistical significance, suggesting possible differences among groups in their perceptions of technology integration issues.

- **Struggles with Aligning to Regulatory Changes**

Test Statistic: 0.03

P-value: 0.872

This indicates strong group agreement regarding struggles with aligning to regulatory changes.

- **Unclear Leadership in ERM-GRC**

Test Statistic: 0.37

P-value: 0.543

Shows no significant differences among groups concerning unclear leadership in ERM-GRC.

- **Cultural Resistance to Change**

Test Statistic: 4.22

P-value: 0.040

Indicates significant differences between groups in perceptions of cultural resistance to change, suggesting that this issue is viewed differently across the organization.

- **Summary**

The results primarily indicate a consensus among the groups on most issues, except for cultural resistance to change and, to a lesser extent, technology integration and resource allocation issues. The significant result of cultural resistance to change highlights it as a particularly divisive issue within the organization. It warrants focused attention to understand and address varying perceptions and potentially foster a more adaptable organizational culture. The borderline significant results for technology integration and resource allocation suggest areas where perceptions might differ slightly, possibly influenced by departmental or role-based experiences. These areas may benefit from targeted improvements to enhance organizational alignment and effectiveness.

#### **4.6.7 Cliff's Delta (Effect Size)**

---

Cliff's Delta between 'Risk Management Domain' and 'Lack of Strategy Integration':  
-0.95 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Communication Issues in ERM-GRC':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Differing Approaches to Risk Assessment':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Lack of Consistency in Policy Enforcement':  
-0.95 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Resource Allocation Issues':  
-0.95 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Technology Integration Issues':  
-0.96 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Struggles with Aligning to Regulatory Changes':  
-0.97 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Unclear Leadership in ERM-GRC':  
-0.96 (large)  
Cliff's Delta between 'Risk Management Domain' and 'Cultural Resistance to Change':  
-0.96 (large)

*Figure 34 With risk management domain*

#### **4.6.8 Interpretation With Risk Management Domain**

Based on figure 34 interpretations are as below

- **Lack of Strategy Integration**

Delta: -0.95 (large)

This sizeable negative delta indicates a significant difference in perceptions regarding the lack of strategy integration across different groups, with one group likely perceiving much more significant issues than others.

- **Communication Issues in ERM-GRC**

Delta: -0.97 (large)

A significant effect size suggests a substantial divergence in views on communication issues within ERM-GRC, implying that experiences or perceptions vary significantly among different groups.

- **Differing Approaches to Risk Assessment**

Delta: -0.97 (large)

Indicates a significant difference between groups concerning their views on the approaches to risk assessment, with some groups likely encountering more inconsistencies or challenges.

- **Lack of Consistency in Policy Enforcement**

Delta: -0.95 (large)

The large delta suggests a significant variance in how different groups perceive the consistency of policy enforcement within the organization.

- **Resource Allocation Issues**

Delta: -0.95 (large)

A large delta indicates significant disparities in perceptions regarding resource allocation, pointing to potential inequities or disagreements among groups on resource distribution.

- **Technology Integration Issues**

Delta: -0.96 (large)

This significant effect size implies considerable differences among groups regarding technology integration issues, suggesting that some groups may face more challenges than others.

- **Struggles with Aligning to Regulatory Changes**

Delta: -0.97 (large)

A large delta points to a significant divergence in how different groups perceive the organization's struggles with aligning to regulatory changes.

- **Unclear Leadership in ERM-GRC**

Delta: -0.96 (large)

Indicates substantial differences in perceptions of leadership clarity within ERM-GRC, which could affect group morale and clarity of strategic direction.

- **Cultural Resistance to Change**

Delta: -0.96 (large)

Suggests a significant difference between groups in how they perceive cultural resistance to change within the organization, which might impact the effectiveness of change initiatives.

- **Summary**

Overall, these results demonstrate significant differences in perceptions among different organizational groups regarding critical challenges in risk management and governance. These disparities can have profound implications for implementing effective changes, requiring targeted interventions to address specific concerns of different groups to foster a more cohesive and efficient approach to risk management and policy implementation.

#### **4.6.9 Being involved in risk assessment activities**



Cliff's Delta between 'If involved in Risk Assessment' and 'Lack of Strategy Integration':  
 -0.96 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Communication Issues in ERM-GRC':  
 -0.97 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Differing Approaches to Risk Assessment':  
 -0.97 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Lack of Consistency in Policy Enforcement':  
 -0.95 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Resource Allocation Issues':  
 -0.95 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Technology Integration Issues':  
 -0.97 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Struggles with Aligning to Regulatory Changes':  
 -0.97 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Unclear Leadership in ERM-GRC':  
 -0.97 (large)  
 Cliff's Delta between 'If involved in Risk Assessment' and 'Cultural Resistance to Change':  
 -0.97 (large)

*Figure 35 With being involved in risk assessment activities*

#### **4.6.10 Interpretation With being involved in risk assessment activities**

Based on figure 35 interpretations are as below

- **Lack of Strategy Integration**

Delta: -0.96 (large)

This large effect size suggests a significant difference in perceptions regarding the lack of strategy integration across different groups. Those involved in risk assessment may perceive strategy integration issues more critically than those not involved.

- **Communication Issues in ERM-GRC**

Delta: -0.97 (large)

Similarly, a large negative delta indicates a significant difference in perceptions of communication issues within ERM-GRC, with those involved in risk assessment likely experiencing these issues more intensely.

- **Differing Approaches to Risk Assessment**

Delta: -0.97 (large)

This indicates a large effect size, suggesting significant differences between groups on their views on risk assessment approaches, highlighting a possible divide based on involvement in these processes.

- **Lack of Consistency in Policy Enforcement**

Delta: -0.95 (large)

This large delta suggests significant disparities in how groups perceive the consistency of policy enforcement, possibly influenced by their direct involvement in risk-related activities.

- **Resource Allocation Issues**

Delta: -0.95 (large)

A significant effect size here indicates that perceptions of resource allocation issues vary significantly, likely showing that those involved in risk assessment feel resources may not be adequately allocated.

- **Technology Integration Issues**

Delta: -0.97 (large)

A large delta points to significant differences in perceptions of technology integration issues, with a more significant impact felt by those directly dealing with risk management tools and technologies.

- **Struggles with Aligning to Regulatory Changes**

Delta: -0.97 (large)

This result suggests that those involved in risk assessment perceive more struggles with regulatory changes, a critical insight for managing compliance and adaptation strategies.

- **Unclear Leadership in ERM-GRC**

Delta: -0.97 (large)

This indicates a substantial difference in how leadership clarity is perceived within ERM-GRC, with those involved in risk assessment possibly feeling the impact of unclear leadership more acutely.

- **Cultural Resistance to Change**

Delta: -0.97 (large)

Shows a significant divergence in views regarding cultural resistance to change, with those involved in risk assessment perhaps more aware of or affected by resistance within the organization.

- **Summary**

The consistently large negative values of Cliff's Delta across all tested aspects suggest that individuals involved in risk assessment perceive more significant organizational issues and challenges than those not involved. This points to a need for targeted communication and policy adjustments to bridge the gap in perceptions and enhance the effectiveness of risk management practices across the board. These insights can help in tailoring training, resource allocation, and leadership strategies to better support those involved in risk management, fostering a more cohesive and effective risk management culture.

#### **4.7 Final Summary**

- **Significant Perceptual Differences Based on Involvement in Risk Management**

The analysis consistently revealed substantial differences in perceptions between employees involved in risk assessment and those who are not. This was particularly evident from the Cliff's Delta results, which indicated large effect sizes across a range of organizational issues. This suggests that involvement in risk assessment significantly affects one's experiences and opinions regarding organizational processes and challenges.

- **Challenges in Strategy Integration and Policy Enforcement**

Results from the Kruskal-Wallis test and histogram analyses highlight issues in strategy integration and consistency in policy enforcement as major employee concerns.

The significant disparities in perceptions suggest a gap between policy formulation and its practical application, which may lead to inefficiencies and frustrations among those directly involved in risk assessment.

- **Communication and Resource Allocation are Key Areas of Concern**

Communication issues within ERM-GRC and resource allocation were repeatedly identified as significant concerns through various analyses.\*\* These issues affect the efficiency of risk management processes and influence the overall effectiveness of organizational risk management strategies.\*\* Improved communication channels and more equitable resource distribution may help mitigate these concerns.

- **Impact of Organisational Culture and Leadership on Risk Management**

The findings underscore the critical role of leadership clarity and organizational culture in shaping risk management effectiveness. Unclear leadership and cultural resistance to change were significant predictors of dissatisfaction and operational challenges in risk management. Fostering a culture that supports clear leadership and is open to change could enhance the effectiveness of risk management practices.

- **Need for Proactive and Adaptive Risk Management Practices**

The analyses, mainly the correlation matrices, suggest that proactive and adaptive risk management practices must be sufficiently integrated within some organizational segments. The high correlation between proactivity in risk management and the adaptability of tools to regulations indicates that more adaptive approaches could lead to better outcomes in proactive risk management efforts.

- **Final Summary**

Overall, the detailed analysis of survey data from the organizational study on risk management reveals critical insights into how different facets of risk management are perceived within the organization, particularly highlighting the impact of employee

involvement in risk assessment. Addressing these identified issues with strategic interventions in communication, leadership, and policy enforcement can significantly enhance the effectiveness and efficiency of risk management operations within the organization.

## CHAPTER V:

### DISCUSSION

#### 5.1 Discussion of Results

This chapter discusses the findings in the results section, connecting them with the existing literature and theoretical frameworks introduced in earlier chapters. The discussion focuses on the study's research questions. It presents critical insights into the alignment between Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) in Information Technology (IT) companies. The chapter also addresses the study's practical and theoretical implications and highlights areas for future research.

#### 5.2 Discussion on Stakeholder Influence on ERM-GRC Alignment in IT Companies

The data analysis revealed significant variations in how different groups perceive stakeholder influence on ERM-GRC alignment. **Cliff's Delta** values across various metrics (e.g., stakeholder risk consultation, internal stakeholder clarity, and external influence on risk strategy) indicated significant differences in how individuals involved in risk management compared to those who were not. Respondents involved in risk management consistently reported less favourable perceptions of stakeholder engagement and the effectiveness of communication channels. This suggests that those more deeply involved in ERM activities have a more critical view of stakeholder management, possibly due to their proximity to the operational challenges.

In particular, the negative **Cliff's Delta** of -0.97 for **Stakeholder Risk Consultation** highlights that risk management professionals feel there is a substantial gap in how stakeholder consultations are integrated into risk strategies. This critical perspective extends to **Stakeholder Feedback Integration**, where a delta of -0.98

suggests a similarly large perception gap regarding how effectively feedback is incorporated into ERM processes.

These findings underscore the importance of developing more transparent and structured mechanisms for involving stakeholders in risk management. Enhanced stakeholder consultation, coupled with feedback loops, could help bridge the gap in perceptions between those directly involved in risk assessment and other organizational members.

### **5.3 Discussion on Effectiveness of Strategies for ERM-GRC Alignment in IT Companies**

The survey data provided mixed insights regarding the effectiveness of alignment strategies. **Histograms** (Figure 23) showed that most respondents agreed that policies and procedures are aligned well (Level 5 agreement). However, responses about the effectiveness of communication and reporting were bimodal, with peaks in both disagreement (Level 2) and strong agreement (Level 5). This response polarisation suggests that while some departments or groups experience strong alignment between ERM and GRC, others face significant challenges.

The **Kruskal-Wallis test** also revealed notable differences in how tools for ERM-GRC alignment are integrated into strategic planning. Groups heavily involved in risk management reported more significant challenges in tool integration, as indicated by the low p-value (0.014) for differences between groups in this area. This suggests that integrating risk management tools into broader strategic frameworks is inconsistent across the organization.

To address these challenges, organizations should thoroughly review how risk management tools are incorporated into their strategic planning processes. Streamlined

tool integration and more effective training and communication could help close the gaps observed between different organizational groups.

#### **5.4 Discussion on Top Tools and Techniques for Assessing ERM-GRC Alignment in IT Companies**

The survey results indicated that most respondents agreed that tools for ERM-GRC alignment are generally effective, particularly in risk communication and strategic planning (Figure 23). However, a significant proportion of respondents remained neutral on the issue of tool adaptability to changing regulations, reflecting uncertainty about whether existing tools are flexible enough to handle dynamic compliance requirements. The bimodal distribution in responses to the adaptability of tools (peaks at disagreement and strong agreement) further supports this ambiguity.

Moreover, the Kruskal-Wallis test results pointed to significant differences in how groups perceive the provision of stakeholder training related to ERM-GRC tools (p-value of 0.038), suggesting that training programs may not be uniformly effective across different departments.

To enhance the effectiveness of these tools, organizations should focus on improving the adaptability of their ERM-GRC tools and implementing more consistent training programs to ensure that all staff are well-prepared to use these tools effectively.

#### **5.5 Discussing on Key Challenges in ERM-GRC Alignment in IT Companies: Insights from Quantitative Analysis**

Several challenges were identified through the quantitative analysis, including:

- **Cultural Resistance to Change:** The Kruskal-Wallis test revealed statistically significant differences in perceptions of cultural resistance across the organization (p-value of 0.040), suggesting that some groups perceive more significant barriers to change than others.



- Resource Allocation Issues: The data, with a p-value of 0.054, indicated that there might be slight variations in how different groups perceive resource allocation challenges, with some departments feeling more constrained than others.
- Technology Integration Issues: At the threshold of significance (p-value of 0.050), the data pointed to potential discrepancies in how technology integration is managed, particularly concerning the alignment of ERM and GRC tools.
- Addressing these challenges will require targeted strategies, such as developing more vital leadership around change management, ensuring equitable resource distribution, and enhancing the integration of technology solutions that support both ERM and GRC framework

## **5.6 Conclusion**

In conclusion, the results of this study emphasize the intricate and multifaceted nature of aligning ERM (Enterprise Risk Management) and GRC (Governance, Risk, and Compliance) in IT companies. Factors such as stakeholder influence, effective communication, and tool integration are crucial in determining alignment success—however, challenges like cultural resistance and inconsistent resource allocation act as barriers that must be addressed. By focusing on these areas, organizations can enhance their risk management and compliance frameworks, leading to better alignment and improved resilience in the face of evolving risks. In conclusion, this study's results highlight the complex and multifaceted nature of ERM-GRC alignment in IT companies. Stakeholder influence, effective communication, and tool integration are critical factors that impact alignment success, while challenges such as cultural resistance and inconsistent resource allocation present barriers that must be overcome. By addressing these areas, organizations can strengthen their risk management and compliance

frameworks, ensuring better alignment and improved resilience in the face of evolving risks.

CHAPTER VI:  
SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

**6.1 Summary**

This dissertation examined the alignment between Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) frameworks in Information Technology (IT) companies. The primary goal was to explore how ERM can act as a catalyst for improving the integration and effectiveness of GRC frameworks within IT organizations. This research utilized both qualitative and quantitative methodologies, including surveys and inferential statistical techniques, to assess the stakeholder influence, effectiveness of strategies, tools, techniques, and challenges associated with ERM-GRC alignment.

Key findings from the study include:

- **Stakeholder Influence:** It was evident that stakeholder influence, particularly from senior management and regulatory bodies, plays a significant role in shaping the effectiveness of ERM-GRC alignment. These stakeholders' engagement helps ensure that ERM initiatives are aligned with corporate governance and compliance objectives.
- **Effectiveness of Strategies:** Different strategies, such as fostering a risk-aware culture, leveraging cross-functional collaboration, and using technology to automate risk assessment and compliance, were effective in achieving ERM-GRC alignment. However, resource constraints, particularly in smaller IT firms, present challenges in fully realizing these strategies.
- **Tools and Techniques:** Automated tools, including GRC platforms, real-time monitoring systems, and data analytics, were identified as the most effective for assessing the alignment between ERM and GRC frameworks. These tools enable

organizations to maintain continuous compliance while providing insights into emerging risks.

- **Metrics and Indicators:** Several metrics, including risk response time, regulatory compliance scorecards, and risk event frequency, were validated as indicators of ERM-GRC alignment success. These metrics help track progress, identify gaps, and ensure that alignment efforts are meeting organizational objectives.
- **Challenges:** Major challenges included cultural resistance to change, the complexity of integrating multiple compliance requirements, and resource constraints, particularly in rapidly evolving IT environments where agility is crucial.

## **6.2 Implications**

The findings of this study have several practical implications for IT companies aiming to improve their ERM and GRC alignment:

- **Strategic Adaptation:** IT companies must adapt their risk management strategies to consider the evolving regulatory landscape and the increasing complexity of IT risks. This includes investing in technology solutions that support integrated risk management and compliance processes.
- **Stakeholder Engagement:** Senior leadership should actively participate in ERM-GRC initiatives to ensure strategic goals are aligned. Engaging stakeholders such as regulatory bodies and customers early in the process can help shape the direction of risk management strategies and ensure compliance with industry standards.
- **Technology Integration:** Automation and data analytics tools should be prioritized to streamline risk management and compliance processes. By leveraging these

tools, IT companies can monitor real-time risks and respond proactively, minimizing the likelihood of regulatory violations or risk events.

- **Organizational Culture:** Fostering a risk-aware culture is critical. Employees at all levels should be trained and encouraged to engage in risk management activities, as their involvement is essential for the success of ERM-GRC alignment. Leadership should focus on change management practices to overcome resistance and ensure that risk management is embedded in daily operations.

### **6.3 Recommendations for Future Research**

- **Longitudinal Studies:** Future research could explore the long-term impacts of ERM-GRC alignment on organizational performance, focusing on how sustained integration improves resilience and regulatory compliance over time.
- **Cross-Industry Comparisons:** While this study focused on the IT sector, comparing ERM-GRC alignment across different industries would provide broader insights into how different sectors address the challenges of risk management and compliance.
- **Emerging Risks:** As technologies such as artificial intelligence, machine learning, and blockchain gain prominence, future studies should examine how these technologies influence ERM-GRC alignment and what new risks they introduce.
- **Regulatory Evolution:** Given the rapidly changing regulatory landscape in data privacy and cybersecurity areas, research should focus on how organizations can stay agile and adaptive in their compliance efforts without compromising on governance and risk management.

### **6.4 Conclusion**

In conclusion, this study has demonstrated that effective ERM-GRC alignment is critical for IT companies aiming to enhance their governance, mitigate risks, and

maintain regulatory compliance. By addressing the challenges of resource constraints, cultural resistance, and regulatory complexity, IT companies can create robust risk management frameworks that support operational efficiency and strategic growth. The successful alignment of ERM with GRC frameworks strengthens organizational resilience and positions companies to adapt to the ever-changing IT risk landscape.

These findings and recommendations are poised to significantly enhance the Governance, Risk Management, and Compliance (GRC) frameworks of organizations, particularly in high-stakes sectors like finance, healthcare, and technology, where effective risk management is paramount. Companies such as banks, insurance firms, and tech enterprises grappling with complex regulatory requirements can leverage these insights to refine their risk management and stakeholder engagement processes.

In conclusion, the results underscore the urgent need for strategic interventions in communication, leadership, and policy enforcement to elevate the effectiveness of organizational risk management. Employees directly involved in risk assessment activities have identified noteworthy inconsistencies in communication, resource allocation, and alignment of risk strategies. By addressing these perceptions through strengthened communication channels, equitable resource allocation, and enhanced policy enforcement, organizations can achieve superior risk management outcomes.

The study further emphasizes that decisive, proactive leadership coupled with a supportive organizational culture is crucial for successful GRC processes. Organizations that foster adaptable, transparent cultures and exhibit leadership clarity are positioned to integrate proactive risk management practices seamlessly. When combined with agile tools that keep pace with regulatory changes, these elements will enhance regulatory compliance and empower employees to navigate risks more effectively.

To create a cohesive and resilient GRC environment, organizations should prioritize closing perceptual gaps among employees, streamlining communication, and reinforcing leadership clarity. By implementing these recommendations, organizations will build a unified risk management framework, vastly improving their adaptability and responsiveness in today's complex regulatory and operational landscapes.

This chapter provided a comprehensive summary of the research findings, discussed the implications for IT companies, and offered recommendations for future research. The alignment of ERM and GRC frameworks remains a crucial area of focus for organizations seeking to navigate complex risk environments while maintaining compliance and strategic agility.

APPENDIX A  
SURVEY COVER LETTER

**QUESTIONNAIRE- Enterprise Risk Management as a Catalyst for Strategic  
Governance, Risk, and Compliance (GRC) Alignment in IT Companies**

Demographic Details:

I am from risk domain

Yes

No

Gender

Male

Female

Prefer not to say

Age Group

18-34

35-54

55-64

65+

Highest Educational Background

Undergraduate

Post Graduate

Professional Degree

Doctorate/PhD

Other: \_\_\_\_\_

Experience in the Industry



0-2

3-5

6-8

9-11

11+

I have been extensively involved in the risk assessment activities.

Yes

No

### **Section 1: Assessing Stakeholder Influence on ERM-GRC Processes**

Your responses will be measured on a 5-point Likert scale with the following options:

1 = Strongly Disagree

2 = Disagree

3 = Neither Agree nor Disagree

4 = Agree

5 = Strongly Agree

Please select the option that best reflects your opinion for each statement.

Stakeholders are regularly consulted about their risk tolerance and risk management preferences.

1      2      3      4      5

The views of external stakeholders significantly influence the risk management strategies of our organisation.

1      2      3      4      5

Internal stakeholders have a clear understanding of their roles and responsibilities in the risk management process.

1      2      3      4      5

Feedback from stakeholders is systematically incorporated into the updating of risk management policies and procedures.

1      2      3      4      5

Stakeholder engagement is perceived as a critical factor in the effectiveness of GRC activities.

1      2      3      4      5

There is a formal mechanism in place for stakeholders to influence decisions related to ERM-GRC processes.

1      2      3      4      5

Regular assessments are conducted to measure the impact of stakeholder influence on the effectiveness of ERM-GRC processes.

1      2      3      4      5

The organisation's leadership effectively communicates the importance of stakeholder input in governing risk and compliance.

1      2      3      4      5

Stakeholder influence aligns with the long-term strategic goals of the organisation in the context of ERM-GRC.

1      2      3      4      5

There is adequate training provided to stakeholders to understand and effectively contribute to the ERM-GRC processes.

1      2      3      4      5

## Section 2: Evaluating the Effectiveness of Strategies for ERM-GRC

### Alignment

Your responses will be measured on a 5-point Likert scale with the following options:

1 = Strongly Disagree

2 = Disagree

3 = Neither Agree nor Disagree

4 = Agree

5 = Strongly Agree

#### Risk Identification Consistency

The methods used for identifying risks in ERM and GRC are consistent across all departments.

1      2      3      4      5

#### Policy and Procedure Alignment

Policies and procedures are aligned between the ERM and GRC frameworks to ensure coherent risk management and compliance practices.

1      2      3      4      5

#### Communication and Reporting Mechanisms

Communication and reporting mechanisms are effective in conveying ERM and GRC information to relevant stakeholders.

1      2      3      4      5

#### Training and Awareness Programs

There are comprehensive training and awareness programs in place that enhance understanding and execution of ERM-GRC alignment.

1      2      3      4      5

### Compliance with Regulatory Requirements

Our organisation consistently meets or exceeds all regulatory requirements through integrated ERM-GRC activities.

1      2      3      4      5

### Risk Mitigation Effectiveness

The strategies implemented effectively mitigate risks identified through the ERM and GRC processes.

1      2      3      4      5

### Feedback Loops and Continuous Improvement

There are effective feedback loops in place that facilitate continuous improvement of ERM and GRC processes.

1      2      3      4      5

## **Section 3: Evaluation of Tools and Techniques for ERM-GRC Alignment Assessment**

Your responses will be measured on a 5-point Likert scale with the following options:

1 = Strongly Disagree

2 = Disagree

3 = Neither Agree nor Disagree

4 = Agree

5 = Strongly Agree

The current tools effectively integrate risk management principles into all levels of strategic planning.

1      2      3      4      5

The techniques used allow for a comprehensive assessment of compliance risks across the organisation.

1      2      3      4      5

The tools provided enable clear and consistent communication of risk and compliance information across departments.

1      2      3      4      5

The risk management tools are adaptable to changes in regulatory requirements and risk landscapes.

1      2      3      4      5

The techniques employed facilitate proactive identification and management of emerging risks.

1      2      3      4      5

The alignment assessment tools effectively measure the integration of ERM and GRC functions within the organisation.

1      2      3      4      5

There is adequate training available for staff on using these ERM-GRC alignment tools and techniques.

1      2      3      4      5

The techniques and tools used for ERM-GRC alignment are regularly updated to reflect the latest best practices and industry standards.

1      2      3      4      5

#### **Section 4.1: Challenges to ERM-GRC Alignment**

Your responses will be measured on a 5-point Likert scale with the following options:

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Neither Agree nor Disagree
- 4 = Agree
- 5 = Strongly Agree

Our organisation makes the employees that do not belong from the risk assessment domain perform risk assessments which leads to copy paste jobs without any outcomes.

- 1
- 2
- 3
- 4
- 5

#### **Section 4.2: Challenges to ERM-GRC Alignment**

Your responses will be measured on a 5-point Likert scale with the following options:

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Neither Agree nor Disagree
- 4 = Agree
- 5 = Strongly Agree

Our organisation's ERM and GRC strategies are not effectively integrated at the strategic planning level.

- 1
- 2
- 3
- 4
- 5

There is inadequate communication between our risk management and compliance departments.

- 1
- 2
- 3
- 4
- 5

ERM and GRC in our organisation use significantly different approaches for risk assessment.

1 2 3 4 5

There is a lack of consistency in enforcing policies and procedures across risk management and compliance functions.

1 2 3 4 5

Resources are disproportionately allocated between risk management and compliance, hindering effective ERM-GRC alignment.

1 2 3 4 5

The technology and tools used for ERM and GRC are not compatible or integrated.

1 2 3 4 5

Our organisation struggles to align ERM and GRC processes in response to regulatory changes.

1 2 3 4 5

There is unclear leadership and ownership of integrated ERM-GRC initiatives within our organisation.

1 2 3 4 5

Organisational culture resists the changes required to align ERM and GRC processes.

1      2      3      4      5



## REFERENCES

- Ashby, S., Palermo, T. and Power, M., (2012) 'Risk culture in financial organizations: An interim report.' *London School of Economics and Political Science*.
- Barney, J., (1991) 'Firm resources and sustained competitive advantage', *Journal of Management*, 17(1), pp. 99-120.
- Beasley, M. S., Clune, R., & Hermanson, D. R., (2005) 'Enterprise risk management: An empirical analysis of factors associated with the extent of implementation', *Journal of Accounting and Public Policy*, 24(6), pp. 521-531.
- Bhimani, A., (2009) 'Risk management, corporate governance and management accounting: Emerging interdependencies', *Management Accounting Research*, 20(1), pp. 2-5.
- COSO (2017) 'Enterprise Risk Management: Integrating with Strategy and Performance.' Available at: <https://www.coso.org> (Accessed: 16 October 2024).
- Deloitte (2019) 'Risk in focus: Risk management in the digital era.' Available at: <https://www2.deloitte.com/> (Accessed: 15 October 2024).
- Deloitte (2020) 'Global Risk Management Survey: Mitigating Regulatory Risks with ERM.' Available at: <https://www2.deloitte.com> (Accessed: 16 October 2024).
- Deloitte (2021) Bridging GRC and ERM for IT Companies: A Strategic Approach. Available at: <https://www2.deloitte.com> (Accessed: 16 October 2024).
- Donaldson, L., (2001) 'The contingency theory of organizations.' *Sage*.
- Forrester (2021) 'Business resilience through GRC integration.' Available at: <https://www.forrester.com/> (Accessed: 15 October 2024).
- Freeman, R. E., (1984) 'Strategic management: A stakeholder approach.' *Boston: Pitman*.

- Frigo, M. L., & Anderson, R. J., (2011) 'Strategic risk management: A foundation for improving enterprise risk management and governance', *Journal of Corporate Accounting & Finance*, 22(3), pp. 81-88.
- Frigo, M.L. and Anderson, R.J., (2011) 'What is strategic risk management?', *Strategic Finance*, 92(10), pp. 21-22.
- Gartner (2021) 'Risk Management and AI in IT Companies: A Survey of Technology Investment Trends.' Available at: <https://www.gartner.com> (Accessed: 16 October 2024).
- Gartner (2021) 2021 'GRC benchmarking survey'. Available at: <https://www.gartner.com/> (Accessed: 15 October 2024).
- Gates, S., Nicolas, J. and Walker, P.L., (2012) 'Enterprise risk management: A process for enhanced management and improved performance', *Management Accounting Quarterly*, 13(3), pp. 28-38.
- Hoyt, R. E., & Liebenberg, A. P., (2011) 'The value of enterprise risk management', *Journal of Risk and Insurance*, 78(4), pp. 795-822.
- IBM (2021) 'AI in risk management: A new era.' Available at: <https://www.ibm.com/> (Accessed: 15 October 2024).
- Jensen, M.C. and Meckling, W.H., (1976) 'Theory of the firm: Managerial behavior, agency costs and ownership structure', *Journal of Financial Economics*, 3(4), pp. 305-360.
- Kaplan, R.S. and Mikes, A., (2012) 'Managing risks: A new framework', *Harvard Business Review*, 90(6), pp. 48-60.
- KPMG (2021) 'Risk-Aware Culture and Strategic GRC Alignment in IT Companies.' Available at: <https://home.kpmg.com> (Accessed: 16 October 2024).
- KPMG (2022) 'Challenges in GRC Transformation: Cultural Resistance and Change Management.' Available at: <https://home.kpmg/> (Accessed: 16 October 2024).

- KPMG (2022) GDPR compliance and risk mitigation strategies. *Available at: <https://home.kpmg/>* (Accessed: 16 October 2024).
- KPMG (2022) 'The Role of Governance in IT Strategy: Aligning Technology with Business Objectives.' *Available at: <https://home.kpmg.com>* (Accessed: 16 October 2024).
- KPMG (2022) 'Transforming risk management in the digital age.' *Available at: <https://home.kpmg/>* (Accessed: 15 October 2024).
- Lam, J., (2014) 'Enterprise risk management: From incentives to controls.' *John Wiley & Sons*.
- McKinsey & Company (2020) 'Developing Risk-Aware Cultures in IT Through ERM.' *Available at: <https://www.mckinsey.com>* (Accessed: 16 October 2024).
- McKinsey & Company (2020) 'Harnessing RPA in compliance.' *Available at: <https://www.mckinsey.com/>* (Accessed: 15 October 2024).
- McKinsey & Company (2020) 'Overcoming Resource Constraints in GRC Implementation.' *Available at: <https://www.mckinsey.com/>* (Accessed: 16 October 2024).
- McKinsey & Company (2020) 'The Role of Risk-Aware Culture in Organizational Resilience.' *Available at: <https://www.mckinsey.com>* (Accessed: 16 October 2024).
- McKinsey & Company (2021) 'Leveraging GRC Automation for a Resilient IT Landscape.' *Available at: <https://www.mckinsey.com>* (Accessed: 16 October 2024).
- Mikes, A. and Kaplan, R.S., (2015) 'When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management', *Journal of Applied Corporate Finance*, 27(1), pp. 37-40.

- Morrow, J., (2011) 'Risk intelligence: Learning to manage what we don't know', *Business Strategy Review*, 22(4), pp. 42-45.
- Oetzel, J. and Getz, K.A., (2012) 'Why and how might firms respond strategically to violent conflict?', *Journal of International Business Studies*, 43(2), pp. 166-186.
- Paape, L. and Speklé, R.F., (2012) 'The adoption and design of enterprise risk management practices: An empirical study', *European Accounting Review*, 21(3), pp. 533-564.
- Power, M., (2009) 'The risk management of nothing', *Accounting, Organizations and Society*, 34(6-7), pp. 849-855.
- PwC (2020) 'ERM and regulatory compliance in the IT sector.' Available at: <https://www.pwc.com/> (Accessed: 16 October 2024).
- PwC (2020) 'SOX compliance trends and impact.' Available at: <https://www.pwc.com/> (Accessed: 15 October 2024).
- PwC (2021) 'Enterprise Risk Management Survey: Improving Risk Visibility Through ERM.' Available at: <https://www.pwc.com> (Accessed: 16 October 2024).
- PwC (2022) 'Compliance and Risk Visibility: The Impact of Integrated GRC Frameworks.' Available at: <https://www.pwc.com> (Accessed: 16 October 2024).
- PwC (2022) 'Strategic Risk Management in IT: The Convergence of ERM and GRC.' Available at: <https://www.pwc.com> (Accessed: 16 October 2024).
- PwC (2022) 'The Impact of ERM on Regulatory Compliance for IT Enterprises.' Available at: <https://www.pwc.com> (Accessed: 16 October 2024).
- PwC (2022) 'The Impact of Regulatory Complexity on GRC Alignment.' Available at: <https://www.pwc.com/> (Accessed: 16 October 2024).

- Racz, N., Weippl, E. and Seufert, A., (2010) 'Governance, risk & compliance (GRC) software—An exploratory study of software vendor and market research perspectives', *Information Systems Management*, 27(4), pp. 332-345.
- Racz, N., Weippl, E., & Seufert, A., (2010) 'A frame of reference for research of integrated governance, risk and compliance (GRC)', *Communications and Multimedia Security*, 106, pp. 106-115.
- Sax, J. and Andersen, T.J., (2019) 'Making risk management strategic: Integrating enterprise risk management with strategic planning', *European Management Review*, 16(3), pp. 617-632.
- Simons, R., (1999) 'How risky is your company?', *Harvard Business Review*, 77(3), pp. 85-94.
- Victor, A.A., Moronkunbi, M.A., Oyedeji, O.C., Victor, P.O. and Samuel, S.A., (2024) 'The Role of IT Governance Risk and Compliance (IT GRC) in Modern Organizations.' *International Journal of Latest Technology in Engineering, Management & Applied Science*, 13(6), pp.44-50.
- Woods, M., (2009) 'A contingency theory perspective on the risk management control system within Birmingham City Council', *Management Accounting Research*, 20(1), pp. 69-81.