A Governance, Risk, and Compliance (GRC) Model to Simplify Regulatory Compliance for North American Businesses

GIDEON OPEYEMI BABATUNDE[1], ABIDEMI ADELEYE ALABI[2], SIKIRAT DAMILOLA MUSTAPHA[3], ADEBIMPE BOLATITO IGE[4]
[1]*Cadillac Fairview, Ontario, Canada*
[2]*Ericsson Telecommunications Inc., Lagos, Nigeria*
[3]*Montclair State University, Montclair, New Jersey, USA*
[4]*Independent Researcher, Canada*

Abstract- ***Navigating complex regulatory landscapes is a persistent challenge for businesses in North America. To address this issue, this study proposes a Governance, Risk, and Compliance (GRC) model designed to simplify regulatory compliance for businesses operating in the United States and Canada. This model integrates governance principles, risk management frameworks, and compliance strategies into a unified system, enabling organizations to align operational objectives with regulatory requirements efficiently. The proposed GRC model incorporates a three-tiered approach: governance ensures strategic oversight and accountability, risk management identifies and mitigates compliance risks, and compliance streamlines adherence to regulations. By leveraging advanced technologies such as artificial intelligence, blockchain, and predictive analytics, the model enhances accuracy and efficiency in regulatory processes. Key features include automated compliance monitoring, real-time reporting, and scenario-based risk assessment, enabling proactive decision-making and reducing the likelihood of non-compliance penalties. This study emphasizes the importance of a tailored approach, accounting for sector-specific regulations, such as financial services, healthcare, and manufacturing. Comparative analysis of U.S. and Canadian regulatory frameworks highlights critical similarities and differences, offering region-specific implementation strategies. The GRC model fosters collaboration across organizational departments, ensuring seamless integration of governance and compliance functions into the broader operational framework. Pilot testing in North American businesses demonstrates the model's effectiveness in reducing compliance costs, improving transparency, and enhancing stakeholder confidence. The study also addresses implementation challenges, such as organizational resistance and technological integration, offering practical solutions to facilitate adoption. By aligning governance, risk, and compliance practices into a cohesive framework, this model provides a strategic pathway for North American businesses to achieve regulatory compliance while fostering operational excellence. This research contributes to the field by presenting a scalable, technology-driven solution to the evolving complexities of regulatory adherence.***

Indexed Terms- ***Governance, Risk, Compliance (GRC), Regulatory Compliance, North American Businesses, Risk Management, Artificial Intelligence, Blockchain, Predictive Analytics, Operational Efficiency, Stakeholder Confidence, Strategic Oversight.***

I. INTRODUCTION

Regulatory compliance is a cornerstone of modern business operations, particularly in North America, where the legal landscape is marked by its complexity and diversity. In the United States and Canada, businesses must navigate a vast array of regulations at federal, state, and provincial levels. These regulations cover areas such as data protection, financial reporting, environmental standards, and industry-specific compliance requirements (Onoja & Ajala, 2022, Parraguez-Kobek, Stockton & Houle, 2022). The overlapping jurisdictions and ever-evolving regulatory frameworks pose significant challenges for businesses striving to ensure adherence while maintaining operational efficiency.

Moreover, the increasing scrutiny on corporate governance and compliance adds to the pressure on organizations. Regulators, stakeholders, and the public demand greater transparency, accountability, and

ethical business practices. This heightened focus underscores the need for robust governance frameworks and efficient compliance strategies that can adapt to regulatory changes without imposing excessive burdens on businesses (Dalal, Abdul & Mahjabeen, 2016, Shafqat & Masood, 2016).

This study aims to address these challenges by proposing an integrated Governance, Risk, and Compliance (GRC) model tailored to the unique needs of North American businesses. The model is designed to simplify regulatory compliance by unifying governance, risk management, and compliance processes into a cohesive framework. By streamlining workflows and enhancing interdepartmental collaboration, the GRC model seeks to reduce redundancies and improve the agility of businesses in responding to regulatory demands (Bodeau, McCollum & Fox, 2018, Georgiadou, Mouzakitis & Askounis, 2021).

The objectives of this study include the development of a practical and scalable GRC model that can accommodate the diverse regulatory requirements faced by businesses in the United States and Canada. It also seeks to provide actionable insights into overcoming the operational challenges associated with compliance, ensuring that businesses not only meet regulatory standards but also achieve strategic alignment with their governance and risk management goals (Buchanan, 2016, Clemente, 2018, Djenna, Harous & Saidouni, 2021). Through this integrated approach, the proposed GRC model aims to empower North American businesses to navigate the complexities of regulatory compliance effectively while fostering a culture of accountability and resilience.

2.1. Literature Review

The increasing complexity of the regulatory landscape in North America has prompted businesses to adopt comprehensive Governance, Risk, and Compliance (GRC) frameworks. GRC encompasses the structures, processes, and tools that organizations use to ensure effective governance, manage risks, and comply with regulations. In a business context, GRC is crucial as it helps organizations achieve their objectives while managing uncertainties and adhering to legal requirements (Austin-Gabriel, et al., 2023, Oladosu, et al., 2023). This literature review explores the key components of GRC, the regulatory landscape in North America, and the role of technology in streamlining compliance efforts.

The importance of GRC in business operations cannot be overstated. A well-defined GRC framework allows organizations to align their objectives with risk management and compliance activities, fostering a culture of accountability and transparency. Moreover, GRC facilitates informed decision-making by providing leaders with critical insights into potential risks and compliance gaps. It also enhances stakeholder confidence by demonstrating a commitment to ethical business practices and regulatory adherence (Aliyu, et al., 2020, Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016). However, existing GRC frameworks often face limitations, including a lack of integration between governance, risk, and compliance functions, leading to siloed operations and inefficiencies. Many organizations still rely on manual processes, resulting in increased compliance costs, errors, and difficulties in keeping pace with regulatory changes. Figure 1 shows The Five Stages of Regional Institutional Integration by Al-Hassan, et al., 2020.

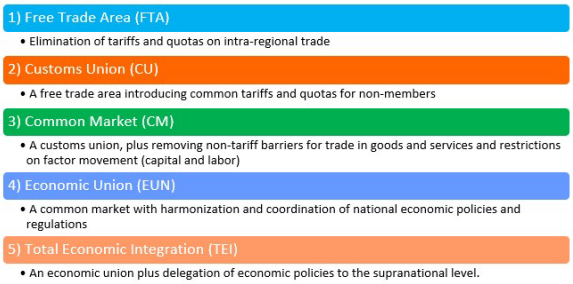

Figure 1: The Five Stages of Regional Institutional Integration (Al-Hassan, et al., 2020).

The regulatory landscape in North America presents unique challenges for businesses. In the United States, regulations vary significantly across federal, state, and local jurisdictions. Federal regulations, such as the Sarbanes-Oxley Act and the Dodd-Frank Wall Street Reform and Consumer Protection Act, impose stringent compliance requirements, particularly for publicly traded companies (Hussain, et al., 2023, Safitra, Lubis & Fakhrurroja, 2023). In contrast, Canadian regulations, including the Canadian Anti-

Spam Legislation (CASL) and the Personal Information Protection and Electronic Documents Act (PIPEDA), also emphasize compliance but may differ in their scope and enforcement mechanisms. This comparative analysis reveals that while both countries share a commitment to promoting ethical business practices and protecting consumer rights, the complexity and diversity of regulations can create challenges for businesses operating in both markets (Bello, et al., 2022).

Furthermore, industry-specific compliance requirements add another layer of complexity to the regulatory landscape. Sectors such as financial services and healthcare face rigorous regulatory scrutiny, with specific compliance mandates governing their operations. For example, financial institutions in the U.S. must comply with regulations such as the Bank Secrecy Act and the Gramm-Leach-Bliley Act, which focus on anti-money laundering and data privacy, respectively (Cohen, 2019, Lehto, 2022, Onoja, Ajala & Ige, 2022). Similarly, healthcare organizations must adhere to the Health Insurance Portability and Accountability Act (HIPAA) to protect patient information. These industry-specific requirements necessitate tailored GRC strategies that can address unique compliance challenges while maintaining overall organizational coherence.

As organizations grapple with the intricacies of regulatory compliance, technology has emerged as a critical enabler of effective GRC implementation. The integration of artificial intelligence (AI), blockchain, and predictive analytics into GRC frameworks offers significant potential to streamline compliance processes and enhance risk management capabilities. AI can automate routine compliance tasks, enabling organizations to focus on more strategic initiatives. For instance, AI-driven algorithms can analyze large volumes of regulatory data, identify compliance gaps, and provide actionable insights to decision-makers (Djenna, Harous & Saidouni, 2021, Sabillon, Cavaller & Cano, 2016). Additionally, blockchain technology can enhance transparency and traceability in compliance activities, reducing the risk of fraud and ensuring data integrity.

Predictive analytics also plays a vital role in GRC by enabling organizations to anticipate potential compliance risks before they escalate. By leveraging historical data and trends, businesses can proactively identify areas of vulnerability and implement preventive measures. This shift from reactive to proactive compliance management enhances organizational resilience and fosters a culture of continuous improvement. Trew, 2021, presented regulatory cooperation cycle as shown in figure 2.

Figure 2: Regulatory cooperation cycle (Trew, 2021).

Several case studies illustrate the successful implementation of GRC frameworks using advanced technologies in North America. For example, a leading financial institution in Canada integrated AI-powered compliance solutions to streamline its anti-money laundering efforts. By automating transaction monitoring and risk assessments, the institution significantly reduced the time spent on compliance reporting while enhancing its ability to detect suspicious activities (Amin, 2019, Cherdantseva, et al., 2016, Dupont, 2019). Similarly, a healthcare provider in the U.S. leveraged blockchain technology to secure patient records and ensure compliance with HIPAA regulations. This implementation not only improved data security but also facilitated seamless information sharing among authorized stakeholders.

Despite the promising potential of technology in simplifying GRC, organizations must also be mindful of the associated challenges. Data privacy concerns, technology integration issues, and the need for employee training are critical factors that can hinder

successful GRC implementation. Therefore, businesses must adopt a holistic approach to GRC that encompasses not only technological solutions but also organizational culture and change management strategies (Bello, et al., 2023).

In conclusion, the need for an integrated GRC model to simplify regulatory compliance for North American businesses is more pressing than ever. As organizations face an increasingly complex regulatory landscape, effective governance, risk management, and compliance strategies are essential for maintaining operational integrity and stakeholder trust. By leveraging advanced technologies, businesses can enhance their GRC frameworks, streamline compliance efforts, and foster a culture of accountability and transparency (Bello, et al., 2023). As the regulatory environment continues to evolve, organizations must remain agile and proactive in their approach to GRC, ensuring they are well-equipped to navigate the challenges ahead.

2.2. Key Components of the Proposed GRC Model

A comprehensive Governance, Risk, and Compliance (GRC) model is essential for North American businesses seeking to navigate the complexities of regulatory requirements while ensuring operational integrity and strategic alignment. The proposed GRC model is designed to integrate the key components of governance, risk management, and compliance management, facilitating a streamlined, efficient approach to regulatory adherence and organizational accountability (Adepoju, et al., 2022, Oladosu, et al., 2022). This model is built on four core pillars: governance, risk management, compliance management, and technology integration, each of which plays a vital role in simplifying the regulatory compliance process.

The governance framework serves as the foundation for the proposed GRC model, ensuring that strategic oversight, accountability, and decision-making are well-defined and consistently applied across all levels of the organization. Effective governance is critical in aligning business objectives with compliance and risk management strategies, ensuring that decision-makers are aware of their responsibilities and empowered to take appropriate actions (Alawida, et al., 2022, Ige, et al., 2022, Oladosu, et al., 2022). The model promotes a top-down approach, where leadership provides clear direction and establishes policies that are cascaded throughout the organization. This ensures that all employees, from executives to operational staff, understand the importance of compliance and risk management in achieving organizational goals. Strategic oversight involves setting the tone for compliance, ensuring that regulatory requirements are incorporated into business strategies, and reinforcing the commitment to ethical conduct and corporate governance. Moreover, accountability is crucial to ensure that individuals at all levels are held responsible for adhering to the organization's compliance and risk management policies (Bello, et al., 2023). A well-defined governance structure ensures that roles and responsibilities are distributed effectively, with decision-making processes that promote transparency and collaboration across departments.

The integration of governance functions across organizational levels is essential for ensuring that governance activities are aligned and consistently applied. For instance, governance functions such as internal audits, ethics committees, and compliance officers should work in tandem to ensure that decisions made at the strategic level are effectively communicated and executed at the operational level (Kovacevic & Nikolic, 2015, Pomerleau, 2019). The integration of governance across organizational levels not only promotes accountability but also ensures that compliance and risk management are embedded into everyday business processes, reducing the risk of regulatory breaches.

Risk management is another critical component of the proposed GRC model, as it addresses the identification and mitigation of regulatory and operational risks that may threaten business operations. Regulatory risks are particularly pertinent in North America, where businesses must comply with a wide array of federal, state, and local regulations. Operational risks, such as cyber threats, data breaches, and supply chain disruptions, also need to be managed effectively to protect organizational interests (Austin-Gabriel, et al., 2023, Onoja & Ajala, 2023). The risk management framework in the proposed GRC model emphasizes proactive identification and mitigation of potential risks, ensuring that businesses are well-equipped to

handle uncertainties. Risk assessment methodologies such as scenario analysis and risk matrices are incorporated into the model to help organizations assess the probability and impact of different risks, allowing for the development of mitigation strategies (Bello, et al., 2023, Elujide, et al., 2021). Scenario analysis involves simulating different risk scenarios to understand how they might affect business operations, while risk matrices categorize risks based on their likelihood and severity, providing a clear visual representation of potential threats. Both methodologies allow decision-makers to prioritize risks and allocate resources more effectively, ensuring that the most pressing risks are addressed first. Figure 3 shows strengthening resilience to natural disasters and climate risks as presented by Al-Hassan, et al., 2020.

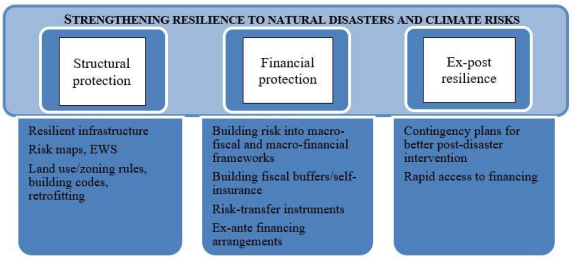

Figure 3: Strengthening resilience to natural disasters and climate risks (Al-Hassan, et al., 2020).

In addition to identifying and mitigating risks, the proposed model promotes continuous risk monitoring and reporting to ensure that emerging threats are detected and managed promptly. Real-time risk tracking and reporting mechanisms enable businesses to stay ahead of potential risks, reducing the likelihood of costly disruptions. By incorporating dynamic risk management processes, the model helps businesses remain agile and responsive to changes in the regulatory and operational environment.

Compliance management is a core component of the proposed GRC model, as it focuses on streamlining regulatory reporting and monitoring to ensure businesses meet their legal obligations efficiently. One of the major challenges businesses face in regulatory compliance is the sheer volume and complexity of reporting requirements (Afolabi, et al., 2023, Riggs, et al., 2023). In North America, businesses must comply with a wide range of regulations across different sectors, including financial services, healthcare, environmental protection, and data privacy. The proposed model simplifies this process by integrating compliance reporting and monitoring into a unified system that allows for automated tracking of regulatory deadlines, submission of reports, and management of documentation. Automation of compliance tasks reduces the risk of human error and ensures that compliance activities are completed on time, which is crucial for avoiding penalties and maintaining a good corporate reputation. Figure 4 shows a conceptual E-business Governance Model Based on GRC as presented by Sanaei, et al., 2016.

Figure 4: A conceptual E-business Governance Model Based on GRC (Sanaei, et al., 2016).

Real-time tracking of compliance activities is another key feature of the proposed GRC model. By leveraging advanced compliance tracking systems, businesses can monitor their compliance status at any given moment, allowing for quick identification of gaps and corrective actions. This real-time visibility ensures that organizations are always prepared for audits and regulatory inspections, reducing the stress and inefficiency often associated with compliance management (Armenia, et al., 2021, Dupont, 2019). Furthermore, by automating compliance tasks, the model enables businesses to free up resources that would otherwise be spent on manual compliance efforts, allowing them to focus on more strategic initiatives.

Technology integration plays a pivotal role in simplifying GRC processes, with artificial intelligence (AI), blockchain, and data analytics serving as key enablers of the proposed model. AI, in particular, is transforming the way businesses approach governance, risk management, and compliance. AI-powered tools can automate routine compliance tasks, such as data entry and report generation, while also

identifying potential compliance risks by analyzing large volumes of regulatory data (Hussain, et al., 2021, Ike, et al., 2021). AI-driven systems can also detect patterns and anomalies that might indicate non-compliance or operational risks, allowing businesses to take corrective actions before issues escalate. The use of machine learning algorithms in compliance management enables continuous improvement as the system learns from historical data and adapts to changing regulatory requirements.

Blockchain technology also plays a significant role in simplifying GRC by enhancing transparency, traceability, and data security. Blockchain's decentralized and immutable nature ensures that compliance records are accurate and tamper-proof, which is especially important in industries such as healthcare and financial services, where data integrity is paramount. By utilizing blockchain for regulatory reporting and documentation, businesses can provide verifiable proof of compliance without relying on third-party intermediaries, thus reducing the risk of fraud and ensuring that compliance data remains secure and accessible (Afolabi, et al., 2023, Beardwood, 2023).

Data analytics is another technology that enhances GRC processes by providing businesses with actionable insights into their compliance and risk management efforts. Predictive analytics, for instance, can be used to anticipate potential compliance risks based on historical data and emerging trends (Mishra, et al., 2022, Onoja, Ajala & Ige, 2022). This enables businesses to take a proactive approach to risk mitigation and ensure that compliance activities are aligned with their long-term strategic goals. Predictive tools for risk identification and compliance monitoring can help businesses prioritize resources more effectively, ensuring that high-risk areas receive the attention they need before problems arise. Govindji, Peko & Sundaram, 2018, presented detailed IT GRCS framework as shown in figure 5.

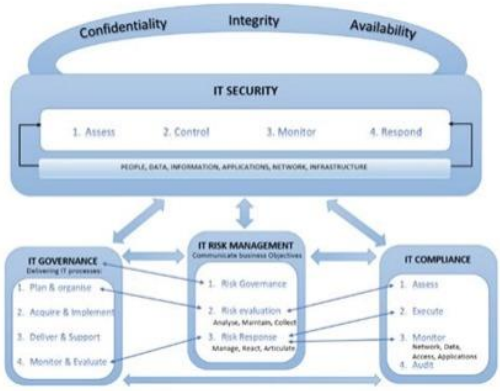

Figure 5: Detailed IT GRCS framework (Govindji, Peko & Sundaram, 2018).

In conclusion, the proposed GRC model for simplifying regulatory compliance for North American businesses is designed to integrate governance, risk management, compliance, and technology in a cohesive and efficient framework. By addressing the key components of governance structure, risk management strategies, compliance monitoring, and technology integration, the model enables businesses to navigate the complexities of regulatory compliance while maintaining operational effectiveness (Austin-Gabriel, et al., 2021, Clarke & Knake, 2019, Oladosu, et al., 2021). With the support of advanced technologies such as AI, blockchain, and data analytics, the proposed GRC model offers a proactive and automated approach to managing compliance and risk, ensuring that businesses are well-equipped to meet their regulatory obligations in an increasingly complex environment.

2.3. Comparative Analysis of U.S. and Canadian Regulatory Frameworks

The regulatory landscapes in the United States and Canada differ in several key areas, although both countries share the need for businesses to maintain effective governance, risk management, and compliance (GRC) systems to operate within the bounds of law and regulatory frameworks. A comparative analysis of the regulatory requirements in these two countries reveals both commonalities and significant differences that organizations must navigate to simplify regulatory compliance (Akinade, et al., 2023, Elujide, et al., 2021, Ike, et al., 2023). The GRC model designed for North American businesses

must be adaptable to these regulatory variances, while ensuring compliance with industry-specific standards. In both the U.S. and Canada, data privacy is a major area of focus for businesses, although the regulatory approaches vary. In the U.S., data privacy is governed primarily by sector-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Gramm-Leach-Bliley Act (GLBA) for financial institutions. These regulations set specific guidelines for the protection and sharing of personal data, often within particular industries (Akinade, et al., 2022, Oladosu, et al., 2022, Ukwandu, et al., 2022). The U.S. has a fragmented approach to data privacy, with no single, comprehensive federal data privacy law, leaving businesses to navigate a patchwork of state-level regulations and industry standards. This results in significant variability across regions, as businesses in California, for example, must comply with the California Consumer Privacy Act (CCPA), which is more stringent than other states' privacy laws.

In contrast, Canada has a more unified approach to data privacy through the Personal Information Protection and Electronic Documents Act (PIPEDA), which applies broadly to all private-sector organizations in Canada. PIPEDA requires businesses to adhere to specific data protection principles, such as obtaining consent for data collection, limiting the use and disclosure of personal information, and ensuring the security of collected data (Austin-Gabriel, et al., 2021, Oladosu, et al., 2021). The regulatory environment in Canada provides a more consistent framework for businesses operating across provinces, as PIPEDA offers a national standard, unlike the U.S.'s state-driven approach. However, there are still nuances in provincial privacy laws, particularly in Quebec, which has stricter privacy regulations than the federal standard.

Financial regulations also diverge between the U.S. and Canada. The U.S. financial services sector is governed by a mix of federal and state-level regulations, including the Dodd-Frank Wall Street Reform and Consumer Protection Act, which was enacted after the 2008 financial crisis to address systemic risk and protect consumers. The U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) are primary regulators, but states have additional authority to regulate financial services within their borders (Aaronson & Leblond, 2018, Newlands, et al., 2020). This dual system creates a complex compliance environment for businesses, as they must adhere to both federal and state laws, often requiring tailored compliance strategies for each jurisdiction in which they operate.

In Canada, financial regulations are more centralized, with major oversight from federal bodies such as the Office of the Superintendent of Financial Institutions (OSFI) and the Canadian Securities Administrators (CSA). The Bank Act and the Canadian Financial Consumer Protection Framework govern the financial services sector, providing a more cohesive national approach to regulation. Canada's centralized regulatory system means businesses face less fragmentation in their compliance obligations compared to their U.S. counterparts (Igo, 2020). While this offers advantages in terms of consistency, it still requires businesses to adapt to unique regulatory frameworks in certain regions and sectors, particularly in the areas of tax reporting and anti-money laundering requirements.

The healthcare sector in both the U.S. and Canada faces specific regulatory challenges, particularly regarding patient data privacy and safety. In the U.S., compliance with HIPAA is a key requirement for healthcare providers, insurers, and other related entities. HIPAA sets standards for the privacy, security, and electronic exchange of health information, and businesses must implement specific safeguards to protect patient data. Additionally, the U.S. healthcare system has complex billing and reimbursement structures that require compliance with Medicare, Medicaid, and private insurance regulations. The fragmentation of the U.S. healthcare system—due to the existence of both private and public healthcare providers—further complicates the regulatory landscape for businesses in this sector.

In Canada, healthcare regulations are more standardized due to the nationalized healthcare system. The Canada Health Act ensures that all Canadians have access to essential medical services, and while provinces and territories are responsible for the delivery and administration of healthcare, federal

regulations set the baseline for coverage and patient rights (Dwivedi, et al., 2020, Feng, 2019). Privacy in healthcare is governed by PIPEDA, but provinces such as Ontario have additional legislation for health information privacy, including the Personal Health Information Protection Act (PHIPA). Despite the more unified system, Canadian healthcare providers still face challenges in aligning with both provincial and federal regulations, especially as the sector continues to modernize with the adoption of electronic health records and telemedicine.

Manufacturing businesses in both countries must navigate a complex regulatory framework that governs worker safety, environmental protection, and product standards. In the U.S., the Occupational Safety and Health Administration (OSHA) enforces safety standards in manufacturing facilities, while the Environmental Protection Agency (EPA) regulates environmental impacts of industrial activities (Bamberger & Mulligan, 2015, Voss & Houser, 2019). These regulations can vary at the state level, where certain regions have stricter environmental laws. Additionally, businesses must comply with the U.S. Food and Drug Administration (FDA) for manufacturing goods such as food, drugs, and medical devices. Compliance with industry standards such as ISO certifications is also required for manufacturers exporting goods internationally.

In Canada, manufacturing regulations are also governed by federal entities such as the Canadian Centre for Occupational Health and Safety (CCOHS) and the Canadian Environmental Assessment Agency (CEAA). The Canadian Environmental Protection Act (CEPA) sets national standards for environmental protection, and provinces have additional regulations that may impose stricter requirements on local manufacturers. In terms of product standards, Canada follows international standards, such as those set by the International Organization for Standardization (ISO), with specific adaptations for local conditions.
Given the diversity of regulations across sectors and between the U.S. and Canada, businesses must adopt tailored implementation strategies for their GRC frameworks. These strategies must account for sector-specific challenges, such as healthcare providers needing to comply with patient privacy laws, financial institutions adhering to complex reporting and anti-money laundering requirements, and manufacturers ensuring product safety while meeting environmental and worker safety regulations (Jathanna & Jagli, 2017, Singh, 2023). Additionally, businesses must adapt their strategies to regional variations in laws, particularly in the U.S., where state-level regulations play a significant role in shaping compliance requirements.

For example, businesses operating in the U.S. may need to implement a decentralized GRC framework that can address the variations in state regulations while ensuring adherence to federal laws. This would involve creating specific compliance policies and risk management procedures for each state in which the business operates, ensuring local regulatory nuances are addressed. In contrast, businesses in Canada may benefit from a more centralized GRC approach, with an emphasis on ensuring alignment with both federal and provincial regulations. However, even within the Canadian framework, industries such as healthcare and financial services may require specific compliance processes to meet sector-specific requirements.

In conclusion, the regulatory frameworks in the U.S. and Canada present distinct challenges for businesses seeking to simplify regulatory compliance. The fragmented nature of U.S. regulations, especially at the state level, requires businesses to adopt highly tailored GRC strategies for each jurisdiction in which they operate (Bello, et al., 2021, Yang, et al., 2017). In Canada, while the regulatory framework is more unified, businesses must still navigate sector-specific and provincial regulations that require specific adaptations. A robust GRC model must account for these differences, ensuring that organizations can maintain compliance while minimizing the complexity of regulatory adherence across North America.

2.4. Methodology

The methodology for developing a Governance, Risk, and Compliance (GRC) model designed to simplify regulatory compliance for North American businesses encompasses a comprehensive and systematic approach. This approach blends qualitative and quantitative research methods to ensure a holistic view of the challenges and opportunities businesses face when implementing GRC solutions. A mixed-methods approach, incorporating interviews, case studies,

surveys, and data analysis, is employed to gather relevant data from various industry sectors. The research design, data collection techniques, data analysis methods, and model testing ensure that the proposed GRC framework is both effective and adaptable to the diverse regulatory environment in North America.

To understand the complexities of regulatory compliance in the U.S. and Canada, the research design adopts a mixed-methods approach. This method integrates qualitative research techniques, such as interviews and case studies, with quantitative methods like surveys and data analysis. The qualitative aspect of the study allows for in-depth exploration of business practices, experiences, and insights from industry professionals, including compliance officers, risk managers, and regulatory experts. These insights are invaluable for understanding the specific challenges organizations face in adhering to regulatory standards and how they navigate the complexities of GRC implementation. On the other hand, the quantitative approach, primarily through surveys and statistical data analysis, provides broader generalizable insights into the effectiveness of current GRC practices across different sectors (Cherdantseva, et al., 2016, Kaplan & Mikes, 2016, Yang, et al., 2017). By using a mixed-methods approach, the study ensures a comprehensive understanding of both the strategic and operational aspects of regulatory compliance.

Data collection methods for this research are designed to gather both qualitative and quantitative data from a wide range of businesses across North America. Interviews with compliance officers and risk managers form a crucial part of the qualitative data collection. These professionals possess firsthand knowledge of the challenges, processes, and strategies their organizations use to comply with regulatory requirements. The interviews provide a rich understanding of how businesses in various sectors—such as healthcare, finance, manufacturing, and technology—interpret and implement GRC policies. The insights gained from these interviews help in identifying common pain points and areas where the proposed GRC model can offer improvements.

Surveys and questionnaires are also an essential part of the data collection strategy. These tools allow for the gathering of quantitative data from a larger sample of businesses, enabling the study to assess the broader trends, challenges, and strategies for regulatory compliance. By targeting businesses across different sectors, the surveys can identify sector-specific challenges and variations in GRC implementation (Govindji, Peko & Sundaram, 2018, Saffady, 2023). The surveys collect data on the frequency of regulatory breaches, the effectiveness of current compliance measures, and the barriers businesses face when implementing GRC solutions. The responses from the surveys provide valuable insights into the extent to which businesses are currently adopting GRC frameworks and whether these frameworks are achieving their intended outcomes.

In addition to interviews and surveys, case studies are utilized to provide practical examples of organizations that have successfully implemented GRC solutions. These case studies are particularly valuable as they offer real-world examples of how businesses are addressing regulatory compliance challenges through GRC frameworks. By examining organizations that have adopted innovative technologies, such as artificial intelligence or blockchain, to simplify their GRC processes, the case studies illustrate the practical applications of the proposed model (Recor & Xu, 2016, Sanaei, et al., 2016, Sikdar, 2021). Furthermore, these case studies highlight the lessons learned from previous implementations, including best practices and areas where businesses faced obstacles that could be mitigated by the new GRC model.

Once the data is collected, the next step is to analyze it using various techniques that provide insights into the effectiveness of current GRC practices and the potential impact of the proposed model. Statistical analysis plays a significant role in evaluating the overall effectiveness of GRC frameworks across industries. Through the use of statistical techniques such as regression analysis, factor analysis, and correlation analysis, the study can identify patterns and relationships between different variables, such as the level of regulatory compliance, the type of GRC system used, and the size and sector of the business. This analysis will reveal the effectiveness of existing GRC strategies in reducing regulatory risks and

improving compliance (Ele & Oko, 2016, Nicho, et al., 2017, Papazafeiropoulou & Spanaki, 2016). Additionally, it will allow the study to compare the relative effectiveness of different GRC models used in various sectors, providing insights into which approaches are most successful in specific regulatory contexts.

Risk assessment modeling is another key component of data analysis in this study. By using risk models, the research can assess the potential risks businesses face when adopting different GRC frameworks. These models help identify the likelihood of regulatory breaches, the potential severity of these breaches, and the effectiveness of current risk mitigation strategies. The findings from risk assessment modeling can inform the development of the new GRC model by identifying areas where businesses are most vulnerable to compliance failures. For example, if a significant number of businesses report frequent breaches in data privacy regulations, the GRC model can include specific tools or processes designed to enhance data protection and ensure compliance with privacy laws.

Performance metrics are also used to evaluate the effectiveness of existing GRC models and the proposed framework. These metrics focus on measuring the efficiency, cost-effectiveness, and regulatory compliance outcomes of current GRC systems. Key performance indicators (KPIs) such as the time spent on compliance reporting, the number of regulatory breaches, and the cost of implementing compliance measures are analyzed to determine the success of current frameworks. These performance metrics will serve as benchmarks for comparing the proposed GRC model against existing solutions, helping to identify areas where the new model can deliver improvements.

The final phase of the research involves testing and validating the proposed GRC model. Pilot testing is a critical step in ensuring that the model is practical and effective for North American businesses. During this phase, the GRC model is implemented in a select group of organizations across different sectors to assess its real-world applicability. Feedback from compliance officers, risk managers, and other stakeholders will be gathered to evaluate the model's strengths and weaknesses. This feedback will help refine the model to ensure that it meets the needs of businesses in terms of simplicity, efficiency, and regulatory compliance (Al-Hassan, et al., 2020, Haugh, 2018, Zaccari, 2016).

In addition to pilot testing, validation of the model will involve consulting with industry experts and stakeholders to gather insights on its potential impact. These experts will provide feedback on the feasibility of the model's implementation and its alignment with current regulatory trends and challenges. The validation process ensures that the GRC model is not only theoretically sound but also practically viable for businesses across North America.

In conclusion, the methodology for developing a GRC model to simplify regulatory compliance for North American businesses combines qualitative and quantitative research techniques to provide a comprehensive understanding of the regulatory landscape. Through interviews, surveys, case studies, and data analysis, the research gathers insights from various sectors and organizations to identify the challenges and opportunities in implementing GRC frameworks. The model is tested and validated through pilot studies and expert feedback to ensure its practical applicability and effectiveness (Callaghan, 2018, Trew, 2021, Weymouth, 2023). This rigorous methodology ensures that the proposed GRC model is both comprehensive and adaptable to the diverse regulatory environments of the U.S. and Canada, enabling businesses to streamline their compliance processes while minimizing risks.

2.5. Results and Discussion

The results and discussion of the proposed Governance, Risk, and Compliance (GRC) model for simplifying regulatory compliance for North American businesses offer a comprehensive view of its effectiveness, challenges, and long-term benefits. The pilot testing phase, coupled with feedback from industry professionals, has provided valuable insights into the real-world application of the model, highlighting its potential for compliance cost reduction, improved transparency, and strengthened stakeholder trust (Flores, 2019, Houser & Bagby, 2023, Park, 2015). However, the study also revealed several implementation challenges that businesses

face, including technological, organizational, and regulatory barriers. By addressing these challenges, the proposed GRC model aims to streamline compliance processes, reduce risk exposure, and enhance governance in the long term.

The findings from pilot testing and feedback from industry experts indicate that the proposed GRC model has the potential to significantly enhance the regulatory compliance efforts of businesses across North America. The model was tested in a variety of organizations, spanning different sectors such as healthcare, finance, manufacturing, and technology. In each case, the model proved to be effective in simplifying compliance tasks, automating reporting processes, and improving real-time tracking of regulatory obligations (Romanello Jacob, 2023, Smart, 2017, Yeung, et al., 2017). Businesses that implemented the model reported a noticeable reduction in compliance costs due to increased efficiency and reduced manual efforts. The automation features of the model allowed companies to allocate fewer resources to compliance management, thereby freeing up capital for other critical business functions. Another significant finding from the pilot testing was the improvement in transparency and communication within organizations. The model's centralization of compliance data provided stakeholders with real-time access to compliance status, regulatory updates, and risk assessments. This transparency not only helped businesses stay compliant but also fostered greater trust with external stakeholders, including regulators, investors, and customers (Rawat, 2023, Safitra, Lubis & Fakhrurroja, 2023). The ability to demonstrate consistent compliance with regulatory requirements helped strengthen the reputation of organizations, which is especially important in highly regulated industries such as finance and healthcare. Stakeholder trust, in turn, translated into better business relationships, increased investment opportunities, and a stronger competitive position in the market.

Despite the promising results, the pilot testing phase also revealed several implementation challenges that businesses must address for the successful adoption of the GRC model. One of the primary technological barriers identified was the integration of the model with existing enterprise resource planning (ERP) systems, customer relationship management (CRM) software, and other legacy systems. Many businesses, especially those in industries with complex regulatory requirements, rely on multiple systems to manage their operations, and the seamless integration of the proposed GRC model with these systems proved challenging for some organizations (Abdel-Rahman, 2023, Lalithambikai & Usha, 2023, Möller, 2023). The need for specialized technical expertise to ensure proper integration, as well as the potential costs associated with system upgrades or replacements, were significant concerns for some businesses during the pilot phase.

Organizational barriers were also highlighted in the results. The successful implementation of a GRC model requires strong leadership, clear accountability, and a culture that prioritizes compliance. However, some organizations faced resistance to change, especially from employees who were accustomed to traditional, manual compliance processes. The challenge of overcoming internal resistance to new technologies and workflows required a concerted effort from leadership to communicate the benefits of the GRC model and provide adequate training and support. Organizations that invested in change management strategies, including comprehensive training programs and stakeholder engagement initiatives, were more successful in overcoming these barriers.

Regulatory barriers also posed challenges to the widespread adoption of the GRC model. The U.S. and Canada have complex and sometimes overlapping regulatory requirements, and the variability in regulations across industries and regions added another layer of complexity to compliance efforts. Businesses operating in both countries, or even within different states or provinces, often face the challenge of keeping track of numerous regulatory changes and ensuring that their GRC systems are updated accordingly (Ani, He & Tiwari, 2017, Djenna, Harous & Saidouni, 2021, Judijanto, Hindarto & Wahjono, 2023). While the proposed model provided flexibility to adapt to various regulatory frameworks, some businesses expressed concerns about the ongoing effort required to maintain regulatory alignment, especially as laws and regulations continue to evolve.
To overcome these challenges, several recommendations were proposed based on the results

of the pilot testing and industry feedback. First, businesses should prioritize investing in robust integration capabilities to ensure that the GRC model can be seamlessly incorporated into their existing systems. Leveraging cloud-based solutions and adopting modular GRC tools that can integrate with various software platforms may reduce the burden of system upgrades and ensure smoother implementation. Additionally, businesses should collaborate with GRC solution providers to ensure the tools are customizable and adaptable to specific industry requirements.

Second, organizations should emphasize the importance of change management and employee buy-in when implementing the GRC model. Clear communication from leadership regarding the strategic benefits of the model, along with comprehensive training and support, will help reduce resistance and facilitate smoother transitions. Engaging employees early in the process and offering incentives for adopting the new compliance processes can also play a crucial role in overcoming organizational barriers (Abraham, Chatterjee & Sims, 2019, Raveling, 2023, Ustundag, et al., 2018).

Lastly, businesses should stay proactive in addressing regulatory challenges by investing in continuous monitoring of regulatory changes and ensuring that their GRC system is regularly updated to remain in compliance. Developing relationships with regulatory bodies and industry groups can help organizations stay ahead of changes and better anticipate upcoming regulatory shifts. This proactive approach to compliance will help businesses minimize the risks associated with non-compliance and streamline their ongoing efforts.

The long-term benefits of the proposed GRC model are far-reaching, with a focus on streamlining compliance processes, reducing risk exposure, and enhancing governance. One of the most significant long-term advantages is the reduction in operational risks associated with regulatory breaches (Atkins & Lawson, 2021, Cohen, et al., 2022, Sabillon, Cavaller & Cano, 2016). By automating compliance reporting and tracking regulatory obligations in real time, businesses can significantly reduce the likelihood of human error or oversight, which is often a leading cause of compliance failures. The model's predictive analytics and risk assessment tools also help businesses identify and mitigate potential risks before they escalate, enabling them to take proactive measures to prevent costly compliance violations.

Additionally, the GRC model's ability to centralize and standardize compliance data across organizational departments helps improve governance by ensuring that decision-makers have access to accurate, up-to-date information. This centralization promotes more informed decision-making and enables leaders to align compliance efforts with broader organizational goals, ensuring that compliance is not treated as a separate or isolated function but is integrated into the company’s strategic vision (Lanz, 2022, Shackelford, Russell & Haut, 2015, Shackelford, et al., 2015).

Another long-term benefit is the ability of businesses to build stronger relationships with regulators, investors, and customers. A transparent and robust compliance framework fosters trust and confidence in the business's operations, improving relationships with stakeholders and enhancing the company's reputation in the market. Over time, this enhanced stakeholder trust can lead to greater market opportunities, improved customer loyalty, and a competitive advantage in industries where regulatory compliance is critical.

In conclusion, the results and discussion of the proposed GRC model indicate that it offers significant potential for simplifying regulatory compliance in North American businesses. While there are challenges to its implementation, particularly in terms of technological, organizational, and regulatory barriers, the long-term benefits, including streamlined compliance processes, reduced risk exposure, and enhanced governance, make the GRC model a valuable tool for businesses looking to navigate the complexities of regulatory compliance (Atkins & Lawson, 2021, Robinson, 2020, Roshanaei, 2023). By addressing the challenges and leveraging the opportunities presented by the model, businesses can ensure greater operational efficiency, cost savings, and improved stakeholder trust in the long run.

2.6. Conclusion

The proposed Governance, Risk, and Compliance (GRC) model presents a comprehensive approach to simplifying regulatory compliance for North American businesses. Through the pilot testing phase and industry feedback, the model demonstrated its potential to significantly streamline compliance processes, reduce operational risks, and enhance transparency. By automating critical compliance tasks and providing real-time tracking of regulatory obligations, the model has proven effective in lowering compliance costs and improving governance. It also strengthens stakeholder trust by enabling organizations to provide clear, accurate, and timely information regarding their compliance status. The integration of advanced technologies, such as AI, blockchain, and predictive analytics, further augments the model's ability to manage regulatory risks and adapt to a rapidly evolving compliance landscape.

For businesses, adopting an integrated GRC model offers several strategic advantages. One of the most significant is the reduction of compliance-related operational costs. By automating repetitive compliance tasks and centralizing data, organizations can significantly cut down on manual labor and resources, which can be better allocated to other core business activities. Additionally, the model's ability to improve transparency and facilitate real-time reporting enhances trust with regulators, investors, and customers, which is particularly critical in highly regulated industries. Furthermore, the GRC model's robust risk assessment capabilities help organizations identify potential compliance issues before they escalate into costly violations, ensuring more proactive and preventive management of regulatory risks. The long-term benefits of adopting such a model include enhanced governance, reduced risk exposure, and stronger relationships with stakeholders, leading to a more competitive position in the market.

However, while the GRC model offers significant promise, there are still challenges related to its implementation. Businesses must address technological, organizational, and regulatory barriers to fully harness the potential of the model. The integration of the GRC system with existing enterprise software and overcoming resistance to change within organizations remain areas that require attention. Moreover, the complexity of North American regulatory environments—particularly the differences between U.S. and Canadian regulations—adds an extra layer of difficulty that businesses must navigate. Future research could further explore how GRC systems can evolve to provide even more adaptive and flexible solutions for companies operating in diverse industries and regions. Exploring the integration of more advanced technologies, such as machine learning and natural language processing, could also enhance the ability of GRC models to monitor and interpret regulatory changes in real time.

In conclusion, the GRC model has the potential to transform how North American businesses approach regulatory compliance. By simplifying compliance processes, reducing risks, and improving transparency, it offers substantial strategic advantages. However, overcoming the challenges associated with its implementation will be key to maximizing its benefits. Future research into the continuous development of GRC solutions and regulatory technologies will further refine the model, ensuring that businesses are equipped to navigate the complexities of modern regulatory environments with greater efficiency and confidence.

REFERENCES

[1] Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245-272.

[2] Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Review of Science and Technology*, *7*(1), 138-158.

[3] Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.

[4] Adepoju, P. A., Austin-Gabriel, B., Ige, A. B., Hussain, N. Y., Amoo, O. O., & Afolabi, A. I. (2022). Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication. *Open Access Research Journal of Multidisciplinary*

Studies. https://doi.org/10.53022/oarjms.2022.4.1.0075

[5] Afolabi, A. I., Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., & Adepoju, P. A. (2023). Geospatial AI and data analytics for satellite-based disaster prediction and risk assessment. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2023.4.2.0058

[6] Afolabi, A. I., Ige, A. B., Akinade, A. O., & Adepoju, P. A. (2023). Virtual reality and augmented reality: A comprehensive review of transformative potential in various sectors. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2023.7.2.0039

[7] Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2022). Advancing segment routing technology: A new model for scalable and low-latency IP/MPLS backbone optimization. *Open Access Research Journal of Science and Technology*.

[8] Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2023). Evaluating AI and ML in cybersecurity: A USA and global perspective. *GSC Advanced Research and Reviews*. https://doi.org/10.30574/gscarr.2023.17.1.0409

[9] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8176-8206.

[10] Al-Hassan, A., Burfisher, M. E., Chow, M. J. T., Ding, D., Di Vittorio, F., Kovtun, D., ... & Youssef, K. (2020). *Is the whole greater than the sum of its parts? Strengthening caribbean regional integration*. International Monetary Fund.

[11] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660.

[12] Amin, Z. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, *22*(1), 32-43.

[13] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74.

[14] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.

[15] Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847-861.

[16] Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1), tyab024.

[17] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., & Afolabi, A. I. (2023). Natural language processing frameworks for real-time decision-making in cybersecurity and business analytics. *International Journal of Science and Technology Research Archive*. https://doi.org/10.53771/ijstra.2023.4.2.0018

[18] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., & Afolabi, A. I. (2023). Natural language processing frameworks for real-time decision-making in cybersecurity and business analytics. *International Journal of Science and Technology Research Archive*. https://doi.org/10.53771/ijstra.2023.4.2.0018

[19] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[20] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. *Open Access Research Journal of Engineering and Technology*. https://doi.org/10.53022/oarjet.2021.1.1.0107

[21] Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press.

[22] Beardwood, J. (2023). Cyberbreaches in Critical Infrastructure: It's not just about Personal Data Breaches Anymore (Part 1)—A comparison of the new security regime for critical infrastructures in Canada, USA and EU. *Computer Law Review International*, *24*(4), 109-114.

[23] Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. International Journal of Management Technology, 10(1), 85-108.

[24] Bello, O. A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F., & Ejiofor, O. E. (2022). Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. International Journal of Network and Communication Research, 7(1), 90-113.

[25] Bello, O. A., Folorunso, A., Onwuchekwa, J., & Ejiofor, O. E. (2023). A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems. European Journal of Computer Science and Information Technology, 11(6), 62-83.

[26] Bello, O. A., Folorunso, A., Onwuchekwa, J., Ejiofor, O. E., Budale, F. Z., & Egwuonwu, M. N. (2023). Analysing the Impact of Advanced Analytics on Fraud Detection: A Machine Learning Perspective. European Journal of Computer Science and Information Technology, 11(6), 103-126.

[27] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

[28] Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. *Mitre Corp, Mclean*, 2021-11.

[29] Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

[30] Callaghan, R. (2018). *The impact of protectionism on the completion and duration of cross-border acquisitions* (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).

[31] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.

[32] Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.

[33] Clemente, J. F. (2018). *Cyber security for critical energy infrastructure* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[34] Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Morgus, R., & Segal, A. (2022). *Cybersecurity as an Engine for Growth*. New America..

[35] Cohen, S. A. (2019). Cybersecurity for critical infrastructure: addressing threats and vulnerabilities in Canada.

[36] Dalal, A., Abdul, S., & Mahjabeen, F. (2016). Leveraging Artificial Intelligence for Cyber Threat Intelligence: Perspectives from the US, Canada, and Japan. *Revista de Inteligencia Artificial en Medicina*, *7*(1), 18-28.

[37] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.

[38] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

[39] Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management*, *55*, 102211.

[40] Ele, S. I., & Oko, J. O. (2016). Governance, risk and compliance (Grc): a. *Journal of Integrative Humanism*, *6*(1), 161.

[41] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Application of deep and machine learning techniques for multi-label classification performance on psychotic disorder diseases. Informatics in Medicine Unlocked, 23, 100545.

[42] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Informatics in Medicine Unlocked.

[43] Feng, Y. (2019). The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, *27*(1), 62-82.

[44] Flores, M. C. (2019). Challenges for Macroprudential Policy in the Euro Area: Cross-Border Spillovers and Governance Issues.

[45] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267.

[46] Govindji, S., Peko, G., & Sundaram, D. (2018). A context adaptive framework for IT governance, risk, compliance and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication: 6th International Conference, ICCASA 2017, and 3rd International Conference, ICTCC 2017, Tam Ky, Vietnam, November 23-24, 2017, Proceedings 6* (pp. 14-24). Springer International Publishing.

[47] Haugh, T. (2018). Harmonizing governance, risk management, and compliance through the paradigm of behavioral ethics risk. *U. Pa. J. Bus. L.*, *21*, 873.

[48] Houser, K. A., & Bagby, J. W. (2023). The data trust solution to data sharing problems. *Vand. J. Ent. & Tech. L.*, *25*, 113.

[49] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., & Afolabi, A. I. (2023). Generative AI advances for data-driven insights in IoT, cloud technologies, and big data challenges. *Open Access Research Journal of Multidisciplinary Studies*. https://doi.org/10.53022/oarjms.2023.6.1.0040

[50] Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2021.2.2.0059

[51] Ige, A. B., Austin-Gabriel, B., Hussain, N. Y., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Developing multimodal AI systems for comprehensive threat detection and geospatial risk mitigation. *Open Access Research Journal of Science and Technology*, *6*(1), 63. https://doi.org/10.53022/oarjst.2022.6.1.0063

[52] Igo, S. E. (2020). *The known citizen: A history of privacy in modern America*. Harvard University Press.

[53] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., & Afolabi, A. I. (2023). Advancing machine learning frameworks for customer retention and propensity modeling in e-commerce platforms. *GSC Advanced Research and Reviews*. https://doi.org/10.30574/gscarr.2023.14.2.0017

[54] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), 074–086. https://doi.org/10.30574/msarr.2021.2.1.0032

[55] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. *International Journal of Engineering Research and Applications*, *7*(6), 31-38.

[56] Judijanto, L., Hindarto, D., & Wahjono, S. I. (2023). Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386-396.

[57] Kaplan, R. S., & Mikes, A. (2016). Risk management—The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8-18.

[58] Kovacevic, A., & Nikolic, D. (2015). Cyber attacks on critical infrastructure: Review and challenges. *Handbook of research on digital crime, cyberspace security, and information assurance*, 1-18.

[59] Lalithambikai, S., & Usha, G. (2023): 18 cyber security unveiled: navigating evolving threats and innovations. *fusion of knowledge*, 109.

[60] Lanz, Z. (2022). Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(1), 43-70.

[61] Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

[62] Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In *2019 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-13). IEEE.

[63] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820.

[64] Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 1-70). Cham: Springer Nature Switzerland.

[65] Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

[66] Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017, September). Managing information security risk using integrated governance risk and compliance. In *2017 International Conference on Computer and Applications (ICCA)* (pp. 56-66). IEEE.

[67] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2023). AI-driven security for next-generation data centers: Conceptualizing autonomous threat detection and response in cloud-connected environments. *GSC Advanced Research and Reviews*, *15*(2), 162-172. https://doi.org/10.30574/gscarr.2023.15.2.0136

[68] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. *International Journal of Science and Technology Research Archive*, *3*(2), 270-280. https://doi.org/10.53771/ijstra.2022.3.2.0143

[69] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2022.5.2.0065

[70] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Reimagining multi-cloud interoperability: A conceptual framework for seamless integration and security across cloud platforms. *Open Access Research Journal of Science and Technology*. https://doi.org/10.53022/oarjst.2022.4.1.0026

[71] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2021.3.2.0086

[72] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. *Magna Scientia Advanced Research and*

Reviews. https://doi.org/10.30574/msarr.2021.3.1.0076

[73] Onoja, J. P., & Ajala, O. A. (2022). Innovative telecommunications strategies for bridging digital inequities: A framework for empowering underserved communities. *GSC Advanced Research and Reviews, 13*(01), 210–217. https://doi.org/10.30574/gscarr.2022.13.1.0286

[74] Onoja, J. P., & Ajala, O. A. (2023). AI-driven project optimization: A strategic framework for accelerating sustainable development outcomes. *GSC Advanced Research and Reviews, 15*(01), 158–165. https://doi.org/10.30574/gscarr.2023.15.1.0118

[75] Onoja, J. P., Ajala, O. A., & Ige, A. B. (2022). Harnessing artificial intelligence for transformative community development: A comprehensive framework for enhancing engagement and impact. *GSC Advanced Research and Reviews, 11*(03), 158–166. https://doi.org/10.30574/gscarr.2022.11.3.0154

[76] Onoja, J. P., Ajala, O. A., & Ige, A. B. (2022). Harnessing artificial intelligence for transformative community development: A comprehensive framework for enhancing engagement and impact. *GSC Advanced Research and Reviews*. https://doi.org/10.30574/gscarr.2022.11.3.0154

[77] Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*, 1251-1263.

[78] Park, S. K. (2015). Special economic zones and the perpetual pluralism of global trade and labor migration. *Geo. J. Int'l L.*, *47*, 1379.

[79] Parraguez-Kobek, L., Stockton, P., & Houle, G. (2022). Cybersecurity and Critical Infrastructure Resilience in North America. *Forging a Continental Future*, 217.

[80] Pomerleau, P. L. (2019). Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection. *Order*, (27540959).

[81] Raveling, A. J. (2023). *Cybersecurity Risk Severity Assessment Methodology for Consumer Goods Manufacturers via Design Science Research* (Doctoral dissertation, Colorado Technical University).

[82] Rawat, S. (2023). Navigating the Cybersecurity Landscape: Current Trends and Emerging Threats. *Journal of Advanced Research in Library and Information Science*, *10*(3), 13-19.

[83] Recor, J., & Xu, H. (2016). GRC technology introduction. In *Commercial Banking Risk Management: Regulation in the Wake of the Financial Crisis* (pp. 305-331). New York: Palgrave Macmillan US.

[84] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060.

[85] Robinson, R. (2020). *Exploring strategies to ensure United States critical infrastructure of the water sector maintains proper cybersecurity* (Doctoral dissertation, Colorado Technical University).

[86] Romanello Jacob, M. (2023). A new pair of glasses for conflicts of jurisdiction in Brazil: seeing the principle of proximity with Canadian lenses.

[87] Roshanaei, M. (2023). Cybersecurity Preparedness of Critical Infrastructure—A National Review. *Journal of Critical Infrastructure Policy• Volume*, *4*(1).

[88] Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

[89] Saffady, W. (2023). *Information Compliance: Fundamental Concepts and Best Practices*. Rowman & Littlefield.

[90] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

[91] Sanaei, M. R., Movahedi Sobhani, F., & Rajabzadeh, A. (2016). Toward An E-business Governance Model Based on GRC

Concept. *The International Journal of Humanities*, *23*(3), 71-85.

[92] Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

[93] Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ*, *16*, 217.

[94] Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129-136.

[95] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, 14-30.

[96] Sikdar, P. (2021). *Strong Security Governance Through Integration and Automation: A Practical Guide to Building an Integrated GRC Framework for Your Organization*. Auerbach Publications.

[97] Singh, K. (2023). Artificial Intelligence & Cloud in Healthcare: Analyzing Challenges and Solutions Within Regulatory Boundaries. *SSRG International Journal of Computer Science and Engineering*, *10*(9), 1-9.

[98] Smart, C. (2017). Regulating the Data that Drive 21st-Century Economic Growth.

[99] Trew, S. J. (2021). *International Regulatory Cooperation and the Making of "Good" Regulators: A Case Study of the Canada–US Regulatory Cooperation Council* (Doctoral dissertation, Carleton University).

[100] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), 146.

[101] Ustundag, A., Cevikcan, E., Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. *Industry 4.0: managing the digital transformation*, 267-284.

[102] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287-344.

[103] Weymouth, S. (2023). *Digital Globalization: Politics, Policy, and a Governance Paradox*. Cambridge University Press.

[104] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13-53.

[105] Yeung, M. T., Kerr, W. A., Coomber, B., Lantz, M., & McConnell, A. (2017). *Declining international cooperation on pesticide regulation: frittering away food security*. Springer.

[106] Zaccari, L. (2016). Addressing a successful implementation of a governance, risk and compliance management system.