Novelty Journals

ISSN 2394-7322

International Journal of Novel Research in Marketing Management and Economics
Vol. 11, Issue 1, pp: (180-196), Month: January - April 2024, Available at: www.noveltyjournals.com

Enhancing Anti-Money Laundering and Counter-Terrorist Financing Strategies through Integrated Cybersecurity and Compliance Measures

Japinye A. O.*

Banking Supervision Department, Central Bank of Nigeria, Lagos, Nigeria.

DOI: https://doi.org/10.5281/zenodo.10973122

Published Date: 15-April-2024

Abstract: **This research study investigated the integration of cybersecurity measures into Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies within financial institutions. The study aimed to assess the current state of AML/CTF strategies, evaluate the integration of cybersecurity measures, and investigate the impact of integrated cybersecurity and compliance measures on AML/CTF effectiveness. A quantitative approach was employed, utilizing surveys and statistical analyses to collect and analyze data from 400 participants in financial institutions. The findings revealed a significant positive correlation between the effectiveness of AML/CTF strategies and compliance with AML/CTF regulations. Additionally, the study found that a positive perception of the importance of cybersecurity was associated with a higher level of integration in AML/CTF operations. However, while compliance and cybersecurity integration had a positive impact on AML/CTF effectiveness, perception did not show a significant impact. The study concluded by discussing the implications of these findings and suggesting future research directions to enhance the integration of cybersecurity measures into AML/CTF strategies. These findings contribute to the understanding of the complex interplay between cybersecurity, regulatory compliance, and anti-financial crime strategies within financial institutions, providing valuable insights for policymakers and practitioners in the field.**

Keywords: **Anti-Money Laundering (AML); Counter-Terrorist Financing (CTF); Cybersecurity; Regulatory Compliance.**

1. INTRODUCTION

Money laundering and terrorist financing pose significant threats to the global financial system, necessitating continuous advancements in strategies to combat these illicit activities (Teichmann, 2020). In recent years, the convergence of cybersecurity and regulatory compliance has emerged as a crucial frontier in the fight against money laundering and counter-terrorist financing (Akartuna, Johnson and Thornton, 2022; Lessambo, 2023a). The potential synergies between cybersecurity and AML/CTF strategies also offer a promising frontier. Collaboration, robust risk management, and a technology-driven approach can emerge as avenues for a resilient defence. As the financial sector braces for future challenges, the insights from this study can provide a roadmap for enhancing integrated strategies, ensuring the continued efficacy of AML and CTF efforts in an ever-evolving landscape.

The financial industry has witnessed a paradigm shift with the rapid evolution of technology, giving rise to unprecedented opportunities and challenges. Financial institutions, as the gatekeepers of monetary transactions, face the daunting task of adapting to a digital era where the boundaries between physical and virtual financial spaces blur (Osei, Cherkasova and

Oware, 2023). The proliferation of online transactions, digital currencies, and complex financial instruments has created new avenues for money launderers and terrorists to exploit vulnerabilities in the system (Dupont, 2019). As a result, a comprehensive approach that combines robust cybersecurity measures with stringent regulatory compliance has become imperative to safeguard the integrity of the financial ecosystem (Uddin, Ali and Hassan, 2020). AML refers to measures implemented by financial institutions to detect and prevent illicit activities involving money laundering derived from criminal activities, while CTF involves efforts to combat the financing of terrorism by disrupting the flow of funds to terrorist organizations (Gaviyau and Sibindi, 2023). CTF aims to thwart the financing of terrorist activities, ensuring that resources are not available for planning and executing acts of terrorism. In addressing financial crimes, global efforts to combat AML and CTF have been significantly shaped by some international bodies, including the Financial Action Task Force (FATF).

Advancements in artificial intelligence (AI) and machine learning (ML) have emerged as powerful tools in the arsenal against financial crimes. These technologies offer the capability to analyze vast datasets, identify patterns, and detect anomalies with unparalleled speed and accuracy (Han et al., 2020). Integrating AI and ML into the systems of financial institutions holds the promise of fortifying AML and CTF efforts, providing proactive and adaptive defence against evolving threats (Alhajeri and Alhashem, 2023). Institutions can use these technologies to improve their capacity to identify suspicious activity and to expedite compliance procedures, which guarantees adherence to the constantly changing regulatory environment. On the other hand, cybersecurity is paramount in the financial sector, safeguarding institutions from malicious activities that can jeopardize the integrity of financial systems and compromise sensitive data (Aschi et al., 2022). The significance of cybersecurity lies in maintaining the confidentiality, integrity, and availability of financial information, ensuring trust among stakeholders and protecting against financial crimes and fraud (Kuzior et al., 2022). In recent times, financial institutions have faced an array of evolving cyber threats (Kaur, Habibi Lashkari and Habibi Lashkari, 2021). Moreover, while the use of fintech and other emerging technologies creates new attack surfaces and opportunities, the widespread use of mobile banking also creates new vulnerabilities (Mustapha et al., 2023). Proactive cybersecurity measures and careful monitoring of new trends are essential to remain ahead of the curve and protect the financial industry.

The integration of cybersecurity measures with AML and CTF strategies represents a pivotal nexus in the financial sector's ongoing battle against illicit activities (Lessambo, 2023b). Financial organizations can strengthen their regulatory compliance, improve detection capabilities, and strengthen defenses by investigating potential synergies between these domains (Mishra et al., 2022). In this complex landscape, the intersection of cybersecurity and AML/CTF strategies holds immense promise. Cybersecurity, with its arsenal of advanced technologies and threat intelligence, has the potential to augment the traditional methods employed in AML and CTF (Khan and Malaika, 2021). Through the integration of robust cybersecurity measures, financial institutions can create a more resilient defense against the evolving tactics of money launderers and terrorists. The synergies lie in the shared goal of identifying and mitigating risks. Cybersecurity tools, powered by artificial intelligence (AI) and machine learning (ML), can analyze vast datasets in real-time (El Hajj and Hammoud, 2023). These technologies offer a force multiplier effect, enabling financial institutions to detect anomalies, monitor transactions, and identify potential threats more efficiently (Pattnaik, Ray and Raman, 2024). Case studies of successful integrations provide valuable insights (Ash Siddiqi, Darwiyanto and Priyadi, 2023

The aim of this study is to investigate the current landscape of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) through integrated cybersecurity and compliance strategies. The objectives are as follows:

1. To assess the current state of AML and CTF strategies by measuring the effectiveness of current AML/CTF strategies and compliance with AML/CTF regulations.

2. To evaluate the integration of cybersecurity measures in AML and CTF strategies by assessing the integration level of cybersecurity in AML/CTF operations and the perception of the importance of cybersecurity in AML/CTF.

3. To investigate the impact of integrated cybersecurity and compliance measures on AML and CTF effectiveness by examining the relationship between AML/CTF effectiveness, integration level of cybersecurity measures in AML/CTF, and compliance with AML/CTF regulations.

The next section is a literature review section that aims to provide a theoretical foundation for understanding and interpreting the complex interactions between cybersecurity, regulatory compliance, and financial crime prevention in the context of AML and CTF strategies. The analysis seeks to offer a structured approach to studying how integrating cybersecurity

measures can enhance AML and CTF efforts by discussing various theoretical frameworks. These theoretical frameworks contribute to a comprehensive analysis of how integrating cybersecurity measures can enhance AML and CTF strategies, providing researchers and practitioners with valuable insights for improving cybersecurity and compliance measures in financial institutions.

2. LITERATURE REVIEW

2.1 Systems Theory

Systems theory provides a holistic lens to analyze the interconnected elements of cybersecurity, regulatory compliance, and anti-financial crime strategies within financial institutions (Gupta, Dwivedi and Shah, 2023). It views these components as interdependent, emphasizing the need for a coherent and integrated approach to understanding the ripple effects of changes (Uddin, Ali and Hassan, 2020). This will allow scholars to explore how integrating cybersecurity measures influences the entire AML and CTF system, considering the dynamic relationships between technological advancements, regulatory requirements, and organizational practices.

However, systems theory may face criticism for oversimplifying complexities and neglecting individual agency within the system (Karanikas and Zerguine, 2024). It might struggle to capture the nuanced decision-making processes and ethical considerations at the micro-level (Turner and Baker, 2019). Furthermore, the approach may minimize the particular difficulties and traits of each component by emphasizing interconnectedness. Systems theory is quite helpful in the research despite these criticisms. It provides a comprehensive framework to assess the systemic impact of cybersecurity integration in AML and CTF efforts. This can contribute to assessing integration efficacy, pinpointing any bottlenecks, and providing suggestions for a more adaptable and resilient financial ecosystem by comprehending the interconnection.

2.2 Risk Management Frameworks

Risk Management Frameworks, such as the COSO ERM model, offer a structured approach to identify, assess, and respond to risks in the integration of cybersecurity with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies (Jarjoui and Murimi, 2021; Marquez-Tejon, Jimenez-Partearroyo and Benito-Osorio, 2021). This model assists in comprehensively understanding potential threats and vulnerabilities while providing guidelines for risk mitigation (Marquez-Tejon, Partearroyo and Benito-Osorio, 2023). However, a critical analysis reveals potential limitations, including the inherent challenge of predicting and quantifying evolving cyber threats accurately (Crotty and Daniel, 2022). The dynamic nature of technology and the quick growth of cyber hazards may also make it difficult for the framework to adapt. Despite these limitations, its application in the study is beneficial. This can be applied systematically to evaluate risks associated with the integration, guiding financial institutions in developing adaptive strategies (Cremer et al., 2022). The framework, when used judiciously, offers a valuable tool for enhancing the overall risk resilience of AML and CTF efforts in the context of evolving cybersecurity landscapes and Regulatory Compliance Models.

2.3 Social Network Theory

Social Network Theory, as a theoretical framework for the study, offers a unique perspective on the collaborative aspects of integrating cybersecurity with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies (Carley, 2020). It emphasizes the relationships and information flows among stakeholders, including financial institutions, regulatory bodies, and technology providers. However, the negative aspect of Social Network Theory lies in its potential oversimplification of complex relationships and the assumption that well-connected nodes equate to effective collaboration (Parker, 2019). The framework may overlook power dynamics, conflicting interests, and informal connections that impact decision-making (Muijs, West and Ainscow, 2010). Despite this limitation, Social Network Theory proves useful in understanding the social fabric influencing the integration process (Chikouche et al., 2018). It provides insights into communication patterns and the diffusion of innovations, aiding researchers in comprehending the relational dynamics shaping successful collaborations in the realm of AML, CTF, and cybersecurity integration.

2.4Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) is a valuable theoretical framework for analyzing the integration of cybersecurity measures into Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies (Marangunić and Granić, 2014; Cavus, Omonayajo and Mutizwa, 2022). TAM, developed by Davis in 1989, focuses on

individuals' acceptance and adoption of new technologies (Davis, Bagozzi and Warshaw, 1989). It posits that perceived ease of use and perceived usefulness are crucial factors influencing technology adoption. TAM provides insights into how financial professionals within institutions might perceive and accept the integration of advanced cybersecurity technologies (Hasani et al., 2023). However, a potential limitation lies in its emphasis on individual perceptions, potentially overlooking broader organizational or systemic factors influencing technology adoption (Ursavaş, 2022). In the context of AML and CTF, where collaborative efforts and systemic resilience are paramount, TAM's individual-centric focus might not fully capture the organizational dynamics involved, but TAM remains a useful tool. Understanding individual perceptions of the ease and usefulness of integrated cybersecurity measures is vital for successful adoption within financial institutions. The study can enhance the efficacy of AML and CTF activities by customizing tactics to address issues, improve user acceptance, and optimize the integration process by identifying its individual-level insights.

3. METHODOLOGY

To achieve the objectives of this study, an online hosted survey with Google Forms was used to anonymously collect quantitative data from 400 participants whose professions on LinkedIn contain certification or job roles connected to cybersecurity, compliance, AML, or CTF. When considering the research philosophy for this study, the chosen philosophy for this study is positivism, which emphasizes objective data collection and analysis (Ryan, 2018). Positivism was chosen due to the study's focus on measurable outcomes related to cybersecurity integration in AML and CTF strategies. While interpretivism, which focuses on understanding subjective meanings and interpretations, was also considered, it was deemed less suitable for a study with strictly quantitative survey questions. Pragmatism, which allows for a combination of both positivist and interpretivist approaches, was also considered but ultimately not chosen, as it may not align as closely with the study's focus on quantitative data collection and analysis.

For the research design, the survey-based approach was selected for its efficiency in reaching a large number of participants and collecting quantitative data (Newton, 2023). While a qualitative research design would have allowed for a deeper exploration of subjective experiences and perceptions, it was not deemed suitable for this study's focus on quantitative data collection. The sampling strategy of convenience sampling was chosen for its practicality in identifying participants on LinkedIn with relevant certifications or job roles (Etikan, Musa and Alkassim, 2016). Despite the potential for bias, efforts were made to minimize this through careful selection criteria. A sample size of 400 participants was determined to achieve a balance between statistical power and practicality (Israel, 1992; Andrade, 2020). This sample size is considered sufficient to capture a diverse range of perspectives and experiences within the target population, while also ensuring the reliability and generalizability of the findings.

The questionnaire is designed to be comprehensive, covering various aspects of AML, CTF, and cybersecurity integration. The questions are structured to be clear and concise, with multiple-choice Likert type answers to ensure uniformity in responses. The questionnaire starts with demographic information, including age, gender, position and role, and organization type. This information provides context and allows for the analysis of responses based on different demographic variables. The first objective of the study focuses on assessing the current state of AML and CTF strategies. Participants are asked about their confidence in their organization's ability to detect and prevent money laundering and terrorist financing activities, their satisfaction with current strategies, the frequency of strategy reviews, alignment with regulations and best practices, and the effectiveness of training programs.

The second objective of the study evaluates the integration of cybersecurity measures in AML and CTF operations. Participants are asked about the integration level of cybersecurity measures, consideration of cybersecurity risks in strategy development, the effectiveness of cybersecurity controls, reporting and investigation of cybersecurity incidents, and collaboration between cybersecurity and AML/CTF teams. The third objective of the study investigates the impact of integrated cybersecurity and compliance measures on AML and CTF effectiveness. This objective builds on the variables measured in the first and second objectives, examining the relationship between AML/CTF effectiveness, integration level of cybersecurity measures, and compliance with regulations. Ethical considerations were paramount throughout the research process, including informed consent, confidentiality, and voluntary participation. Participants were informed about the purpose of the study, their rights as participants, and the confidentiality measures in place to protect their data. Moreover, no personally identifiable data was collected from the participants. Informed consent was obtained from all participants before they began the survey, and their participation was voluntary. Given the survey nature of the study, several limitations were acknowledged in the study, including the potential for sampling bias and self-reporting bias. These limitations are all those that are typically associated with all survey-related studies.

Novelty Journals

ISSN 2394-7322

International Journal of Novel Research in Marketing Management and Economics
Vol. 11, Issue 1, pp: (180-196), Month: January - April 2024, Available at: www.noveltyjournals.com

4. RESULTS

4.1 Socio-Demographic Characteristics of Participants

Table 4.1 below presents the socio-demographic characteristics of the respondents in the study. The majority of respondents were in the 45-54 age range (38.3%), with the 35-44 years group being the closest (28.7%). In terms of gender, there were more male respondents (66.3%) than female (33.7%). Regarding positions, most respondents were in operational/non-management roles (49.3%), followed by middle management (34.0%). The organizations represented were diverse, with private sector/corporate and non-profit/NGO sectors being the most prevalent.

The socio-demographic characteristics of the participants in this study provide valuable insights into the composition of the sample and can help contextualize the findings. Age distribution shows a diverse range, with the majority falling between 35 and 54 years old, comprising nearly 85% of the sample. This indicates a relatively mature and experienced group, which may suggest a certain level of expertise and familiarity with the subject matter. However, the lower representation of younger participants (18-24 years old) and older participants (65+ years old) could limit the generalizability of the findings to these age groups. Gender distribution indicates a predominance of male participants, making up 66.3% of the sample. This gender imbalance may reflect broader trends in the cybersecurity, compliance, AML, and CTF fields, where men are traditionally more represented. It also raises questions about gender diversity and inclusion in these industries.

Regarding position or role within organizations, the majority of participants are in operational/non-management roles (49.3%), followed by middle management (34.0%) and executive/upper management (8.5%). This distribution suggests that the study captured perspectives from various levels within organizations, providing a comprehensive view of the subject matter. However, the lower representation of executive/upper management may limit the depth of insights into high-level decision-making processes. In terms of organization type, the sample is fairly evenly distributed among government/public sector, non-profit/NGO, private sector/corporate, and educational/research institutions. This diversity in organizational backgrounds enhances the generalizability of the findings across different sectors. However, the relatively smaller proportion of participants from other types of organizations (7.0%) could limit the applicability of the findings to these specific sectors.

Table 4.1: Participants' Socio-Demographic Characteristics

Socio-Demographic Characteristics	Frequency	Percentage
Age		
18 - 24 years	8	2.0
25 - 34 years	50	12.5
35 - 44 years	115	28.7
45 - 54 years	153	38.3
55 - 64 years	66	16.5
64+ years	8	2.0
Gender		
Male	265	66.3
Female	135	33.7
Position		
Executive/Upper Management	34	8.5
Middle Management	136	34.0
Operational/Non-Management	197	49.3
Others	33	8.3
Organization		
Government/Public Sector	32	8.0
Non-Profit/NGO	123	30.8
Private Sector/Corporate	123	30.8
Educational/Research Institution	94	23.5
Others	28	7.0

Novelty Journals

ISSN 2394-7322

International Journal of Novel Research in Marketing Management and Economics
Vol. 11, Issue 1, pp: (180-196), Month: January - April 2024, Available at: www.noveltyjournals.com

4.2 Descriptive Statistics

Table 4.2 below presents the descriptive results for the variable "effectiveness of current AML/CTF strategies", highlighting areas of strength and areas for improvement in organizations' AML/CTF strategies. This is based on participants' perceptions regarding their organizations' anti-money laundering and counter-terrorist financing efforts. While there is generally a positive perception of effectiveness, there are also areas such as alignment with regulations and industry best practices that require attention. The majority of participants (86.3%) expressed some level of confidence in their organization's ability to detect and prevent money laundering and terrorist financing activities, with 40.8% being moderately to extremely confident. This positive perception indicates a generally effective current strategy, which is encouraging for organizations.

In terms of satisfaction with the outcomes of current AML/CTF strategies, a significant proportion of participants (89.5%) reported being at least slightly satisfied, with 9.3% being very to extremely satisfied. While there is room for improvement, this suggests a moderate level of satisfaction overall, indicating that the strategies are yielding some positive outcomes. Regarding the frequency of AML/CTF strategies review and update, a considerable number of participants (58.3%) reported that strategies are reviewed and updated occasionally to very often. This proactive approach to addressing emerging risks is crucial in the constantly evolving landscape of financial crime and demonstrates a commitment to staying ahead of potential threats.

In terms of alignment with regulatory requirements and industry best practices, the majority of participants (57.0%) reported that their strategies are moderately to completely aligned. However, 43% reported only slight alignment or no alignment, raising concerns about regulatory compliance and effectiveness. This indicates a need for organizations to focus on aligning their strategies more closely with regulatory requirements and industry standards. Regarding the effectiveness of training programs in ensuring staff understand and comply with AML/CTF regulations, a large proportion of participants (84.1%) reported that training programs are at least slightly effective. This suggests that organizations are investing in training, which is essential for ensuring staff compliance with regulations. However, there is still room for improvement in this area to ensure that training programs are as effective as possible.

Table 4.2: Effectiveness of current AML/CTF strategies

Statements	Frequency	Percentage
How confident are you in your organization's ability to detect and prevent money laundering and terrorist financing activities?		
Not Confident at all	55	13.8
Slightly Confident	182	45.5
Moderately Confident	100	25.0
Very Confident	54	13.5
Extremely Confident	9	2.3
How satisfied are you with the outcomes of your current AML/CTF strategies		
Not Satisfied at all	42	10.5
Slightly Satisfied	203	50.7
Moderately Satisfied	118	29.5
Very Satisfied	32	8.0
Extremely Satisfied	5	1.3
How frequently are your AML/CTF strategies reviewed and updated to address emerging risks?		
Never	43	10.8
Rarely	124	31.0
Occasionally	187	46.8
Often	40	10.0
Very Often	6	1.5
How well do your AML/CTF strategies align with regulatory requirements and industry best practices?		
Not Aligned at all	26	6.5
Slightly Aligned	146	36.5

Moderately Aligned	142	35.5
Very Aligned	64	16.0
Completely Aligned	22	5.5
How effective are your training programs in ensuring that staff understand and comply with AML/CTF regulations		
Not Effective at all	64	16.0
Slightly Effective	197	49.3
Moderately Effective	100	25.0
Very Effective	34	8.5
Extremely Effective	5	1.3

Table 4.3, presents the descriptive results for the variable "Compliance with AML/CTF regulations". This provides insights into participants' familiarity with, training on, confidence in, and the effectiveness of internal controls for compliance with AML/CTF regulations, as well as the transparency of their organization's reporting process for AML/CTF compliance issues. The data indicates that there is room for improvement in several areas. While a majority of participants (86%) reported being at least slightly familiar with current AML/CTF regulations, 14% indicated they were not familiar at all. This suggests that there may be a need for increased awareness and training on regulatory requirements within organizations to ensure full compliance. In terms of training frequency, a significant proportion of participants (69.3%) reported receiving training on AML/CTF regulations and compliance requirements rarely or never. This indicates a potential gap in training programs, which are crucial for keeping staff informed and compliant with regulations.

Regarding confidence in their organization's ability to comply with AML/CTF regulations, while the majority of participants (86.6%) reported being at least slightly confident, there is still a notable percentage (60.8%) who are not confident at all or only slightly confident. This suggests that there may be areas where organizations need to improve their compliance processes to enhance confidence levels. The effectiveness of internal controls for ensuring compliance with AML/CTF regulations also raises some concerns, with 67.1% of participants reporting that the controls are not effective at all or only slightly effective. This indicates a need for organizations to review and strengthen their internal control mechanisms to ensure full compliance with regulations. In terms of the transparency of the reporting process for AML/CTF compliance issues, the majority of participants (66.1%) reported that the process is only slightly transparent or not transparent at all. This suggests that there may be issues with the reporting process that need to be addressed to improve transparency and accountability within organizations.

Table 4.3: Compliance with AML/CTF regulations

Statements	Frequency	Percentage
How familiar are you with the current AML/CTF regulations applicable to your organization?		
Not Familiar at all	56	14.0
Slightly Familiar	172	43.0
Moderately Familiar	104	26.0
Very Familiar	44	11.0
Extremely Familiar	24	6.0
How often do you receive training on AML/CTF regulations and compliance requirements?		
Never	67	16.8
Rarely	210	52.5
Occasionally	67	16.8
Often	36	9.0
Very Often	20	5.0
How confident are you in your organization's ability to comply with AML/CTF regulations?		
Not Confident at all	54	13.5
Slightly Confident	189	47.3

Moderately Confident	92	23.0
Very Confident	37	9.3
Extremely Confident	28	7.0
How effective are the internal controls in place to ensure compliance with AML/CTF regulations?		
Not Effective At all	83	20.8
Slightly Effective	185	46.3
Moderately Effective	69	17.3
Very Effective	40	10.0
Extremely Effective	23	5.8
How transparent is your organization's reporting process for AML/CTF compliance issues?		
Not Transparent At all	101	25.3
Slightly Transparent	163	40.8
Moderately Transparent	68	17.0
Very Transparent	48	12.0
Extremely Transparent	20	5.0

Table 4.4 presents the descriptive results for the variable "Integration level of cybersecurity in AML/CTF operations", providing insights into how cybersecurity measures are integrated into organizations' AML/CTF policies and procedures, how cybersecurity risks are considered in the development of AML/CTF strategies, how effectively cybersecurity controls are implemented, how often cybersecurity incidents are reported and investigated, and the collaborative relationship between cybersecurity and AML/CTF teams. The data indicates that there is room for improvement in several areas. A significant proportion of participants (68.1%) reported that cybersecurity measures are either not integrated at all or only slightly integrated into their organization's AML/CTF policies and procedures. This suggests that there may be a need for organizations to enhance the integration of cybersecurity measures to better protect against cyber threats.

In terms of the consideration of cybersecurity risks in the development of AML/CTF strategies, a majority of participants (71.1%) reported that cybersecurity risks are rarely or never considered. This indicates a potential gap in risk assessment processes, which are crucial for identifying and mitigating cybersecurity threats. Regarding the effectiveness of cybersecurity controls, while a majority of participants (83.8%) reported that controls are at least slightly effective, there is still a notable percentage (70.3%) who indicated that controls are not effective at all or only slightly effective. This suggests that there may be areas where organizations need to improve their cybersecurity controls to better protect against cyber threats. The frequency of reporting and investigating cybersecurity incidents in relation to AML/CTF activities also raises some concerns, with 80.3% of participants reporting that incidents are rarely or never reported and investigated. This indicates a potential gap in incident response processes, which are crucial for addressing and mitigating the impact of cybersecurity incidents. Regarding the collaborative relationship between cybersecurity and AML/CTF teams, the minority of participants (43.3%) reported that the relationship is at least moderately collaborative. A notable percentage (56.7%) of participants indicated that the relationship is not collaborative at all or only slightly collaborative. This suggests that there may be opportunities for organizations to improve collaboration between teams to enhance cybersecurity measures and protect against cyber threats.

Table 4.4: Integration level of cybersecurity in AML/CTF operations

	Frequency	Percentage
How well are cybersecurity measures integrated into your organization's AML/CTF policies and procedures?		
Not Integrated At all	79	19.8
Slightly Integrated	193	48.3
Moderately Integrated	73	18.3
Very Integrated	40	10.0
Extremely Integrated	15	3.8

How frequently are cybersecurity risks considered in the development of AML/CTF strategies?		
Never	97	24.3
Rarely	187	46.8
Occasionally	84	21.0
Often	27	6.8
Very Often	5	1.3
How effectively are cybersecurity controls implemented to protect AML/CTF data and systems?		
Not Effective At all	65	16.3
Slightly Effective	216	54.0
Moderately Effective	97	24.3
Very Effective	18	4.5
Extremely Effective	4	1.0
How often are cybersecurity incidents reported and investigated in relation to AML/CTF activities?		
Never	81	20.3
Rarely	240	60.0
Occasionally	67	16.8
Often	8	2.0
Very Often	4	1.0
How collaborative is the relationship between cybersecurity and AML/CTF teams in your organization?		
Not Collaborative At all	69	17.3
Slightly Collaborative	158	39.5
Moderately Collaborative	135	33.8
Very Collaborative	30	7.5
Extremely Collaborative	8	2.0

Table 4.5 presents the descriptive statistics for the variable "Perception of the importance of cybersecurity in AML/CTF", revealing important insights into how participants perceive the role of cybersecurity in their organization's AML/CTF strategies. The majority of participants (83.1%) believe that cybersecurity is at least slightly important in ensuring the effectiveness of AML/CTF strategies, with 13.3% considering it very to extremely important. This indicates a strong recognition of the role of cybersecurity in supporting the effectiveness of AML/CTF efforts. However, the fact that 17% perceive it as not important at all or only slightly important suggests that there may be a subset of participants who do not fully appreciate the importance of cybersecurity in AML/CTF. Regarding the alignment of cybersecurity measures with the goals of AML/CTF efforts, a majority of participants (78.4%) perceive at least some level of alignment, with 6.3% considering it very to extremely aligned. This indicates that, overall, there is a perception of alignment between cybersecurity measures and AML/CTF goals. However, the fact that 21.8% perceive no alignment or only slight alignment suggests that there may be room for improvement in ensuring that cybersecurity measures are closely aligned with AML/CTF goals.

Participants' awareness of potential cybersecurity threats facing their organization's AML/CTF activities is also noteworthy, with 75.2% reporting at least some awareness and 10.7% considering themselves very to extremely aware. This indicates a generally high level of awareness of cybersecurity threats, which is crucial for effectively mitigating risks. In terms of the emphasis placed on cybersecurity training and awareness for AML/CTF staff, the majority of participants (75.4%) reported at least some emphasis, with 6.8% indicating a very high emphasis. This suggests that organizations recognize the importance of training and awareness in enhancing cybersecurity measures for AML/CTF activities. Regarding satisfaction with the current level of cybersecurity integration in their organization's AML/CTF activities, the descriptive statistics show a mixed perception among participants. While the majority of participants (87.4%) reported at least some level of satisfaction, with 47.6% being moderately to extremely satisfied, 12.8% are not satisfied at all. This is where participants feel that cybersecurity integration could be improved in their organization's AML/CTF activities. The fact that a significant

number of participants (39.8%) reported only slight satisfaction suggests that there may be room for enhancement in cybersecurity integration to meet the expectations and needs of stakeholders.

Table 4.5: Perception of the importance of cybersecurity in AML/CTF

Statement	Frequency	Percentage
How important do you believe cybersecurity is in ensuring the effectiveness of AML/CTF strategies?		
Not Important At all	68	17.0
Slightly Important	218	54.5
Moderately Important	61	15.3
Very Important	45	11.3
Extremely Important	8	2.0
How well do you think cybersecurity measures align with the goals of AML/CTF efforts in your organization?		
Not Aligned At all	87	21.8
Slightly Aligned	221	55.3
Moderately Aligned	67	16.8
Very Aligned	19	4.8
Extremely Aligned	6	1.5
How aware are you of the potential cybersecurity threats facing your organization's AML/CTF activities?		
Not Aware At all	99	24.8
Slightly Aware	202	50.5
Moderately Aware	56	14.0
Very Aware	29	7.2
Extremely Aware	14	3.5
How much emphasis does your organization place on cybersecurity training and awareness for AML/CTF staff?		
No Emphasis At all	99	24.8
Slightly Emphasis	237	59.3
Moderately Emphasis	37	9.3
High Emphasis	16	4.0
Very High Emphasis	11	2.8
How satisfied are you with the current level of cybersecurity integration in your organization's AML/CTF activities?		
No Satisfied At all	51	12.8
Slightly Satisfied	159	39.8
Moderately Satisfied	117	29.3
Very Satisfied	53	13.3
Extremely Satisfied	20	5.0

4.3 Inferential Statistics

Objective 1: To assess the current state of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies by measuring the effectiveness of current AML/CTF strategies and compliance with AML/CTF regulations.

Table 4.6: Correlations

		Effective	Compliance
Effective	Pearson Correlation	1	.111*
	Sig. (2-tailed)		.026
	N	400	400
Compliance	Pearson Correlation	.111*	1
	Sig. (2-tailed)	.026	
	N	400	400
*. Correlation is significant at the 0.05 level (2-tailed).			

Novelty Journals

ISSN 2394-7322

International Journal of Novel Research in Marketing Management and Economics
Vol. 11, Issue 1, pp: (180-196), Month: January - April 2024, Available at: www.noveltyjournals.com

The correlation analysis presented in Table 4.6 shows a significant positive correlation (r = 0.111, p = 0.026) between the effectiveness of AML/CTF strategies and compliance with AML/CTF regulations. This implies that as the effectiveness of strategies to detect and prevent money laundering and terrorist financing activities increases, so does compliance with regulations. This finding is important as it suggests that organizations with more effective AML/CTF strategies are more likely to comply with regulations, which is crucial for combating financial crimes.

Objective 2: To evaluate the integration of cybersecurity measures in AML and CTF strategies by assessing the integration level of cybersecurity in AML/CTF operations and the perception of the importance of cybersecurity in AML/CTF.

Table 4.7: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.220[a]	.049	.046	.39649

a. Predictors: (Constant), Perception

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.197	1	3.197	20.337	.000[b]
	Residual	62.567	398	.157		
	Total	65.764	399			

a. Dependent Variable: Integration

b. Predictors: (Constant), Perception

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.974	.182		16.332	.000
	Perception	.216	.048	.220	4.510	.000

a. Dependent Variable: Integration

The regression analysis in Tables 4.7 indicates that the perception variable has a significant impact on the integration of cybersecurity measures in AML/CTF policies and procedures ($\beta = 0.220$, $p < 0.001$). The R-squared value of 0.049 suggests that about 4.9% of the variance in integration can be explained by the perception variable. The ANOVA results show that the regression model is significant ($F = 20.337$, $p < 0.001$), indicating that the perception variable is a statistically significant predictor of integration. Overall, the results suggest that a positive perception of the importance of cybersecurity is associated with a higher level of integration in AML/CTF operations. The coefficient for the Perception of the importance of cybersecurity in AML/CTF in the regression analysis is 0.216. This means that for every one-unit increase in the Perception of the importance of cybersecurity in AML/CTF, we would expect an increase of 0.216 units in the Integration level of cybersecurity measures in AML/CTF, holding all other variables constant.

Objective 3: To investigate the impact of integrated cybersecurity and compliance measures on AML and CTF effectiveness by examining the relationship between AML/CTF effectiveness, integration level of cybersecurity measures in AML/CTF, and compliance with AML/CTF regulations

Table 4.8: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.157[a]	.025	.017	.42344

a. Predictors: (Constant), Compliance, Perception, Integration

The R-value (0.157) in Table 4.8 indicates a weak positive correlation between the predictors (Compliance, Perception, Integration) and the Effective variable. R Square (0.025) shows that only 2.5% of the variance in effectiveness is explained by the predictors.

Novelty Journals

ISSN 2394-7322

International Journal of Novel Research in Marketing Management and Economics
Vol. 11, Issue 1, pp: (180-196), Month: January - April 2024, Available at: www.noveltyjournals.com

Table 4.9: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.793	3	.598	3.333	.020[b]
	Residual	71.004	396	.179		
	Total	72.796	399			
a. Dependent Variable: Effective						
b. Predictors: (Constant), Compliance, Perception, Integration						

The F-statistic (3.333) in Table 4.9 is used to test the overall significance of the regression model. It compares the variance explained by the model to the variance not explained. The p-value (0.020) indicates whether the regression model is statistically significant. Here, the p-value is less than 0.05, suggesting that the model is significant.

Table 4.10: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.725	.312		8.726	.000
	Perception	-.015	.052	-.015	-.295	.768
	Integration	.120	.054	.114	2.227	.026
	Compliance	.105	.043	.123	2.452	.015
a. Dependent Variable: Effectiveness						

The regression analysis in Table 4.10 indicates that the overall model includes compliance, perception, and integration as predictors of the effectiveness of AML/CTF. The coefficient for Perception (-0.015) indicates that for a one-unit increase in Perception, there is a decrease of 0.015 units in the Effectiveness of AML/CTF. However, this effect is not statistically significant (p = 0.768). The coefficient for Integration (0.120) indicates that for a one-unit increase in Integration, there is an increase of 0.120 units in the Effectiveness of AML/CTF, and this effect is statistically significant (p = 0.026). The coefficient for Compliance (0.105) indicates that for a one-unit increase in Compliance, there is an increase of 0.105 units in the Effectiveness of AML/CTF, and this effect is statistically significant (p = 0.015).

5. CRITICAL DISCUSSION

The finding from this research that there is a significant positive correlation between the effectiveness of AML/CTF strategies and compliance with AML/CTF regulations is supported by various academic journal sources. This relationship is crucial in understanding how effective strategies can lead to better regulatory compliance, ultimately aiding in combating financial crimes. The finding that effective AML/CTF strategies are positively correlated with compliance with AML/CTF regulations is supported by existing literature (Manning, Wong and Jevtovic, 2020). A study by Gaviyau and Sibindi (2023) emphasizes the importance of effective AML policies in ensuring compliance with regulations. The study highlights that robust AML strategies, including strong internal controls and risk assessment mechanisms, are essential for meeting regulatory requirements. This aligns with the finding that effective AML/CTF strategies are positively correlated with compliance. Furthermore, research by Manning, Wong and Jevtovic (2020) suggests that the effectiveness of AML measures can influence the level of compliance within financial institutions. They argue that when institutions perceive AML measures as effective in detecting and preventing money laundering, they are more likely to comply with regulations. This supports the idea that effective strategies can lead to increased compliance.

However, the strength and causality of the correlation relationship warrant further investigation to fully understand the dynamics between strategy effectiveness and regulatory compliance in combating financial crimes. It is important to note that while this finding is supported by academic literature, the correlation coefficient of 0.111 indicates a relatively weak relationship. This suggests that while there is a positive association between effectiveness and compliance, other factors may also influence compliance levels. Additionally, the research does not establish a causal relationship between effectiveness and compliance as correlation is not proof of causation (Macnish, 2021; Negri, 2023). It is possible that organizations with a strong commitment to compliance are more likely to implement effective AML/CTF strategies, rather

than the strategies themselves directly leading to compliance. Further research using longitudinal or experimental designs could provide more insight into the causal nature of this relationship.

The finding that a positive perception of the importance of cybersecurity is associated with a higher level of integration in AML/CTF operations is consistent with several academic studies (Lessambo, 2023a). Uchendu et al. (2021) examined the relationship between organizational culture and cybersecurity practices. They found that organizations that prioritize cybersecurity as an integral part of their culture are more likely to have comprehensive cybersecurity measures in place, including integration with other operational areas such as AML/CTF strategies. This supports the notion that perception plays a significant role in determining the level of integration of cybersecurity measures. Additionally, a study by Hasani et al. (2023) focused on the importance of top management support for cybersecurity initiatives. They found that organizations where top management perceives cybersecurity as a strategic priority are more likely to integrate cybersecurity measures across different operational functions, including AML/CTF strategies. Another paper by Oroni and Xianping (2023) underscores Cyber Security Awareness's multidimensional nature, involving technical and psychological elements, and the role of managerial support in bolstering an organization's cybersecurity posture. This finding aligns with the idea that perception, particularly at the leadership level, can drive the integration of cybersecurity measures.

However, it is important to note that perception alone may not be sufficient to ensure effective integration of cybersecurity measures (Marotta and Madnick, 2020; Savaş and Karataş, 2022). Other factors, such as organizational structure, resource allocation, and regulatory requirements, also play a significant role. For example, a study by Marotta and Madnick (2021) highlighted the importance of regulatory pressures in driving organizations to integrate cybersecurity measures into their operations. This suggests that while perception is important, it needs to be supported by a holistic approach that considers various organizational and external factors. Therefore, it is important for organizations to consider a range of factors beyond perception to ensure effective integration of cybersecurity measures.

The finding regarding the impact of integrated cybersecurity and compliance measures on AML/CTF effectiveness, as indicated by the regression analysis, suggests that while compliance and integration of cybersecurity measures have a statistically significant positive impact on AML/CTF effectiveness, perception does not show a significant impact. However, the finding regarding perception not showing a significant impact on AML/CTF effectiveness contrasts with some studies that emphasize the role of perception in driving organizational behaviour (FATF, 2021) (Jeong et al., 2021). Moreover, a study by Willie (2023) highlighted the importance of perception in shaping organizational culture and practices related to cybersecurity. The study found that organizations where employees perceive cybersecurity as important are more likely to have robust cybersecurity measures in place.

This finding aligns with existing literature that emphasizes the importance of compliance and integration in enhancing AML/CTF effectiveness. For example, a study by Lessambo (2023a) found that organizations with integrated cybersecurity and compliance measures were better able to detect and prevent financial crimes. The study highlighted the importance of a holistic approach that combines compliance with regulatory requirements and effective integration of cybersecurity measures. Similarly, a study by Manning, Wong and Jevtovic (2020) focused on the relationship between compliance and AML/CTF effectiveness. They found that organizations that prioritize compliance with AML/CTF regulations are more effective in combating money laundering and terrorist financing. This supports the idea that compliance plays a crucial role in enhancing AML/CTF effectiveness.

The earlier theoretical review of systems theory, risk management frameworks, social network theory, and the technology acceptance model (TAM) provides a comprehensive framework for understanding the integration of cybersecurity measures into Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies. These theoretical perspectives offer valuable insights into the interconnectedness of various components, the management of risks, the role of social networks, and the acceptance of technology in this context. The findings of the study align with these theoretical perspectives in several ways. Firstly, the study emphasizes the importance of an integrated approach to AML and CTF strategies, which is in line with the holistic view of systems theory (Gupta, Dwivedi and Shah, 2023). Systems theory's emphasis on understanding the ripple effects of changes and the dynamic relationships between technological advancements, regulatory requirements, and organizational practices resonates with the study's findings on the impact of integrated cybersecurity measures on AML and CTF effectiveness.

Secondly, the study's focus on risk management aligns with the use of risk management frameworks such as COSO ERM (Marquez-Tejon, Jimenez-Partearroyo and Benito-Osorio, 2021). The study's findings on the positive impact of compliance and integration on AML/CTF effectiveness reflect the risk management approach of identifying, assessing, and responding to risks in the integration of cybersecurity measures (Marquez-Tejon, Partearroyo and Benito-Osorio, 2023). Thirdly, the study's consideration of perception and integration in AML/CTF operations corresponds to the insights provided by social network theory (Carley, 2020). Social network theory's emphasis on relationships and information flows among stakeholders is reflected in the study's findings on the importance of perception and integration in driving AML/CTF effectiveness. Finally, the use of the TAM to analyze the acceptance of cybersecurity measures within financial institutions aligns with TAM's focus on individual perceptions of technology adoption (Davis, Bagozzi and Warshaw, 1989). The study's findings on the significance of perception in driving integration efforts resonate with TAM's emphasis on perceived ease of use and usefulness in technology adoption.

6. CONCLUSION

The research findings provide valuable insights into the current state of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) strategies, the integration of cybersecurity measures in these strategies, and their impact on effectiveness. Firstly, the study revealed a significant positive correlation between the effectiveness of AML/CTF strategies and compliance with AML/CTF regulations. This indicates that organizations with more effective strategies are more likely to comply with regulations, which is crucial for combating financial crimes. While this finding is supported by existing literature, the relatively weak correlation suggests that other factors may also influence compliance levels, highlighting the need for further research to understand the dynamics between strategy effectiveness and regulatory compliance. Secondly, the research demonstrated that a positive perception of the importance of cybersecurity is associated with a higher level of integration in AML/CTF operations. This finding underscores the role of perception, particularly at the leadership level, in driving the integration of cybersecurity measures. However, it is important to note that perception alone may not be sufficient, and other factors such as organizational structure and resource allocation also play a significant role in effective integration. Lastly, the study showed that while compliance and integration of cybersecurity measures have a positive impact on AML/CTF effectiveness, perception does not show a significant impact. This finding contrasts with some studies that emphasize the role of perception in driving organizational behavior related to cybersecurity. Further research is needed to explore the causal relationships between these factors and AML/CTF effectiveness.

Future research in this area could explore several important directions to further enhance the industry understanding of AML and CTF strategies and their effectiveness. Some potential future research directions include:

1. **Qualitative Studies:** Conduct qualitative studies to explore the underlying reasons behind the observed correlations and relationships. This could involve interviews or focus groups with stakeholders to understand their perceptions, motivations, and challenges related to AML/CTF strategies and cybersecurity integration.

2. **Comparative Studies:** Compare AML/CTF strategies and cybersecurity integration practices across different industries, regions, or organizational sizes. This could help identify best practices and lessons learned that could be applied in other contexts.

3. **Impact of Technology:** Investigate the impact of emerging technologies such as artificial intelligence, blockchain, and big data analytics on AML/CTF strategies and effectiveness. This could help identify new approaches and tools to enhance AML/CTF efforts.

4. **Regulatory Environment:** Examine the role of the regulatory environment in shaping AML/CTF strategies and compliance levels. This could include studying the impact of regulatory changes on organizational practices and effectiveness.

5. **Organizational Culture:** Explore the role of organizational culture in driving AML/CTF strategies and cybersecurity integration. This could involve assessing the influence of leadership, communication, and employee attitudes towards compliance and cybersecurity.

6. **Cross-Disciplinary Research:** Foster collaboration between researchers from different disciplines such as law, criminology, cybersecurity, and business to bring diverse perspectives to the study of AML/CTF strategies and effectiveness.

REFERENCES

[1] Akartuna, E.A., Johnson, S.D. and Thornton, A.E. (2022). The Money Laundering and Terrorist Financing Risks of New and Disruptive technologies: a futures-oriented Scoping Review. *Security Journal*. doi:https://doi.org/10.1057/s41284-022-00356-z.

[2] Alhajeri, R. and Alhashem, A. (2023). Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management*, [online] 15(4), pp.284–305. doi:https://doi.org/10.4236/iim.2023.154014.

[3] Andrade, C. (2020). Sample Size and Its Importance in Research. *Indian Journal of Psychological Medicine*, [online] 42(1), pp.102–103. doi:https://doi.org/10.4103/IJPSYM.IJPSYM_504_19.

[4] Aschi, M., Bonura, S., Masi, N., Messina, D. and Profeta, D. (2022). Cybersecurity and Fraud Detection in Financial Transactions. *Big Data and Artificial Intelligence in Digital Finance*, pp.269–278. doi:https://doi.org/10.1007/978-3-030-94590-9_15.

[5] Ash Siddiqi, H.I., Darwiyanto, E. and Priyadi, Y. (2023). IT Risk Management Analysis on Bank Xyz E-Banking Service System Using Iso 31000. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 8(1), pp.211–217. doi:https://doi.org/10.29100/jipi.v8i1.3325.

[6] Carley, K.M. (2020). Social cybersecurity: an Emerging Science. *Computational and Mathematical Organization Theory*, [online] 26(4), pp.365–381. doi:https://doi.org/10.1007/s10588-020-09322-9.

[7] Cavus, N., Omonayajo, B. and Mutizwa, M.R. (2022). Technology Acceptance Model and Learning Management Systems: Systematic Literature Review. *International Journal of Interactive Mobile Technologies (iJIM)*, 16(23), pp.109–124. doi:https://doi.org/10.3991/ijim.v16i23.36223.

[8] Chikouche, S., Bouziane, A., Bouhouita-Guermech, S.E., Mostefai, M. and Gouffi, M. (2018). Innovation Diffusion in Social Networks: a Survey. *IFIP advances in information and communication technology*, pp.173–184. doi:https://doi.org/10.1007/978-3-319-89743-1_16.

[9] Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, [online] 47(3). doi:https://doi.org/10.1057/s41288-022-00266-6.

[10] Crotty, J. and Daniel, E. (2022). Cyber threat: Its Origins and Consequence and the Use of Qualitative and Quantitative Methods in Cyber Risk Assessment. *Applied Computing and Informatics*. doi:https://doi.org/10.1108/aci-07-2022-0178.

[11] Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989). User Acceptance of Computer Technology: a Comparison of Two Theoretical Models. *Management Science*, 35(8), pp.982–1003. doi:https://doi.org/10.1287/mnsc.35.8.982.

[12] Dupont, B. (2019). The cyber-resilience of Financial institutions: Significance and Applicability. *Journal of Cybersecurity*, [online] 5(1). doi:https://doi.org/10.1093/cybsec/tyz013.

[13] El Hajj, M. and Hammoud, J. (2023). Unveiling the Influence of Artificial Intelligence and Machine Learning on Financial Markets: a Comprehensive Analysis of AI Applications in Trading, Risk Management, and Financial Operations. *Journal of Risk and Financial Management*, [online] 16(10), p.434. doi:https://doi.org/10.3390/jrfm16100434.

[14] Etikan, I., Musa, S.A. and Alkassim, R.S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, [online] 5(1), pp.1–4. doi:https://doi.org/10.11648/j.ajtas.20160501.11.

[15] FATF (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf.

[16] Gaviyau, W. and Sibindi, A.B. (2023). Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: a Critique. *FinTech, Blockchain and Cryptocurrencies*, 16(Special Issue 7), pp.313–313. doi:https://doi.org/10.3390/jrfm16070313.

[17] Gupta, A., Dwivedi, D.N. and Shah, J. (2023). Financial Crimes Management and Control in Financial Institutions. *Future of Business and Finance*, pp.13–24. doi:https://doi.org/10.1007/978-981-99-2571-1_2.

[18] Han, J., Huang, Y., Liu, S. and Towey, K. (2020). Artificial Intelligence for anti-money laundering: a Review and Extension. *Digital Finance*, 2(3-4), pp.211–239. doi:https://doi.org/10.1007/s42521-020-00023-1.

[19] Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D. and Levallet, N. (2023). Evaluating the Adoption of Cybersecurity and Its Influence on Organizational Performance. *SN Business & Economics*, 3(5). doi:https://doi.org/10.1007/s43546-023-00477-6.

[20] Israel, G.D. (1992). *Determining Sample Size 1*. [online] Agricultural Education and Communication Department, Florida Cooperative Extension Service, Institute of Food and Agricultural Sciences, University of Florida. Available at: https://www.psycholosphere.com/Determining%20sample%20size%20by%20Glen%20Israel.pdf.

[21] Jarjoui, S. and Murimi, R. (2021). A Framework for Enterprise Cybersecurity Risk Management. *Advances in Cybersecurity Management*, pp.139–161. doi:https://doi.org/10.1007/978-3-030-71381-2_8.

[22] Jeong, J.J., Oliver, G., Kang, E., Creese, S. and Thomas, P. (2021). The Current State of Research on people, Culture and Cybersecurity. *Personal and Ubiquitous Computing*. doi:https://doi.org/10.1007/s00779-021-01591-8.

[23] Karanikas, N. and Zerguine, H. (2024). Are the New Safety Paradigms (only) about Safety and Sufficient to Ensure it? an Overview and Critical Commentary. *Safety Science*, 170, pp.106367–106367. doi:https://doi.org/10.1016/j.ssci.2023.106367.

[24] Kaur, G., Habibi Lashkari, Z. and Habibi Lashkari, A. (2021). Cybersecurity Threats in FinTech. *Understanding Cybersecurity Management in FinTech*, pp.65–87. doi:https://doi.org/10.1007/978-3-030-79915-1_4.

[25] Khan, A. and Malaika, M. (2021). Central Bank Risk Management, Fintech, and Cybersecurity. *IMF Working Papers*, 2021(105), p.1. doi:https://doi.org/10.5089/9781513582344.001.

[26] Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H. and Vasilyeva, T. (2022). Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*, 15(12), p.613. doi:https://doi.org/10.3390/jrfm15120613.

[27] Lessambo, F.I. (2023a). AML and Cybersecurity in Banking Industry: Challenges. *Palgrave Macmillan studies in banking and financial institutions*, pp.49–55. doi:https://doi.org/10.1007/978-3-031-23484-2_4.

[28] Lessambo, F.I. (2023b). *Anti-Money Laundering, Counter Financing Terrorism and Cybersecurity in the Banking Industry*. doi:https://doi.org/10.1007/978-3-031-23484-2.

[29] Macnish, K. (2021). Taking Shortcuts: Correlation, Not Causation, and the Moral Problems It Brings. *Advances in Research Ethics and Integrity*, 08, pp.55–70. doi:https://doi.org/10.1108/s2398-601820210000008006.

[30] Manning, M., Wong, G.T.W. and Jevtovic, N. (2020). Investigating the Relationships between FATF Recommendation compliance, Regulatory Affiliations and the Basel Anti-Money Laundering Index. *Security Journal*, 34(3), pp.566–588. doi:https://doi.org/10.1057/s41284-020-00249-z.

[31] Marangunić, N. and Granić, A. (2014). Technology Acceptance model: a Literature Review from 1986 to 2013. *Universal Access in the Information Society*, 14(1), pp.81–95.

[32] Marotta, A. and Madnick, S. (2021). Tackling Cybersecurity Regulatory Challenges: A Proposed Research Framework. *The Role of e-Business during the Time of Grand Challenges*, pp.12–24. doi:https://doi.org/10.1007/978-3-030-79454-5_2.

[33] Marotta, A. and Madnick, S.E. (2020). Analyzing the Interplay Between Regulatory Compliance and Cybersecurity. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.3542563.

[34] Marquez-Tejon, J., Jimenez-Partearroyo, M. and Benito-Osorio, D. (2021). Security as a Key Contributor to Organisational resilience: a Bibliometric Analysis of Enterprise Security Risk Management. *Security Journal*. doi:https://doi.org/10.1057/s41284-021-00292-4.

[35] Marquez-Tejon, J., Partearroyo, M.J. and Benito-Osorio, D. (2023). Integrated Security Management model: a Proposal Applied to Organisational Resilience. doi:https://doi.org/10.1057/s41284-023-00381-6.

[36] Mishra, A., Alzoubi, Y.I., Anwar, M.J. and Gill, A.Q. (2022). Attributes Impacting Cybersecurity Policy development: an Evidence from Seven Nations. *Computers & Security*, [online] 120(1), p.102820. doi:https://doi.org/10.1016/j.cose.2022.102820.

[37] Muijs, D., West, M. and Ainscow, M. (2010). Why network? Theoretical Perspectives on Networking. *School Effectiveness and School Improvement*, 21(1), pp.5–26. doi:https://doi.org/10.1080/09243450903569692.

[38] Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B.A. and Hawa, S. (2023). Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem. *International Journal of Interactive Mobile Technologies*, 17(22), pp.100–116. doi:https://doi.org/10.3991/ijim.v17i22.45261.

[39] Negri, F. (2023). Correlation Is Not Causation, Yet… Matching and Weighting for Better Counterfactuals. *In: Damonte, A., Negri, F. (eds) Causality in Policy Studies. Texts in Quantitative Political Analysis. Springer, Cham.*, pp.71–98. doi:https://doi.org/10.1007/978-3-031-12982-7_4.

[40] Newton, P.M. (2023). Design, Run, and Interpret Survey-Based Research in the Fields of Academic Integrity and Misconduct. *In: Eaton, S.E. (eds) Handbook of Academic Integrity. Springer, Singapore.*, pp.1–18. doi:https://doi.org/10.1007/978-981-287-079-7_182-1.

[41] Oroni, C.Z. and Xianping, F. (2023). Structural Evaluation of Management Capability and the Mediation Role of Cybersecurity Awareness Towards Enterprise Performance. *Journal of Data, Information and Management*, 5(4), pp.345–361. doi:https://doi.org/10.1007/s42488-023-00108-7.

[42] Osei, L.K., Cherkasova, Y. and Oware, K.M. (2023). Unlocking the Full Potential of Digital Transformation in banking: a Bibliometric Review and Emerging Trend. *Future Business Journal*, 9(1). doi:https://doi.org/10.1186/s43093-023-00207-2.

[43] Parker, M.A. (2019). Social Network Theory. *Springer eBooks*, pp.1–4. doi:https://doi.org/10.1007/978-3-319-31816-5_2765-1.

[44] Pattnaik, D., Ray, S. and Raman, R. (2024). Applications of Artificial Intelligence and Machine Learning in the Financial Services industry: a Bibliometric Review. *Heliyon*, [online] 10(1), p.e23492. doi:https://doi.org/10.1016/j.heliyon.2023.e23492.

[45] Ryan, G. (2018). Introduction to positivism, Interpretivism and Critical Theory. *Nurse Researcher*, [online] 25(4), pp.41–49. doi:https://doi.org/10.7748/nr.2018.e1466.

[46] Savaş, S. and Karataş, S. (2022). Cyber Governance Studies in Ensuring cybersecurity: an Overview of Cybersecurity Governance. *International Cybersecurity Law Review*, 3(1). doi:https://doi.org/10.1365/s43439-021-00045-4.

[47] Teichmann, F.M.J. (2020). Current Developments in Money Laundering and Terrorism Financing. *Journal of Money Laundering Control*, ahead-of-print(ahead-of-print). doi:https://doi.org/10.1108/jmlc-05-2019-0043.

[48] Turner, J.R. and Baker, R.M. (2019). Complexity Theory: An Overview with Potential Applications for the Social Sciences. *Systems*, [online] 7(1), p.4. doi:https://doi.org/10.3390/systems7010004.

[49] Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S. (2021). Developing a Cyber Security culture: Current Practices and Future Needs. *Computers & Security*, 109, p.102387. doi:https://doi.org/10.1016/j.cose.2021.102387.

[50] Uddin, Md.H., Ali, Md.H. and Hassan, M.K. (2020). Cybersecurity Hazards and Financial System vulnerability: A Synthesis of Literature. *Risk Management*, 22, pp.239–309. doi:https://doi.org/10.1057/s41283-020-00063-2.

[51] Ursavaş, Ö.F. (2022). Technology Acceptance Model: History, Theory, and Application. *Springer Texts in Education*, pp.57–91. doi:https://doi.org/10.1007/978-3-031-10846-4_4.

[52] Willie, M.M. (2023). *The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture*. [online] Social Science Research Network. doi:https://doi.org/10.2139/ssrn.4564291.