Framing Digital Compliance Cultures: A Qualitative Conceptual Analysis of Institutional Readiness in AML Governance

Zahari Bin Md Rodzi

Faculty of Computer Science and Mathematics Universiti Teknologi MARA Cawangan Negeri Sembilan, Malaysia

Khairul Anuar Bin Abdul Hadi

Faculty of Law, Universiti Teknologi MARA Cawangan Pahang, Malaysia

Nur Aima Binti Shafie*

Accounting Research Institute, Universiti Teknologi MARA, Malaysia

Mohd Taufik Bin Mohd Suffian

Faculty of Accountancy, Universiti Teknologi MARA Cawangan Perak, Malaysia

Nurul Mohammad Zayed

Daffodil International University, Dhaka, Bangladesh

Abstract

This paper explores how institutional readiness for anti-money laundering (AML) digital compliance is shaped not solely by technological infrastructure, but by organizational culture, leadership framing, and interpretive regulatory engagement. Drawing on institutional theory, organizational culture theory, and the Technology-Organisation-Environment (TOE) framework, the study offers a qualitative conceptual analysis that reframes digital transformation in AML governance as a cultural shift rather than a purely technical upgrade. While financial institutions are increasingly urged to adopt Regulatory Technology (RegTech) tools, implementation remains uneven, particularly in developing markets. Thematic findings suggest that compliance is often performed symbolically rather than substantively, with leadership playing a pivotal role in framing legitimacy and encouraging adoption. Regulatory ambiguity further complicates institutional response, requiring culturally embedded interpretation. The paper argues that trust, both technical and relational, is critical to organizational readiness, and that digital compliance success hinges on participatory processes and leadership-driven narratives. This study contributes to the literature by emphasizing the socio-institutional dimensions of digital AML compliance and calls for

regulators to go beyond policy issuance by fostering capacity-building and cultural alignment. It concludes that meaningful AML governance demands a rethinking of risk, compliance, and responsibility in the context of evolving digital ecosystems.

Keywords: Digital Compliance, AML Governance, Institutional Readiness, Compliance Culture, Qualitative Analysis

Introduction

In an era marked by increasingly sophisticated financial crimes and complex international transactions, the transformation of anti-money laundering (AML) governance has become a central pillar in the global financial regulatory agenda. Money laundering schemes have become more intricate, exploiting cross-border digital platforms, decentralized finance (DeFi), virtual assets, and digital payment systems to conceal illicit gains. The pressure on financial institutions to detect and prevent such activities has intensified in parallel with the technological evolution of financial services. Traditional compliance mechanisms, which often rely on manual processes, human judgment, static reporting, and siloed data structures, have shown limitations in dealing with real-time, complex, and high-volume transactional environments. These conventional systems, while once adequate, are increasingly incapable of keeping pace with the scale and speed of modern financial threats.

In response, regulators and international bodies such as the Financial Action Task Force (FATF), Bank Negara Malaysia (BNM), the European Banking Authority (EBA), and the Basel Committee on Banking Supervision have begun promoting more dynamic, data-driven, and automated compliance strategies. Central to this shift is the adoption of Regulatory Technology (RegTech), which leverages artificial intelligence (AI), machine learning, blockchain, and big data analytics to enhance the effectiveness, efficiency, and responsiveness of AML frameworks.

However, while technological capability and regulatory pressure are essential, the effectiveness of RegTech adoption is also deeply influenced by institutional culture, regulatory clarity, and internal leadership. For instance, in the United Kingdom, the Financial Conduct Authority (FCA) has actively supported RegTech innovation through its Regulatory Sandbox, introduced in 2016, allowing financial institutions to test and integrate new compliance technologies in a supervised and controlled environment (FCA, 2022). This has fostered a culture of innovation and experimentation, encouraging institutions to frame digital AML not merely as compliance, but as a driver of competitive advantage. British banks have demonstrated greater integration of real-time monitoring tools and AI-based transaction surveillance because the regulatory environment promotes trust, controlled risk-taking, and shared learning.

In contrast, Singapore, while globally recognized for its robust and stable financial ecosystem, has taken a more prescriptive and top-down approach. The Monetary Authority of Singapore (MAS) has issued detailed guidelines such as the "MAS Notice 626" and continues to update its Technology Risk Management Guidelines, most recently in 2021 (MAS, 2021). These guidelines reflect a disciplined regulatory tone that promotes compliance excellence, yet in practice may limit the speed or scope of innovation due to institutional caution. Compliance officers in Singaporean banks often view digital systems as high-stakes instruments meant to

fulfill detailed regulatory expectations rather than as flexible platforms for adaptive governance.

These two examples illustrate the central thesis of this paper: the adoption of digital AML technology is not solely a technical or policy process, but one that is shaped and conditioned by institutional culture, leadership framing, and the regulatory environment in which it is embedded. Accordingly, this study conceptualizes digital compliance culture by examining how institutional readiness is socially and culturally constructed, and how this construction shapes the integration of RegTech within financial institutions.

Background

The global financial ecosystem has experienced a rapid acceleration in digitalization over the past decade. Financial institutions across advanced and emerging markets are increasingly adopting technologies such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), blockchain, and big data analytics to optimize operational efficiency, strengthen customer engagement, and mitigate systemic risks. According to Deloitte (2021), more than 65% of global financial institutions have adopted at least one AI-based compliance function, and this figure is projected to grow annually. These technologies enable near-instantaneous processing of transactions and automated risk scoring, thereby supporting proactive and intelligent anti-money laundering (AML) surveillance.

However, these digital capabilities have also been exploited by transnational criminal syndicates, who use anonymized blockchain transfers, unregulated virtual assets, and multi-layered international transactions to obscure illicit financial flows. The United Nations Office on Drugs and Crime (UNODC, 2020) estimates that global money laundering transactions account for roughly 2–5% of global GDP annually, or approximately USD 800 billion to USD 2 trillion. In response, regulatory agencies such as the Financial Action Task Force (FATF), the Financial Conduct Authority (FCA), the European Banking Authority (EBA), and Bank Negara Malaysia (BNM) have issued new digital compliance directives encouraging the integration of RegTech and SupTech tools within AML/CFT frameworks.

In Malaysia, BNM's 2023 Financial Sector Blueprint highlights digital transformation and financial crime resilience as national strategic priorities. BNM has issued policy documents such as the AML/CFT and Targeted Financial Sanctions Policy Document (2019, updated 2021) and the Risk Management in Technology (RMiT) policy (2020), urging financial institutions to leverage intelligent systems to enhance compliance outcomes. Nevertheless, adoption remains inconsistent across institutions, particularly among mid-sized banks and non-bank financial institutions. A 2022 report by PwC Malaysia found that only 37% of local financial institutions had implemented AI-driven transaction monitoring, despite regulatory incentives and rising enforcement risks.

The disparity in adoption reflects more than infrastructural constraints. Empirical studies and industry observations suggest that deeper cultural and institutional factors contribute to uneven digital integration. For instance, Gill, Redhead, and Dhutia (2021) observed that within UK-based financial firms, resistance to RegTech adoption often stemmed from internal silos, unclear risk ownership, and a perception that digital tools may increase, not reduce regulatory exposure. In the ASEAN context, Ramayah, Lee, and Wah (2020) noted that the

success of digital compliance implementation correlated strongly with leadership commitment, interdepartmental collaboration, and cultural openness to change. These findings underscore that institutional readiness is not a fixed or purely technical condition; it is shaped by sociocultural narratives, internal trust levels, and leadership framing of compliance objectives.

Most academic and policy literature on RegTech, including foundational works by Zetzsche et al. (2018) and Arner et al. (2017), focuses primarily on technical capability, regulatory harmonization, and risk alignment. While valuable, such studies tend to under-theorize the human, cultural, and interpretive dimensions of digital compliance transformation. Questions remain largely unanswered: How do compliance officers, risk managers, and IT personnel construct meaning around digital AML systems? What implicit assumptions drive acceptance or rejection of automated controls? How is regulatory guidance interpreted differently across institutions, based on internal culture or leadership orientation?

This paper argues that institutional readiness for digital AML compliance must be reconceptualized beyond infrastructural maturity or policy alignment. It must encompass cultural framing, leadership behavior, discursive constructions of risk, and organizational narratives surrounding compliance technology. In the absence of these considerations, digital transformation efforts risk being superficial—focused on technical form rather than functional substance—and may result in symbolic compliance rather than meaningful deterrence.

The key research problem is thus defined as follows: Although regulatory authorities globally, including BNM and FATF, continue to promote the integration of digital AML tools, there is a persistent gap in understanding how financial institutions internalize, interpret, and implement these tools through the lens of organizational culture. The uneven and culturally contingent nature of adoption signals a misalignment between policy intent and institutional reality. This study responds to that gap by exploring how digital compliance is framed within financial institutions, and what sociocultural, leadership, and institutional factors enable or hinder authentic transformation.

To build a solid foundation for the study, the next section reviews the relevant literature to contextualize key concepts, theoretical frameworks, and empirical insights. This is followed by a discussion of the paper's qualitative conceptual methodology. The findings are then presented thematically, reflecting the key institutional logics and cultural framings that shape digital compliance cultures. The paper concludes by synthesizing its contributions and offering recommendations for future research and policy development.

Literature Review
Institutional Theory and AML Governance
Institutional theory provides a valuable structure to understand how coercive, mimetic and normative pressures shape digital money laundering (AML) practices in organizations. The interaction of these pressures reflects the broader institutional environment in which organizations operate, influencing their strategies of culture and conformity governance.

Coercive pressures, which arise from formal regulations and authoritarian mandates imposed by external entities, play a crucial role in the formation of organizational behavior around LBC practices. Burdon and Sorour (2020) emphasize that the evolution of the UK financial service culture is significantly influenced by regulatory agencies and market forces that impose strict compliance requirements. In this context, organizations must respond to legal and institutional pressures to maintain legitimacy and avoid penalties. The coercive nature of these pressures leads organizations to adopt comprehensive governance structures that align themselves with the compulsory practices of the LBC.

In addition to coercive forces, mimetic pressures - systems of the tendency of organizations to imitate their peer successful practices - increase a significant influence on LBC governance. This imitation usually occurs in environments characterized by uncertainty, where organizations seek industry leaders guidance on best practices. Menon (2023) discusses how the adoption of LBC policies in Singapore has gone from a reactive posture focused on crime prevention to a more proactive norm compliance model. This change highlights how organizations within the same industry tend to imitate each other to obtain legitimacy, which in turn shapes their digital lbc governance structures. By immersing colleagues who have successfully sailed regulatory challenges, organizations can mitigate the risks associated with compliance.

Normative pressures, derived from cultural expectations and professional standards within the industry, further complicate the LBC governance scenario. According to Chiu (2018), these normative forces create an environment in which compliance is not only a legal obligation, but also a matter of ethical commitment and social responsibility. Organizations that feel the weight of these normative pressures are required to adopt more robust LBC governance practices that reflect society's expectations. This dynamic is critical in a digital scenario, where transparency and responsibility are increasingly required by stakeholders, leading to greater investment in AML technologies and practices.

Exploring these pressures through the lenses of actor network theory, Al-Abdullah (2015) highlights the urgent need to see LMA compliance not only as a response to external pressures, but also as an evolution network of actors, including financial institutions and application agencies. Thus, Digital LBC governance practices can be seen as a product of interactions between various stakeholders, each contributing to a collective understanding of the conformity standards. By integrating the theory of the actors network into institutional principles, we can appreciate how organizations sail in coercive, memoric and normative pressures to build a cohesive governance structure in their digital operations.

As organizations implement digital LMA strategies, it is essential to understand how lived experiences shape these practices. Menz (2025) calls for a research agenda that focuses on the prospects of money laundering prevention officers, advocating a deeper understanding of how institutional forces manifest themselves in daily compliance activities. In the foreground of the experiences of compliance professionals, researchers can discover the nuances of how coercive, mimetic and normative pressures influence practical governance strategies. This approach not only enriches our theoretical understanding, but also provides actionable information for organizations that seek to improve their LBC practices in an increasingly complex digital environment.

Hence, institutional theory offers a comprehensive structure to analyze how coercive, mimetic and normative pressures intersect to shape digital LBC governance. The regulatory scenario leads organizations to adopt compliance strategies aligned with coercive patterns, while mimetic behaviors promote the imitation of well -sued practices throughout the sector. Meanwhile, normative pressures promote a culture of ethical responsibility and commitment to compliance. By examining these dynamics through various theoretical perspectives, including actor network theory and emphasizing the experiences of field professionals, we can get a different understanding of how organizations adapt their LBC digital governance practices in response to institutional forces. This multifaceted approach increases our understanding of the broader implications of institutional theory in the context of money laundering governance.

Organizational Culture and Technology Adoption
An in-depth examination of how organisational culture influences the adoption of technology reveals that cultural inertia, leadership values and internal trusted dynamics are fundamental factors in successful digital conformity initiatives. Understanding these elements is essential for organisations that aim to navigate the complexity of digital transformation. Cultural inertia, defined as the tendency of consolidated organizations to resist change due to their rooted values and practices, often poses significant challenges in the adoption of new technologies. As Bozkus (2023) highlights, organizational culture is deeply intertwined with the adoption of technology, which requires a cultural change for an effective digital transformation. This inertia can prevent the integration of advanced technologies, highlighting the need for a proactive approach to the change of culture.

Leadership values play a crucial role in facing cultural inertia and promoting an environment in favor of the adoption of technology. Effective leaders are essential to establish a vision that aligns with digital conformity initiatives. Alshammari, Alhallalaqi and Al-Mamary (2024) stress that leadership commitment for digital transformation is essential for modeling organizational culture and facilitating the acceptance of new technologies. When leaders embody values that give priority to innovation, collaboration and adaptability, they can inspire the workforce to embrace the change, overcoming the cultural inertia that could otherwise hinder progress. In addition, leaders who actively promote a culture of trust are better positioned to implement transformative technologies, since the trusted dynamics significantly influence the willingness of employees to interact with new systems.

The role of internal trusted dynamics cannot be overrated, since they are fundamental for the success of the success of technology in organizations. Trust in the organizational context creates an atmosphere in which employees feel safe by expressing their concerns and feedback on new technologies, thus facilitating a more fluid transition. Trushkina et al. (2020) They argue that in the era of the information economy, the promotion of an authentic culture of trust improves the buy-in of employees and reduces resistance to technological changes. This trust promotes a collaborative environment, which is particularly important in compliance initiatives in which adherence to regulations is fundamental for organizational success. The presence of trust not only mitigates the fears associated with the adoption of technology but also encourages the sharing and collaboration of knowledge, leading to a more efficient implementation of digital tools.

In addition, the cultural readiness for the adoption of technology, in particular within small and medium-sized enterprises (SMEs), highlights the importance of cultivating a digital organizational culture. Jewapatarakul and Ueasangkomsate (2024) explore how organizational readiness influences the ability of companies to assimilate new technologies, in particular in the food production sector. Their results indicate that a robust digital culture not only prepares employees for technological transitions, but also supports the acquisition of essential knowledge for digital transformation efforts. In this context, cultural inertia can be reduced by proactively developing a digital mentality among employees, which is crucial to embracing new conformity technologies. Therefore, the leadership that emphasizes continuous improvement and innovation can significantly alter the trajectory of the digital journey of an organization.

The dynamic interaction of organizational culture and adoption of technology is further illustrated in case studies that explore the management of information technology projects. Soncc, Rodríguez and Fernández (2025) have an in -depth analysis of the organizations that have successfully sailed the digital transformation by aligning their cultural values with technological initiatives. These case studies reveal that when organisational culture is aligned with the strategic objectives of the adoption of technology, not only is compliance reached, but there are also improved overall services. Organisations that effectively exploit their cultural resources, while they turn to cultural inertia, are more likely to see the successful integration of new technologies.

In conclusion, organizational culture significantly influences the adoption of technology, with cultural inertia, leadership values and internal trusted dynamics that act as fundamental elements in the process. The navigation of the challenges posed by cultural inertia requires influential leadership that supports change and promotes a trusted environment among employees. The implications of these results are profound: strategically aligning culture with technological initiatives, organizations can not only overcome resistance, but also effectively exploit the opportunities for digital transformation. The interaction of these factors underlines the need for organizations to undertake a holistic approach to the change of culture, ensuring that their digital conformity initiatives are supported by a robust fundamental culture. While literature continues to evolve in response to the current technological progress, the importance of examining these cultural dimensions will remain fundamental for the adoption of successful technology in any organization.

RegTech and Compliance Digitalization
The adoption of regulatory technology solutions (Regtech) represents a significant change in the paradigms of conformity within the financial institutions, influenced by a triadic interaction between technology, organizational culture and regulatory clarity. Using the framework of technology-organization-environment-environment (toe), this revision of literature examines how these dimensions collectively shape the implementation and effectiveness of the digitization of compliance in contemporary institutions.

Technology acts as a catalyst for regtech solutions, facilitating the automation of compliance processes and risk management. Firiza et al. (2024) They say that the integration of advanced technologies, such as artificial intelligence and automatic learning, automates not only routine compliance tasks, but also improves the skills of analysis of organizations. These

technological progress allow more solid compliance monitoring, reducing the burden on human resources and minimizing the risk of human error (Firiza et al., 2024). Olaiya et al. (2024) further clarify this point by highlighting that the Regtech solutions improve the effectiveness of compliance and the management of risks specifically in the financial sector, an environment characterized by constant regulatory changes and greater vigilance. This technological integration directly affects the institutions by promoting a more agile regulatory environment in which the compliance requirements are satisfied with better speed and accuracy.

However, the organizational culture that surrounds the adoption of Regtech solutions is equally crucial. A support culture that embraces innovation and change can significantly improve the distribution and usefulness of technology within organizations. El Khoury, Alshater and Joshipura (2024) point out that organizations without culture of adaptability and opening to technological solutions can face substantial challenges in the implementation of Regtech. Resistance to change can slow down the adoption process and undermine the potential benefits of these technologies (El Khoury et al., 2024). Since organizational culture is often rooted in practices and consolidated beliefs, the promotion of an environment favorable to technological integration requires the commitment of leadership and the establishment of training programs that promote the understanding of the Regtech skills among employees.

In terms of regulatory clarity, its impact on the adoption of Regtech cannot be underestimated. The clear and well -defined regulatory paintings facilitate the most fluid implementation processes for financial institutions, allowing them to perfectly integrate the Regtech solutions in their conformity infrastructure. Aliu, Ikharro and Jegede (2024) argue that a centralized approach to regulatory compliance, strengthened by clear guidelines, can significantly improve the effectiveness of Regtech in the National Centech ecosystem. When regulatory expectations are transparent, organizations are better equipped to use regtech for compliance, knowing that their technological investments are aligned with standards and legal expectations.

Regulatory ambiguity can serve as a barrier to the adoption of Regtech solutions. As noted by Majid and Pangenstituti (2024), the institutions operating in jurisdictions with unclear regulatory landscapes can hesitate to invest in regtech, fearing potential misalignments with floating regulatory requests. This apprehension can suffocate innovation and cause missed opportunities to optimize compliance processes through advanced technology. Therefore, regulatory clarity is essential for the promotion of an environment in which Regtech can thrive, allowing institutions to navigate in the complexity of conformity to trust.

The interaction between technology, organizational culture and regulatory clarity underlines the need for a holistic approach to the adoption of Regtech. The institutions that aim to improve the digitization of conformity must consider these interconnected factors, ensuring that technological infrastructures are supported by a culture of innovation and a favorable regulatory environment. The synthesis of these dimensions leads to better compliance results and fortified risk management strategies. Consequently, when organizations adopt Regtech solutions, they should invest in cultural transformation together with technological progress and support regulatory clarity to achieve the full potential of the digitization of compliance.

Hence, the interaction of technology, organizational culture and regulatory clarity in the context of the framework of the feet illustrates the multifaceted nature of the adoption of the Regtech solution. By exploiting technology and promoting an adaptable organizational culture in a context of a clear regulatory guide, institutions can successfully navigate the panorama of digital conformity. The meaning of this integrated approach is underlined through the results and recommendations in contemporary literature, illustrating that the successful implementation of Regtech is not based exclusively on technology, but a reflection of the strategic alignment of an institution in all sizes.

Methodology
This paper adopts a qualitative, conceptual methodology grounded in an interpretivist epistemology, which prioritizes understanding the meanings and social constructions that actors assign to their experiences within institutional settings. The interpretivist approach is especially suited for unpacking how compliance cultures are framed, negotiated, and internalized across different financial institutions. Given the central aim of this study is to examine cultural and institutional readiness rather than to measure causal relationships or statistical outcomes, a conceptual and exploratory orientation is more appropriate than a purely empirical one.

Rather than collecting new quantitative data, the study synthesizes and interprets existing scholarly literature, policy documents, institutional reports, and case-based evidence to construct a theoretical framework for understanding how digital compliance cultures emerge and operate. The focus is on identifying dominant themes, recurring patterns, and institutional logics that shape the adoption of digital anti-money laundering (AML) systems within financial institutions. This conceptual synthesis allows for the generation of nuanced insights that bridge theory and practice, especially where empirical studies have not yet fully addressed cultural and interpretive dimensions.

The theoretical foundation for this analysis is anchored in three complementary frameworks:
  i.   Institutional Theory (Scott, 2008), which highlights how regulatory, normative, and cognitive pressures shape organizational behavior and institutional legitimacy.
  ii. Organizational Culture Theory (Schein, 2010), which provides insight into how shared assumptions, values, and leadership narratives influence responses to technological change.
  iii. The Technology-Organization-Environment (TOE) Framework (Tornatzky & Fleischer, 1990), which identifies contextual factors that determine technology adoption readiness, including internal competencies, perceived complexity, and environmental dynamism.

Together, these frameworks enable the study to conceptualize digital compliance not as a neutral or technical process, but as an institutional phenomenon shaped by actors' interpretations, cultural values, and environmental constraints. By combining a conceptual synthesis with a proposed empirical inquiry, the methodology aims to advance both theoretical understanding and practical relevance in the domain of digital AML governance.

Thematic Conceptual Findings and Discussion

Theme 1: Compliance as Cultural Performance

Digital AML systems are often adopted as a performative response to regulatory demands rather than internalized practices. In such institutions, compliance departments may implement RegTech solutions primarily to demonstrate alignment with regulatory expectations or to pass audits, rather than as tools to actively detect or prevent financial crime. This results in symbolic compliance, where the presence of technology is equated with effectiveness, even when it is underutilized or poorly integrated with core operational processes.

Performative compliance can manifest in several ways: outdated rule-based monitoring systems being relabeled as AI-driven tools; over-reliance on vendor solutions without internal capacity-building; or incomplete data integration that limits the actual utility of advanced analytics. A study by Levi and Reuter (2020) found that many financial institutions deploy transaction monitoring systems that generate large volumes of false positives, which are rarely acted upon due to resource constraints. These systems exist more to satisfy documentation requirements than to provide real-time, risk-based intervention.

Cultural performance is also shaped by institutional incentives. Where employee evaluation is based on audit outcomes or regulator perception rather than substantive results, compliance professionals are more likely to prioritize form over function. This symbolic framing of technology contributes to a compliance culture that is defensive rather than proactive. Furthermore, if leadership does not model commitment to digital transformation or fails to allocate sufficient budget, RegTech initiatives become marginal and reactive. Thus, compliance technology risks being a "checkbox exercise," reflecting regulatory anxiety rather than institutional innovation.

To address this, institutions must critically examine how compliance success is defined and measured. Integrating RegTech tools meaningfully requires cultural alignment—where staff at all levels understand the purpose and value of digital systems, and where risk detection is treated as a core institutional mission, not just a regulatory formality.

Theme 2: Leadership Framing and Legitimacy

Leadership plays a decisive role in how digital AML systems are perceived and adopted within an institution. When leaders frame compliance as a strategic asset rather than a regulatory burden, it signals to staff that technological innovation is both desirable and supported. In such contexts, RegTech is embedded in enterprise-wide risk management strategies and linked to long-term sustainability goals.

Conversely, where leadership sees AML obligations as externally imposed or merely cost centers, digital tools are often deprioritized. Studies by Gill et al. (2021) and Ramayah et al. (2020) indicate that the presence of an engaged and tech-literate leadership team strongly predicts successful RegTech implementation. Leaders who participate in cross-functional discussions on risk and innovation are more likely to secure buy-in from other departments and ensure budget allocations align with strategic technology investments.

Leadership framing also affects perceived legitimacy of the systems. If frontline staff view RegTech initiatives as top-down impositions with limited explanation or training, resistance is likely. Staff may question the credibility of systems or the motives behind their adoption. This is especially critical in hierarchical institutions, where communication gaps between senior management and operational teams can exacerbate misunderstanding. Trust in digital AML tools grows when leadership is transparent about goals, demonstrates practical knowledge of system capabilities, and fosters a participatory rollout process.

In short, leadership does not only shape policy—it shapes culture. The framing of digital compliance efforts by leadership, whether symbolic or sincere, determines how deeply such systems are embedded and whether they are seen as legitimate solutions to real institutional risks.

Theme 3: Regulatory Ambiguity and Cultural Interpretation
Digital compliance systems operate within a regulatory ecosystem that is itself evolving and, in many jurisdictions, inconsistently articulated. Regulatory ambiguity whether in the form of vague language, overlapping guidelines, or delayed updates compels institutions to interpret rules based on their internal logic, values, and perceived risk exposure.

Such interpretive flexibility can lead to innovation, but it can also foster uneven adoption. In Malaysia, for instance, while BNM has published extensive AML/CFT guidelines (BNM, 2021), smaller financial institutions often struggle to reconcile general regulatory expectations with their own limited operational capacities. Some institutions adopt a conservative interpretation, implementing only the minimum requirements. Others attempt to exceed expectations but do so inconsistently due to lack of internal policy clarity or technological alignment.

Regulatory ambiguity also interacts with institutional culture. Organizations that value compliance as a principle of integrity are more likely to interpret vague guidance in a risk-aware and forward-looking way. Institutions that view regulation as adversarial or punitive may adopt a minimalistic or defensive approach, leading to surface-level implementation of digital tools. This difference in cultural orientation can produce systemic disparities in how digital AML systems are framed and used.

Furthermore, regulatory bodies themselves may struggle to communicate technological expectations effectively. In a review of FATF mutual evaluations from 2018–2022, several jurisdictions were noted to lack specific guidance on how financial institutions should incorporate AI, machine learning, or blockchain analytics into AML operations (FATF, 2022). This regulatory silence amplifies uncertainty and places the burden of interpretation onto institutions, which may lack the expertise to innovate responsibly.

Thus, regulatory ambiguity is not just a governance challenge, it is a cultural signal. It invites institutions to fill gaps with their own assumptions, values, and operational norms. For meaningful compliance, both regulators and institutions must recognize the interpretive nature of digital guidelines and work toward collaborative clarity.

Theme 4: Digital Trust and Organizational Readiness

Trust is a foundational condition for technology adoption, and in the context of digital AML compliance, it is both technical and cultural. Institutions must trust that the systems they adopt are accurate, secure, and aligned with their operational workflows. But more critically, staff must trust that these systems are deployed in ways that support, rather than threaten, their professional roles.

Organizational readiness for digital AML tools hinges on the degree of trust across multiple levels. When compliance officers, IT personnel, and frontline staff collaborate openly, digital systems are more likely to be integrated holistically and used proactively. However, in environments where data is siloed, departments are misaligned, or staff fear that automation may lead to job displacement or punitive oversight, trust erodes. In such settings, even the best-designed systems may be resisted or misused.

Transparency and training are key to cultivating digital trust. Institutions that invest in participatory design processes, conduct regular workshops, and openly discuss system limitations and possibilities tend to experience smoother adoption. Staff engagement is not a secondary step; it is a core strategy. A 2022 report by Deloitte highlighted that financial institutions with inclusive RegTech deployment processes had 43% higher system utilization rates and significantly lower post-implementation resistance.

Moreover, digital trust is shaped by historical experience. Institutions that have encountered prior failures such as system breaches, false alarms, or compliance penalties may carry organizational memory that colors perceptions of new technologies. Leaders must acknowledge these histories and actively rebuild trust through accountability, clear communication, and demonstrated improvements.

Organizational readiness, therefore, is not merely about technical capability or regulatory alignment. It is about cultural confidence, the belief that technology serves the institution's purpose, supports its people, and aligns with its values. Institutions that prioritize trust-building are better positioned to transform compliance from obligation into opportunity. These themes suggest that digital AML adoption is deeply intertwined with organizational culture and institutional logic, not merely with IT capability or compliance infrastructure.

Table 1

Summary of Thematic Findings on Digital Compliance Cultures in AML Governance

Theme	Core Insight	Cultural/Institutional Implication	Illustrative Reference
1. Compliance as Cultural Performance	Digital AML tools are adopted to appease regulators rather than for meaningful use.	Leads to symbolic compliance, audit-focused implementation, and underutilized systems.	Levi & Reuter (2020)
2. Leadership Framing and Legitimacy	Leadership perception shapes legitimacy and depth of adoption.	Strategic framing by leadership increases staff buy-in and long-term integration.	Gill et al. (2021); Ramayah et al. (2020)
3. Regulatory Ambiguity and Cultural Interpretation	Vague regulations lead to inconsistent institutional interpretations.	Institutions either exceed or underperform compliance expectations based on internal culture.	BNM (2021); FATF (2022)
4. Digital Trust and Organizational Readiness	Trust in systems and leadership drives readiness and acceptance.	Transparent deployment, training, and interdepartmental trust increase system effectiveness.	Deloitte (2022)

Conclusion

As digital transformation becomes central to anti-money laundering (AML) compliance, financial institutions must evolve beyond the narrow logic of technology procurement and system installation. Rather than perceiving digital AML systems as isolated tools or reactive measures to regulatory pressure, institutions need to cultivate an internal culture of compliance that is strategic, participatory, and values-driven. While advancements in RegTech offer unprecedented opportunities for real-time monitoring, automated risk assessments, and cross-border surveillance, the actual impact of these technologies hinges on how they are framed, interpreted, and utilized by the people and systems within organizations.

This study underscores that institutional readiness is not a singular technical milestone but a multi-dimensional construct embedded in organizational culture, leadership, trust, and regulatory relationships. The thematic findings-compliance as cultural performance, leadership framing and legitimacy, regulatory ambiguity and cultural interpretation, and digital trust and organizational readiness-highlight the complex interplay of soft factors that either enable or hinder meaningful digital transformation in AML governance.

One critical implication is that regulators must recognize their role not only as policy enforcers but also as enablers of institutional learning. Broad or ambiguous regulatory guidance, while allowing for innovation, can also create confusion and inconsistent application across institutions. Regulators should work more closely with industry players to co-develop contextualized guidelines, foster peer learning platforms, and promote risk-based regulatory sandboxes. For example, Malaysia's use of the Financial Technology Regulatory Sandbox Framework by Bank Negara Malaysia has proven useful in encouraging digital

experimentation under controlled environments, yet its reach must be expanded to include smaller and mid-sized institutions that lack the resources of larger banks.

For institutions themselves, the findings suggest that digital AML efforts should not be confined to compliance departments. Instead, these initiatives must be understood as enterprise-wide transformations that require leadership buy-in, cross-functional alignment, and active involvement from technology, audit, risk, and business development units. Institutions that treat compliance as a dynamic strategic function-integrated with risk governance and corporate ethics-are more likely to realize the full benefits of RegTech tools and reduce exposure to regulatory penalties or reputational damage.

Moreover, there is a significant value in investing in internal communication and capacity-building programs. Staff across all levels must understand not just how to operate compliance systems, but why they matter. This requires a shift from compliance training as a tick-box exercise to an ongoing conversation about institutional integrity and public trust. Digital trust-building mechanisms such as participatory system design, feedback loops, and internal knowledge-sharing platforms can significantly increase staff engagement and ownership over compliance outcomes.

Academically, this paper contributes to the growing discourse on compliance digitalization by reframing institutional readiness as a cultural and interpretive phenomenon rather than a static or technical benchmark. It calls for further empirical research that explores how individuals within organizations-especially in different cultural and regulatory contexts-construct meaning around digital compliance technologies. Qualitative methods such as ethnographic observation, discourse analysis, and narrative inquiry could provide deeper insight into how compliance officers, IT professionals, and regulators perceive, resist, or embrace RegTech systems.

Future research should also explore the comparative dynamics of digital AML adoption across jurisdictions. Differences in political economy, institutional maturity, and historical regulatory philosophies can create vastly different compliance environments, even when the same technology is available. Cross-country studies in Southeast Asia, Europe, and the Middle East could shed light on how institutional framing affects RegTech integration, and what lessons can be learned for developing globally responsive yet locally adaptable compliance frameworks.

Ultimately, meaningful AML governance in the digital age requires more than technological investment. It requires institutional courage-to rethink the assumptions that guide compliance behavior; institutional empathy-to consider the human impact of automation and surveillance; and institutional imagination-to see compliance not merely as obligation but as opportunity. In a globally connected, ethically complex world, the next generation of AML systems must be rooted not only in algorithms and analytics but in values, vision, and trust.
By re-centering the discussion of digital compliance around cultural readiness, leadership engagement, and institutional framing, this paper offers a new lens through which both practitioners and scholars can approach one of the most pressing challenges in financial regulation today.

References
Financial Conduct Authority (FCA). (2022). *Regulatory Sandbox*. Retrieved from https://www.fca.org.uk/firms/innovation/regulatory-sandbox

Monetary Authority of Singapore (MAS). (2021). *Technology Risk Management Guidelines*. Retrieved from https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the Reconceptualization of Financial Regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–413.

Deloitte. (2021). *AI and Compliance in Financial Services: Global Perspectives*. Retrieved from https://www2.deloitte.com

Gill, M., Redhead, S., & Dhutia, A. (2021). Compliance Technology and Institutional Resistance: A UK Perspective. *Journal of Financial Regulation and Compliance*, 29(2), 185–200.

PwC Malaysia. (2022). *The Future of Compliance: Rethinking RegTech in Malaysian Financial Institutions*. Retrieved from https://www.pwc.com/my

Ramayah, T., Lee, J. W. C., & Wah, T. Y. (2020). The Role of Institutional Support and Organizational Culture in Adopting Financial Technology in Southeast Asia. *Asian Journal of Business Research*, 10(1), 45–65.

UNODC. (2020). *Money-Laundering and Global Financial Crime Estimates*. United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2018). From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance. *New York University Journal of Law & Business*, 14(2), 393–446.

Bank Negara Malaysia. (2020). *Risk Management in Technology (RMiT)*. Retrieved from https://www.bnm.gov.my

Bank Negara Malaysia. (2021). *Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions*. Retrieved from https://www.bnm.gov.my

Bank Negara Malaysia. (2023). *Financial Sector Blueprint 2022–2026*. Retrieved from https://www.bnm.gov.my

Burdon, W. M., & Sorour, M. K. (2020). Institutional theory and evolution of 'a legitimate' compliance culture: The case of the UK financial service sector. Journal of Business Ethics, 162(1), 47-80.

Menon, R. E. (2023). From crime prevention to norm compliance: anti-money laundering (AML) policy adoption in Singapore from 1989–2021. Journal of Money Laundering Control, 26(1), 69-92.

Chiu, I. H. (2018). An institutional theory of corporate regulation. Current Legal Problems, 71(1), 279-334.

Al-Abdullah, M. (2015). An actor-network theory approach in investigating the information systems perspective of anti-money laundering compliance through a case study of the Foreign Account Tax Compliance Act (FATCA) implementation in a Jordanian local bank. Virginia Commonwealth University.

Menz, M. (2025). Reorienting the lens–towards a new research agenda on the lived experiences of money laundering prevention officers. Journal of Money Laundering Control, 28(1), 64-79.

Bozkus, K. (2023). Organizational culture change and technology: Navigating the digital transformation. In Organizational Culture-Cultural Change and Technology. IntechOpen.

Alshammari, K. H., Alshallaqi, M., & Al-Mamary, Y. H. (2024). Digital transformation dilemma in the era of changing dynamics: How organizational culture influence the success of digital transformation. Human Systems Management, 43(4), 455-472.

Trushkina, N., Abazov, R., Rynkevych, N., & Bakhautdinova, G. (2020). Digital transformation of organizational culture under conditions of the information economy. Virtual Economics, 3(1), 7-38.

Jewapatarakul, D., & Ueasangkomsate, P. (2024). Digital organizational culture, organizational readiness, and knowledge acquisition affecting digital transformation in SMEs from food manufacturing sector. Sage Open, 14(4), 21582440241297405.

Soncco, J. P., Rodríguez, C. R., & Fernández, C. V. L. (2025). Organizational culture and digital transformation in the management of Information Technology projects: A case study. Technology Rain Journal, 4(1).

Firiza, M. D., Lutfiani, N., Zahra, A. R. A., & Rahardja, U. (2024, October). The role of regtech in automating compliance and risk management. In 2024 12th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-6). IEEE.

Olaiya, O. P., Adesoga, T. O., Pieterson, K., & Qazeem, O. (2024). RegTech Solutions: Enhancing compliance and risk management in the financial industry. GSC Advanced Research and Reviews, 20(2), 8-15.

El Khoury, R., Alshater, M. M., & Joshipura, M. (2024). RegTech advancements-a comprehensive review of its evolution, challenges, and implications for financial regulation and compliance. Journal of Financial Reporting and Accounting.

Aliu, N. F., Ikharo, A. B., & Jegede, A. J. (2024). Enhancing Regulatory Compliance in the National FinTech Ecosystem: A Centralized RegTech Approach. University of Ibadan Journal of Science and Logics in ICT Research, 12(2), 1-11.

Majid, M. A., & Pangestuti, I. R. D. (2024). Challenges in Regulatory Compliance and Risk Management in Emerging Markets. Business Strategy and Innovation: An International Journal, 3(1), 43-55.

Scott, W. R. (2008). *Institutions and organizations: Ideas and interests* (3rd ed.). SAGE Publications.

Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books

Levi, M., & Reuter, P. (2020). *Money laundering: A global perspective*. In N. Lord, M. Levi, D. P. Wall, & M. Innes (Eds.), *Emerging trends in financial crime and regulation* (pp. 13–30). Routledge.

Gill, M., Redhead, S., & Dhutia, A. (2021). Compliance technology and institutional resistance: A UK perspective. *Journal of Financial Regulation and Compliance*, 29(2), 185–200.

Ramayah, T., Lee, J. W. C., & Wah, T. Y. (2020). The role of institutional support and organizational culture in adopting financial technology in Southeast Asia. *Asian Journal of Business Research*, 10(1), 45–65.

Bank Negara Malaysia. (2021). *Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (Policy Document)*.

Financial Action Task Force. (2022). *FATF Annual Report 2021–2022*.
Deloitte. (2022). *RegTech universe: How financial services are managing compliance through technology*. Deloitte Insights.