



American Journal of Governance and Management (AJGM)

VOLUME 1 ISSUE 1 (2026)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

Regulatory Compliance in Saudi Arabia: Frameworks, Governance, and Implementation A Systematic Review of the Post-Vision 2030 Regulatory Environment (2017–2025)

Mohamed Abdelhalim Soliman¹*

Article Information

Received: June 28, 2026

Accepted: September 10, 2026

Published: October 01, 2026

Keywords

*Aml/Cft, Anti-Corruption,
Corporate Governance,
Cybersecurity, Data Protection,
Regulatory Compliance,
Saudi Arabia, Tax Compliance,
Vision 2030*

ABSTRACT

This systematic review provides a picture of the Saudi regulatory compliance environment after Vision 2030 (2017–2025), combining official regulatory instruments and peer-reviewed empirical literature. The review examines changes in the compliance governance landscape and proposes a comprehensive compliance governance framework for Saudi organizations. The study uses a systematic qualitative content analysis coupled with regulatory mapping across six compliance domains: financial regulation and anti-money laundering; corporate governance and disclosure; data protection; cybersecurity; anti-corruption; and taxation. After a structured search in Google Scholar, Scopus, Web of Science, HeinOnline, Westlaw, and official regulatory databases (SAMA, CMA, SDAIA, NCA, ZATCA, Nazaha), 50 sources have been selected using explicit criteria: peer-reviewed articles and official regulatory documents/legal frameworks published between 2017 and 2025; non-academic commentary; and obsolete pre-2017 instruments were excluded. The results demonstrate a clear evolution from fragmented and sanction-oriented regulatory environment to consolidated and risk-based system, characterized by specialized regulators, codified rulebook, digital compliance infrastructure, and harmonization with international standards set by Basel, FATF, G20, and OECD. Moreover, the review highlights implementation issues including regulatory fragmentation, insufficient compliance capacity, disproportional impact on small and medium-sized enterprises, and inconsistency of enforcement. Based on the results of the systematic review, the paper proposes an Integrated Compliance Governance Framework (ICGF) consisting of four pillars: regulatory intelligence; risk-based control environment; integrity culture and accountability; and technology-enabled assurance with a phased implementation roadmap. This review is the first comprehensive systematic effort to outline the post-Vision 2030 Saudi compliance architecture and provides a useful tool for regulators and organizational leadership.

INTRODUCTION

Since the start of Vision 2030 (Kingdom of Saudi Arabia, 2016), Saudi Arabia underwent the most extensive regulatory transformation in the region. Regulatory compliance lies at the core of this agenda: any measure of diversification, privatization, capital markets development, digitalization, and introduction of VAT brought additional or revised compliance obligations for firms, financial institutions, and public organizations. Between 2017 and 2025, the Kingdom created at least six major regulatory architectures: the SAMA Rulebook and AML/CTF Guide (SAMA, 2023a, 2023b); the CMA Corporate Governance Regulations (CMA, 2017); the Personal Data Protection Law implemented in September 2023 by SDAIA (SDAIA, 2023; DLA Piper, n.d.); the frameworks developed by the National Cybersecurity Authority (NCA, 2018, 2019); the reform of anti-corruption regime within Nazaha (Greenberg Traurig, 2024); and mandatory e-invoicing system managed by ZATCA (2021, 2023). Nowadays, Saudi organizations face multiple obligations at once with regard to several regulators, reporting cycles, data definitions, and types of enforcement.

The academic literature tends to follow sectoral lines: banking, governance, data protection, cybersecurity,

integrity, and taxation are usually studied separately (Gerged & Agwili, 2020; Boshnak, 2021; Alsulaiman & Alrodhan, 2014; Alsemairi, 2023; Altawyan, 2020). However, what is absent in the academic literature is systematic cross-domain approach to the issue: the architecture of the Saudi compliance environment, its empirical record, and the challenge to manage multiple obligations simultaneously. This study aims to fill this gap by conducting a systematic review of the Saudi regulatory compliance environment between 2017 and 2025. The study integrates official regulatory instruments with peer-reviewed evidence on the issue in six compliance domains. Moreover, based on the results of the systematic review, the paper proposes an Integrated Compliance Governance Framework (ICGF) for Saudi organizations, which consists of four pillars: regulatory intelligence, risk-based control environment, integrity culture and accountability, and technology-enabled assurance.

The research aims at achieving the following goals: performing a systematic review of the regulatory compliance environment of Saudi Arabia after Vision 2030 was launched; synthesizing data on the major regulatory domains and discovering the key issues that Saudi organizations have to face; developing evidence-

¹ International Business Academy of Switzerland (IBAS), Switzerland

* Corresponding author's email: mohamedabdelhalimsoliman@researchpublication.co

based suggestions and an integrated compliance governance framework. The study adds value by combining primary regulatory documents, which include SAMA Rulebook, AML/CTF Guide, CMA Corporate Governance Regulations, Personal Data Protection Law, NCA cybersecurity controls, Nazaha regulations, and ZATCA e-invoicing requirements, with empirical studies found in peer-reviewed literature. The aforementioned combination offers a cross-regulatory perspective that is rarely covered by prior literature. The rest of the paper reviews relevant theories and empirical studies, provides details on the research methodology, presents the results and comparative analysis, discusses the implications of the findings both theoretically and practically, and suggests recommendations for improving compliance governance in Saudi organizations.

Research Questions

RQ1: How did the regulatory compliance environment of Saudi Arabia evolve after Vision 2030 was launched?

RQ2: What are the major regulatory frameworks that govern compliance in Saudi Arabia and how do they affect certain industries?

RQ3: What problems do Saudi organizations have to overcome to achieve and maintain compliance?

RQ4: How can an integrated compliance governance framework enhance compliance in Saudi organizations?

LITERATURE REVIEW

The present sub-section highlights the theoretical background on regulatory compliance (2.1), institutional and cultural context in Saudi Arabia (2.2), development of the Saudi regulatory regime (2.3), and domain-related empirical literature (2.4). All studies cited have been identified using the approach outlined in Section 3 of the thesis.

Theoretical Foundations of Regulatory Compliance

Although deterrence theory assumes a rational response to expected sanctions, empirical research proves the impact of sanctions to depend on the legitimacy and procedural fairness perceptions; people obey the authorities perceived as legitimate and procedurally fair (Tyler, 2018; Tyler & Fagan, 2008). Responsive regulation theory incorporates these ideas into the pyramid of enforcement starting with the persuasion stage and escalating only in case of cooperation breakdown while moving to de-escalation after compliance restoration (Ayres & Braithwaite, 1992). Empirical testing of the theory has been performed in such areas as food safety regulation (Mascini & Van Wijk, 2009), with its further application to tax administration. Accordingly, research reveals that the responsive approach increases the level of trust and reduces tax base erosion (Alm, Gerbrands, & Kirchler, 2022; Hartner, Rechberger, Kirchler, & Wenzel, 2008). Thus, the mentioned findings are directly related to the move of Saudi regulators to a new risk-based paradigm from sanction-based approaches, which

is illustrated by the phased e-invoicing implementation (ZATCA, 2021, 2023) and comply-or-explain governance model (CMA, 2017). Institutional theory explains the phenomenon of compliance as an adaptation to coercive, mimetic, and normative pressures; thus, Vision 2030 has been viewed as the pressure field that imposes mandatory digital and governance transformation on the Saudi public sector (Aldhafiri, 2026). Lastly, there is also the strand of culture research dedicated to the Gulf region, emphasizing the role of such informal institutions as *wasta* for rule application (Alofi, 2017).

The Saudi Institutional and Cultural Context

Compliance governance in Saudi Arabia takes place in the legal system based on the combination of Shari'ah and the rules adopted by the Council of Ministers as well as specialized regulators. Pre-reform studies highlight such issues as corporate disclosure opacity (Alqahtani, 2020), inconsistency of governance codes enforcement (Zerban, 2017), and absence of a general data protection law (Alsulaiman & Alrodhan, 2014). Informal networks are considered cultural factors affecting the Saudi organizations (Alofi, 2017). Thus, all the mentioned aspects set the initial baseline to assess the reforms implemented since 2016.

Evolution of the Saudi Regulatory Environment

Vision 2030 (Kingdom of Saudi Arabia, 2016) aimed to ensure economic diversification and regulatory quality at the international level. Specialized regulators have been established or consolidated to address these objectives: the CMA to regulate the securities market, SAMA to control the banks and payments, NCA to supervise cybersecurity, SDAIA to govern the data and AI, ZATCA for VAT and e-invoicing, and Nazaha for anti-corruption. During this period, Saudi Arabia has faced increasing international integration, including G20 membership, FATF-driven enhancements following prior concerns regarding terrorist financing risks (Blanchard & Prados, 2007) and commitment to OECD-based tax transparency initiatives. There are two main features distinguishing the post-Vision 2030 regulatory regime: codification of SAMA, combining the circulars into online Rulebook that includes account opening rules and the AML/CTF Guide (SAMA, 2023a, 2023b) and digital enforcement, including the mandatory e-invoicing starting in December 2021 (Phase 1) and Fatoorah integration in January 2023 (Phase 2) (ZATCA, 2021, 2023).

Domain-Specific Empirical Literature

Financial Regulation and Anti-Money Laundering

Early international assessment of Saudi terrorist financing controls (Blanchard & Prados, 2007) accelerated the legislative process. Doubts about the effectiveness of formal AML frameworks in bank-secrecy regimes, where there is no societal responsibility culture among the banks, were voiced by Carr and Jago (2014). More recently, it was suggested to introduce the decentralized and privacy-

preserving architecture combining blockchain technology and federated learning for the purpose of improving AML effectiveness in digital banking (Khan, Alsufyani, & Alsufyani, 2025). Legal scholarship has also addressed the question of cryptocurrencies regulation in the Kingdom, considering SAMA's exclusive right to issue currency and corresponding obligations to the digital asset providers (Habadi & Alsamara, 2025). The current SAMA AML/CTF Guide (2023b) provides information on due diligence, suspicious transactions reporting, and senior management accountability.

Corporate Governance and Disclosure

Gerged and Agwili (2020) analyzed the impact of governance structures on firm value in Saudi-listed firms within CMA comply-or-explain framework; Boshnak (2021) explored corporate governance mechanisms and firm performance in view of CMA supervision; Zerban (2017) discussed accounting and auditing failure caused by uneven compliance and enforcement; Alqahtani (2020) confirmed the problem of disclosure quality and non-conformity enforcement; Amubarak (2020) indicated that smaller firms have compliance problems; and Alamri and Alshekmubarak (2023) considered governance and business ethics in Saudi-listed banks. Thus, the literature reflects improvements in governance quality along with compliance and enforcement gaps.

Data Protection and Privacy

Until 2023, there was no comprehensive personal data protection legislation in Saudi Arabia. These deficiencies were described in works of Alsulaiman and Alrodhan (2014) and Alghamdi and Nor (2023). The Personal Data Protection Law (PDPL) passed by Royal Decree No. M/19 of 2021 and amended by Royal Decree No. M/148 of 2023 took effect on 14 September 2023 along with the implementing regulations (SDAIA, 2023; DLA Piper, n.d.); transition period ended in September 2024 with new rules for data transfers (Morgan Lewis, 2024). Sectoral guides extend PDPL requirements to specific areas, for example, government mobile devices management (Mostafa, 2025). Research related to PDPL compliance is scarce.

Cybersecurity

National Cybersecurity Authority developed Essential Cybersecurity Controls (ECC-1:2018, later updated to ECC 2-2024) for government entities and critical infrastructure and Critical Systems Cybersecurity Controls (CSCC-1:2019) for classified critical systems (NCA, 2018, 2019; ISC2, 2025). Alsemairi (2023) explored the problem of employees' compliance with cybersecurity policy within the context of Saudi public sector, emphasizing the importance of raising awareness and creating supportive organizational climate. Studies focused on cloud adoption in Saudi e-commerce point to regulatory compliance and access management as key barriers (Abdullah, 2026). The interaction of cybersecurity controls and PDPL

requirement of data residency deserves more attention.

Anti-Corruption and Integrity

Saudi anti-corruption governance is based on Nazaha which became significantly empowered in 2024 with the expansion of investigatory and enforcement powers which includes, among other provisions, the right to dismiss public officials (Greenberg Traurig, 2024). Altawyan (2020) stressed the importance of whistleblower protection for Saudi economy under Vision 2030. Al Salman (2026) demonstrated that the financial disclosure by public employees, collected through Nazaha reports, proves efficient for the detection of misbehavior. Comparative studies of the situation in Gulf countries highlight digital channels of reporting available in Saudi Arabia, including Nazaha app (Aladwani, 2026). Digital audit research involving Saudi Big Four companies demonstrates that continuous auditing promotes financial integrity (Al Otaibi & Mohamed, 2025).

Tax Compliance

VAT and subsequent e-invoicing requirement introduced an entirely new field of compliance. Tax research suggests that procedural fairness and trust increase voluntary compliance (Hartner *et al.*, 2008) and that responsive regulation reduces base erosion (Alm *et al.*, 2022), the rationale for ZATCA graduated penalties ranging from SAR 5,000 for failure to issue an e-invoice to SAR 100,000 for invoicing by unregistered person (ZATCA, n.d.-a, n.d.-b). The lack of studies on behavior of Saudi firms in respect to VAT compliance is a noted in Section 6.

Research Gap

There are three distinct gaps. The first one is that existing research is domain-specific; none of it considers banking, governance, data protection, cybersecurity, anti-corruption, and tax compliance in a single theoretical framework. The second one is that the empirical literature does not entirely cover the 2023-2024 implementation wave (PDPL enforcement, the 2024 Nazaha law, e-invoicing Phase 2). Finally, there is no framework to manage multi-regulator compliance in Saudi organizations. Sections 4 and 5 address these gaps with regulatory mapping and the Integrated Compliance Governance Framework.

MATERIALS AND METHODS

This systematic review has been designed with full transparency and reproducibility in mind. This section describes the study design, the search strategy, databases, search terms, inclusion/exclusion criteria, screening process, the final corpus of documents, and the analytical approach.

Research Design

Qualitative content analysis with regulatory mapping is applied in this study. Qualitative content analysis is appropriate in the case of heterogeneous body of legal

and empirical evidence that needs to be systematized (Hsieh & Shannon, 2005). Regulatory mapping allows organizing the regulatory obligations, authorities, and affected domains in an explicit matrix form. In addition to being descriptive, the design of the study is analytical since it describes both what the regulatory environment requires and what is reported about implementation and compliance. In other words, this systematic review is separated from the synthesis and recommendations (Sections 4–5 and 6) of the author.

Search Strategy

A structured search was conducted between June and August 2026 in five bibliographic databases (Google Scholar, Scopus, Web of Science, HeinOnline, and Westlaw) and in six official repositories: SAMA Rulebook (rulebook.sama.gov.sa); CMA regulations portal (cma.gov.sa); SDAIA (sdaia.gov.sa); NCA (nca.gov.sa); ZATCA (zatca.gov.sa); Nazaha (nazaha.gov.sa); and the Vision 2030 portal (vision2030.gov.sa). Searches in the official sources were based on the English versions published on the authorities' websites.

The key search terms were “regulatory compliance Saudi Arabia”; “SAMA compliance”; “CMA corporate governance”; “Saudi data protection”; “anti-corruption Saudi”; and “tax compliance Saudi”. The modifiers by domain were added to produce “anti-money laundering compliance Saudi banks”; “corporate governance Saudi listed companies CMA compliance”; “Personal Data Protection Law Saudi Arabia compliance”; “anti-corruption Saudi Arabia Nazaha effectiveness”; “tax compliance Saudi Arabia VAT ZATCA”; “NCA Essential Cybersecurity Controls Saudi”; and “responsive regulation compliance theory”. Boolean operators were used when applicable.

Inclusion and Exclusion Criteria

Sources were selected if they met all of the following criteria: (a) peer-reviewed journal articles, books, book chapters, and examined theses published from 1 January 2017 until the end of the search period (August 2026); (b) official regulatory documents, statutes, royal decrees, rulebooks, guides, and controls enacted by Saudi regulators between 2017 and 2025; (c) legal and regulatory frameworks of the Kingdom; and (d) empirical evidence on compliance behavior, quality of governance or enforcement in Saudi Arabia.

Sources were excluded if they met any of the following criteria: (a) grey literature (non-academic sources, including promotional and vendor materials; industry sources are used only as references for dates and numbers stated in official documents); (b) outdated regulations superseded prior to 2017 (except where used for historical baseline comparison in Section 2.2); (c) instruments enacted prior to 2017 or after 2025; and (d) empirical research conducted in other Gulf/Middle Eastern and North African jurisdictions except where it pertains to Saudi Arabia. International organization's grey literature

was accepted only if it contained documentation of the Saudi-related international benchmarks.

Screening and Final Corpus

The search process yielded 90 unique web search results and 40 scholarly sources found through six searches of scholars' work. Initial screening for topic, duplicates, and non-academic sources was performed at title/abstract stage, while full-text review was focused on primary regulatory instruments available at official government websites and peer-reviewed articles, books, book chapters, and examined theses providing data and/or theory. The resulting corpus consisted of about 50 sources: 14 primary regulatory instruments and official documents, and 36 peer-reviewed articles, books, book chapters, and examined theses. Appendix A contains the search log; Appendix B – the sources inventory.

Analytical Method

The analysis of regulatory environment consisted of four stages. First, open coding of each instrument to identify the issuing authority, legal basis and year of issue, intended addressees, core obligations, and enforcement mechanisms. Second, domain classification – grouping the codes into the six domains. Third, regulatory mapping, i.e., entering obligations into a matrix containing columns for regulator, instrument, addressees, and enforcement tools (Appendix C); comparative matrix for the pre- and post-Vision 2030 periods was developed (see Section 4.2). Fourth, synthesis of peer-reviewed evidence against the backdrop of regulatory mapping to identify convergence, contradictions and gaps. The author's synthesis is limited to Sections 4–5 and is explicitly marked; recommendations presented in Section 6 are not based on findings of the peer-reviewed studies, but rather represent authors' proposals.

Limitations

Four limitations are worth mentioning. First, the review is based on English versions of official documents; Arab guidance might contain additional information not translated into English. Second, the literature on the 2023–2025 implementation phase is being written, thus some findings in this review are based on the regulatory documents, not independent evaluations. Third, the review is qualitative – it maps the obligations but does not quantify compliance rates across the entire population of Saudi organizations. Fourth, publication bias is possible. These limitations affect the recommendations, which avoid generalization.

RESULTS AND DISCUSSION

This section presents the research findings and author's interpretation thereof. Sections 4.1 to 4.3 present the mapped architecture, pre/post-Vision 2030 comparative analysis of the regime (see Table 1 below), and requirements per sector (see Table 2 below); Sections 4.4 and 4.5 present cross-sector challenges and findings summary,

respectively. Tables 1 and 2 contain the synthesized information derived from the main instruments listed in Section 2.

The Post-Vision 2030 Regulatory Architecture

Six key regulators/instrument families are found via the mapping: SAMA, whose Rulebook contains the rules of banking, including account-opening rules, and whose AML/CTF Guide specifies due diligence, suspicious transaction reporting, and senior management responsibilities for financial institutions (SAMA, 2023a, 2023b). CMA, whose Corporate Governance Regulations (2017) mandate comply-or-explain governance requirements for listed companies (CMA, 2017). SDAIA, the regulator administering the PDPL passed under Royal Decree No. M/19 (2021), amended by Royal Decree No. M/148 (2023), and now in force since 14 September 2023, together with implementing regulations (SDAIA, 2023; DLA Piper, n.d.; Morgan Lewis, 2024). NCA, issuing the Essential Cybersecurity Controls (ECC-1:2018, amended to ECC 2-2024) and Critical Systems Cybersecurity Controls (CSCC-1:2019) applying to government entities and critical infrastructure (NCA, 2018, 2019; ISC2, 2025). Nazaha, whose new law of 2024 has enhanced its

investigation and enforcement powers (GreenbergTraurig, 2024). And ZATCA, administering VAT legislation and Fatoorah programme phases 1 (4 December 2021) and 2 (1 January 2023 onwards) (ZATCA, 2021, 2023).

Comparison of the Pre- and Post-Vision 2030 Regulatory Environment

Table 1 offers a pre/post-Vision 2030 comparison of the regulatory environment across seven dimensions, based on the analyzed instruments, and historical baselines established by Alqahtani (2020), Zerban (2017), and Alsulaiman and Alrodhan (2014). The biggest difference is in the type of enforcement that has switched from rule-based/sanctions enforcement to risk-based/escalated model incorporating persuasion, enforcement escalation, and digital compliance consistent with responsive regulation theory (Ayres & Braithwaite, 1992; Mascini & Van Wijk, 2009) and trust/voluntary compliance theories (Alm *et al.*, 2022; Hartner *et al.*, 2008). The second major change is digitization of the compliance interface itself: e-invoicing, electronic reporting, and digital whistleblowing transform the compliance exercise from paperwork to real-time data generation (ZATCA, 2021, 2023; Aladwani, 2026).

Table 1: Comparison of the Pre- and Post-Vision 2030 Regulatory Environment

Dimension	Pre-Vision 2030 environment	Post-Vision 2030 environment (2017–2025)
Institutional architecture	Mandates spread across ministries and general committees; monetary guidance issued through circulars.	Specialized regulators with explicit mandates: SAMA, CMA, SDAIA, NCA, ZATCA, and Nazaha.
Legal codification	Fragmented circulars, resolutions, and scattered statutory provisions; pre-2017 governance code.	Consolidated codification: SAMA Rulebook and AML/CTF Guide (2023); CMA Corporate Governance Regulations (2017); PDPL and Implementing Regulations (2023).
Enforcement style	Rule-based and sanctions-oriented; limited guidance on graduated escalation.	Risk-based, graduated enforcement; comply-or-explain governance logic; responsive escalation consistent with responsive regulation (Ayres & Braithwaite, 1992).
Digital infrastructure	Paper-based filings; limited e-government integration.	Mandatory e-invoicing via Fatoorah (Phase 1, 4 Dec 2021; Phase 2, 1 Jan 2023); digital reporting and monitoring (ZATCA, 2021, 2023).
Data governance	No comprehensive data protection statute (Alsulaiman & Alrodhan, 2014).	PDPL in force 14 September 2023; Implementing Regulations and updated data transfer rules (SDAIA, 2023; Morgan Lewis, 2024).
International alignment	Selective engagement; international scrutiny of terrorist financing controls (Blanchard & Prados, 2007).	G20, FATF, and OECD-aligned tax transparency; Basel-aligned prudential standards; active mutual evaluation participation.
Sectoral coverage	Banking and capital markets primary; uneven coverage elsewhere.	Cross-cutting coverage including energy, healthcare, public sector, and all VAT-registered businesses (NCA, 2018, 2019; ZATCA, 2023).

Sector-Specific Compliance Requirements

Table 2 presents the sector-specific requirements in banking and financial services, capital markets, healthcare, energy and critical infrastructure, public sector, and all VAT-registered businesses, based on the instruments mapped in Section 4.1 above. There are two structural

characteristics to be highlighted here. First, banking and capital markets remain the most developed sectors in terms of layered regulation and empirical literature (Gerged & Agwili, 2020; Boshnak, 2021; Alamri & Alshekmubarak, 2023). Second, critical infrastructure sectors – energy, healthcare, utilities, transport – have

to cope with double compliance of NCA cybersecurity requirements and PDPL data residency requirements, with very limited coverage in the empirical literature (NCA, 2018, 2019; Abdullah, 2026).

Table 2: Sector-Specific Compliance Requirements

Sector	Regulator(s)	Key instruments	Core requirements
Banking and financial services	SAMA	SAMA Rulebook; AML/CTF Guide (2023)	Customer due diligence, suspicious transaction reporting, sanctions screening, senior management accountability, prudential rules.
Capital markets and listed companies	CMA	Corporate Governance Regulations (2017)	Board composition and independence, audit committees, disclosure and transparency, AGM rights, comply-or-explain reporting.
Healthcare	SDAIA; NCA	PDPL and Implementing Regulations (2023); ECC 2-2024	Patient and sensitive data protection, consent management, cybersecurity controls for health information systems.
Energy and critical infrastructure	NCA	CSCC-1:2019; ECC 2-2024	Critical systems cybersecurity controls, resilience obligations, incident reporting to national authorities.
Public sector	Nazaha; NCA; SDAIA	Nazaha Law (2024); ECC; PDPL	Integrity and disclosure obligations, whistleblowing channels, government data security and protective measures.
All VAT-registered businesses	ZATCA	E-invoicing phases (2021–2023) i	Electronic invoice issuance, Fatoorah platform integration, VAT filing, escalation of fines from SAR 5,000 up to SAR 100,000.

Cross-Domain Implementation Challenges

There are four challenges common across all the sectors. First, regulatory fragmentation: the compliance obligations are set by six regulators, each having its own compliance cycle, data definitions, and calendar of enforcement actions, which results in uneven disclosure and enforcement gaps (Alqahtani, 2020; Zerban, 2017). Second, capacity constraints, particularly of SMEs: the systems that big banks can afford and automate become disproportionately burdensome for small firms (Amubarak, 2020), a trend reflected in the phased approach to the e-invoicing rollout (ZATCA, 2023). Third, the question of enforcement consistency: international literature warns of the possibility of formal compliance without any changes in actual behavior in the case of formal AML frameworks (Carr & Jago, 2014; Unger, 2020), while the issue of consistency of Saudi enforcement remains underresearched. Finally, the human and cultural factor: studies of cybersecurity policy compliance (Alsemairi, 2023) and of informal practices such as *wasta* (Alofi, 2017) show that only the culture supportive of formal control works.

Evidence Summary

First of all, the findings show that the transformation of the Saudi compliance architecture has taken place in respect of institutions, instruments and enforcement technology; secondly, that the areas with the most mature implementation are banking and capital markets; and, thirdly, that the key obstacles to implementation remain fragmentation, capacity, consistency, and culture. These conclusions are based on the reviewed literature; the framework in Section 5 is the author's synthesis and the recommendations in Section 6 are built upon it.

Discussion

This section puts together the six compliance domains (5.1), outlines the theoretical contribution of the paper - the Integrated Compliance Governance Framework (5.2), and its practical contribution - the phased implementation roadmap (5.3). This section represents the author's own synthesis: the evidence it is based on is cited but the framework and roadmap are proposed independently by the author.

Integrating the Six Compliance Domains

Domains are not separate silos but different perspectives of the same governance challenge. As an example, take a Saudi digital bank that should comply with obligations of SAMA in terms of prudence and AML/CFT (SAMA, 2023a, 2023b), CMA in case of listing (CMA, 2017), PDPL in relation to customer data (SDAIA, 2023), NCA in terms of cybersecurity (NCA, 2018, 2019), Nazaha in terms of anti-corruption obligations in public procurement (Greenberg Traurig, 2024), and ZATCA in relation to e-invoicing (ZATCA, 2021, 2023). All these obligations impact the same underlying assets – people, data, systems and processes but are managed by different regulators. Consequently, there is duplication of risk assessments, fragmented control testing, and fragmented assurance functions. This situation reflects institutional theory accounts of the convergence that is driven by Vision 2030 as a coercive pressure field (Aldhafiri, 2026). Domains interrelate in substantial ways, for example, PDPL data minimization impacts AML/CFT due diligence data; NCA controls affect integrity of the e-invoicing infrastructure; and quality of corporate governance impacts perception of anti-corruption and data obligations (Alamri &

Alshekmubarak, 2023; Alqahtani, 2020). Thus, the consideration of the domains as a single compliance system is not a mere convenience but a necessity for efficient risk management.

Theoretical Contribution: The Integrated Compliance Governance Framework (ICGF)

The theoretical contribution of the paper is the Integrated Compliance Governance Framework (ICGF) - a four-pillar framework grounded in the theory of legitimacy (Tyler & Lind, 1992; Tyler & Fagan, 2008), responsive regulation (Ayres & Braithwaite, 1992), and institutional theory (Aldhafri, 2026). Pillar 1 Regulatory Intelligence: the organization maintains a constantly updated inventory of the obligations in all the six domains, with ownership, evidence requirements, and deadlines defined. This addresses fragmentation described in Section 4.4 and applies the mapping methodology of this review to the firm itself. Pillar 2 Risk-Based Control Environment: controls are proportionate to the risk assessment and, as is done by the regulators, high-risk activities (cross-border payments, health data, critical systems) are governed by intensive controls whereas routine obligations have proportionate controls (SAMA, 2023b; NCA, 2018, 2019; ZATCA, 2021). Pillar 3 Integrity Culture and Accountability: applying legitimacy theory, this pillar provides for board-level compliance ownership, effective whistleblower channel, wasta prevention measures and ethics training because disclosure and whistleblower mechanisms work as integrity instruments (Al Salman, 2026; Altawyan, 2020), and culture impacts compliance behavior (Alsemairi, 2023; Alofi, 2017). Pillar 4 Technology-Enabled Assurance: technologies for continuous monitoring such as e-invoicing integration, automated transaction monitoring, audit analytics, privacy tooling transform compliance into continuous assurance rather than periodic examination reflecting regulators' own digital infrastructures (ZATCA, 2023; Al Otaibi & Mohamed, 2025; Khan *et al.*, 2025).

ICGF makes two contributions to the theory. First, it extends the doctrine of responsive regulation (Ayres & Braithwaite, 1992) from the regulator's perspective to the internal governance of the regulated organization suggesting application of the same graduated approach (proportionate controls, escalation/de-escalation) to the obligations of the latter. Second, it links institutional pressure (Aldhafri, 2026) to the organizational response by defining the internal structures for absorbing the externally imposed obligations.

Practical Contribution: An Implementation Roadmap for Saudi Organizations

The practical contribution is the phased roadmap for implementing the ICGF, presented as a suggestion with indicative timings that need to be adapted depending on sector, size, and risk profiles of organizations. Phase 1 (Months 0-3): Baseline and mapping: inventory obligations applicable in each of the six areas using Appendix C; identify the current owners of those obligations and

assess the gaps against the four pillars. Phase 2 (Months 4-6): Governance design: establish a single oversight body for compliance with board reporting; approve compliance charter, risk appetite statement and escalation process; establish regulatory change management. Phase 3 (Months 7-12): Control and culture: implement risk-based controls; train staff; establish whistleblowing and integrity mechanisms with senior leadership sponsorship; redesign decision points where wasta can occur. Phase 4 (Months 13-18): Technology and assurance: automate integrated digital channels for regulators and introduce continuous assurance dashboards. Phase 5 (Ongoing): Evaluation: review annually taking into account regulatory changes, enforcement results, and audit findings.

Every phase addresses a specific challenge identified in Section 4.4 (regulatory fragmentation, capacity, culture, enforcement) and builds on instruments proven to be effective in the Saudi environment. This is not supposed to be a blueprint for all organizations; their implementation should be proportionate to risk and so should the ICGF, just like responsive regulation it relies upon.

CONCLUSION

This systematic review concludes that Saudi Arabia's compliance environment has evolved from a fragmented, circular-based, sanctions-focused system into a more consolidated and specialized regulatory system supported by dedicated regulators, rulebooks, digital enforcement platforms, and greater alignment with international standards. Six major compliance areas were identified: financial regulation and AML/CFT, corporate governance, data protection, cybersecurity, anti-corruption, and taxation, with particularly intensive requirements in banking, capital markets, and critical infrastructure. Key implementation challenges include regulatory fragmentation, limited organizational capacity, inconsistent enforcement, and organizational culture. The proposed Integrated Compliance Governance Framework (ICGF), based on regulatory intelligence, risk-based controls, integrity culture, accountability, and technology-enabled assurance, provides a suitable integrated response. Regulators should reduce fragmentation through unified digital compliance identification and reporting, adopt proportionate enforcement, provide sector-specific SME toolkits, and publish aggregate enforcement statistics. Organizational leaders should establish unified compliance oversight, prioritize controls according to risk, strengthen integrity and whistleblowing mechanisms, and digitize compliance assurance. Future research should quantitatively assess compliance rates, evaluate PDPL and cybersecurity implementation and compliance costs, test ICGF across sectors, and examine the mediating role of organizational culture and behaviour.

REFERENCES

Abdullah, S. B. (2026). Cloud security challenges in Saudi e-commerce platforms under Vision 2030. *Journal of Computer Science and Technology Studies*, 8(2). <https://journals.e-palli.com/home/index.php/ajgm>

- alkindipublisher.com/index.php/jcsts/article/view/12867
- Aladwani, A. (2026). *A comparative study of responses to corruption in the Gulf: National efforts of Kuwait, Saudi Arabia and UAE* [Doctoral dissertation, Brunel University London]. Brunel University Research Archive. <https://bura.brunel.ac.uk/handle/2438/33012>
- Alamri, M. A., & Alsheimbarak, I. A. (2023). Corporate governance and business ethics in Saudi Arabia listed banks: an accountability perspective. *Journal of Accounting Research, Organization and Economics*, 6(1). <https://jurnal.usk.ac.id/JAROE/article/view/34774>
- Aldhafiri, Y. F. (2026). Coercive transformation: vision 2030 as a pressure field and organizational dynamics of coercive digital change in Saudi Arabian public sector. *Journal of Intelligent Decision Making and Information Systems*, 3(4). <https://www.jidmis.org/index.php/jid>
- Alofi, M. G. (2017). *Organizational culture in the telecommunication industry of Saudi Arabia: With emphasis on masta* [Doctoral dissertation, Durham University]. Durham E-Theses. <https://etheses.dur.ac.uk/>
- Alqahtani, A. S. H. (2020). *Accounting disclosure and corporate governance mechanisms in Kingdom of Saudi Arabia* [Doctoral dissertation, Victoria University]. VU Research Repository. <https://vuir.vu.edu.au/>
- Al Salman, H. H. H. (2026). The role of disclosure and transparency in developing integrity in the Saudi public sector. *Acta Innovations*, 46. <https://actainnovations.com/index.php>
- Alsulaiman, L. A., & Alrodhan, W. A. (2014). The status of information privacy in Saudi Arabia. *Computer and Information Science*, 7(3).
- Altawyan, A. A. (2020). The significance of emphasizing anti-corruption rules: whistleblowing for a better economic environment in Saudi Arabia towards Saudi Vision 2030. *Arab Law Quarterly*, 34(1), 74–85.
- Amubarak, W. (2020). *Gaps in expectations with regards to the role of independent directors: Evidence from Saudi Arabia* [Doctoral dissertation, Middlesex University]. Middlesex University Research Repository. <https://repository.mdx.ac.uk/>
- Alm, J., Gerbrands, P., & Kirchler, E. (2022). Using “responsive regulation” to reduce tax base erosion. *Regulation & Governance*, 16(1), 36–53. <https://doi.org/10.1111/rego.12359>
- Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.
- Blanchard, C. M., & Prados, A. B. (2007). *Saudi Arabia: Terrorist financing issues* (CRS Report for Congress). Congressional Research Service.
- Carr, I., & Jago, R. (2014). Corruption, money laundering, secrecy, and social responsibility of banks. In B. Rider (Ed.), *Fighting financial crime in the global economic crisis* (pp. 158–181). Routledge.
- Gerged, A. M., & Agwili, A. (2020). The influence of corporate governance on firm value and profitability: a study of Saudi Arabia’s financial and non-financial listed companies. *International Journal of Business Governance and Ethics*, 14(2), 144–165.
- Hartner, M., Rechberger, S., Kirchler, E., & Schabmann, A. (2008). Procedural fairness and tax compliance. *Economic Analysis and Policy*, 38(1), 137–152. [https://doi.org/10.1016/S0313-5926\(08\)50010-5](https://doi.org/10.1016/S0313-5926(08)50010-5)
- Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- Khan, A. A., Alsufyani, A., Alsufyani, N., & Mohamed, M. A. (2025). BAML: a decentralized approach to secure, privacy-preserving financial compliance for enhancing anti-money laundering with blockchain hyperledger and federated learning. *Peer-to-Peer Networking and Applications*, 18(5), Article 270. <https://doi.org/10.1007/s12083-025-02086-6>
- Kingdom of Saudi Arabia. (2016). *Vision 2030: Kingdom of Saudi Arabia*.
- Mascini, P., & Van Wijk, E. (2009). Responsive regulation at the Dutch Food and Consumer Product Safety Authority: an empirical test of assumptions about the theory. *Regulation & Governance*, 3(1), 27–47.
- Morgan Lewis. (2024, September 12). *Saudi Arabia Personal Data Protection Law: Transition period ends September 14*. <https://www.morganlewis.com/pubs/2024/09/saudi-arabia-personal-data-protection-law-transition-period-ends-september-14>
- National Cyber Security Authority. (2018). *Essential cybersecurity controls (ECC)*.
- National Cyber Security Authority. (2019). *Critical systems cybersecurity controls (CSCC)*.
- Saudi Central Bank. (2023a). *Rules for opening an account*.
- Saudi Central Bank. (2023b). *The guide on anti-money laundering and counter terrorism financing (AML/CTF)*.
- Saudi Data & Artificial Intelligence Authority. (2023). *Personal Data Protection Law and its implementing regulations*. <https://sdaia.gov.sa/en/>
- Tyler, T. R. (2018). Psychology and deterrence of corporate crime. In M. L. Benson, D. P. Farrington, & H. J. Smith (Eds.), *Research handbook on corporate crime and financial misconduct*. Edward Elgar.
- Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: why do people help the police fight crime in their communities? *Ohio State Journal of Criminal Law*, 6(1), 231–275.
- Tyler, T. R., & Lind, E. A. (1992). A relational model of authority in groups. *Advances in Experimental Social Psychology*, 25, 115–191.
- Unger, B. (2020). *Enhancing anti-money laundering policy*. Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament.
- Zakat, Tax and Customs Authority. (2023). *E-invoicing: Roll-out phases*.
- Zakat, Tax and Customs Authority. (n.d.-a). *Taxation violation fines*. Retrieved August 31, 2026, from

<https://zatca.gov.sa/en/RulesRegulations/VAT/Pages/Penalties.aspx>
 Zakat, Tax and Customs Authority. (n.d.-b). *ZATCA releases the violations and fines related to e-invoicing*. Retrieved August 31, 2026, from <https://zatca.gov.sa/en/MediaCenter/News/Pages/E-invoicing-Violations-Fines.aspx>
 Zerban, A. M. (2017). Enron of Saudi Arabia: corporate accounting and auditing failures. *Open Journal of Accounting*, 6(4), 105–127. <https://www.scirp.net/journal/paperinformation?paperid=80434>

Appendices

Appendix A: Search Log (Excerpt)

The search was performed in two phases during the period from June to August 2026. Phase 1 searched for the six main strings; Phase 2 searched for the domain variants and theory anchors. Records were selected in two rounds (title/abstract, followed by full-text). Web and scholarly search outputs yielded 90 web results and 40 records respectively. The final corpus included about 50 sources.

Round	Databases / repositories	Query strings	Results	Retained
Round 1	Google Scholar, Scopus, Web of Science, HeinOnline, Westlaw; SAMA, CMA, SDAIA, NCA, ZATCA, Nazaha, Vision 2030 portals	Six core strings: “regulatory compliance Saudi Arabia”; “SAMA compliance”; “CMA corporate governance”; “Saudi data protection”; “anti-corruption Saudi”; “tax compliance Saudi”	55 unique web results	Screened; retained per criteria
Round 2	Same databases and repositories	Domain variants and theory anchors: “AML compliance Saudi banks”; “CG Saudi listed companies CMA”; “PDPL compliance”; “Nazaha effectiveness”; “VAT ZATCA compliance”; “NCA ECC Saudi”; “responsive regulation theory”	35 unique web results	Screened; retained per criteria
Scholar queries	Google Scholar (via scholarly indexes)	Six domain-specific scholar queries (governance, AML, data protection, anti-corruption, tax, theory)	40 scholarly records	Peer-reviewed items retained
Final corpus			90 web + 40 scholarly	About 50 sources (14 primary instruments; 36 peer-reviewed)

Appendix B: Source Inventory (Summary)

The corpus includes about 50 sources, namely: (a) 14 primary legal instruments and official documents such as Vision 2030 document, SAMA Rulebook Account Opening Rules, SAMA AML/CTF Guide, CMA Corporate Governance Regulations (2017), PDPL and Implementing Regulations, NCA ECC and CSCC, Nazaha related instruments including the 2024 law, and

ZATCA e-invoicing and penalties pages and (b) 36 peer-reviewed

Appendix C: Regulatory Mapping Matrix

The matrix links regulator, device, recipients, obligations, and instruments of enforcement for each of the six domains. This is the analytical tool upon which Section 4 is based.

Domain	Regulator	Instrument	Addressees	Core obligations	Enforcement tools
Financial regulation and AML/CFT	SAMA	Rulebook; AML/CTF Guide (2023)	All financial institutions	CDD/KYC, suspicious transaction reporting, sanctions screening, senior management responsibility	Supervisory examinations; sanctions
Corporate governance	CMA	Corporate Governance Regulations (2017)	Listed joint stock companies	Board composition, independent directors, disclosure, AGM rights	Inspections; fines; enforcement actions

Data protection	SDAIA	PDPL (M/19 of 2021, amended M/148 of 2023); Implementing Regulations	Controllers and processors in the Kingdom	Consent, purpose limitation, data transfer rules, data subject rights	Corrective orders; administrative fines
Cybersecurity	NCA	ECC-1:2018 / ECC 2-2024; CSCC-1:2019	Government entities and critical infrastructure	Essential and critical controls; incident reporting; resilience obligations	Compliance reviews; mandated reporting
Anti-corruption and integrity	Nazaha	Nazaha Law (approved 23 July 2024)	Public officials; entities interacting with government	Integrity obligations, financial disclosure, whistleblowing	Investigations; prosecution referrals; dismissal powers
Taxation	ZATCA	VAT framework; e-invoicing (Phase 1: 4 Dec 2021; Phase 2: 1 Jan 2023)	All VAT-registered businesses	E-invoice issuance, Fatoorah integration, VAT filing	Fines from SAR 5,000 up to SAR 100,000