



American Journal of Economics and Business Innovation (AJEBI)

ISSN: 2831-5588 (ONLINE), 2832-4862 (PRINT)

VOLUME 5 ISSUE 3 (2026)

**PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA**

Strategic Risk Review Strategic Risk and Compliance Planning in Saudi Arabia a Unified Framework for Vision 2030 Transformation

Mohamed Abdelhalim Soliman^{1*}

Article Information

Received: July 05, 2026

Accepted: September 19, 2026

Published: October 20, 2026

Keywords

*Cybersecurity Governance,
Enterprise Risk Management,
Regulatory Compliance, Saudi
Regulatory Framework, Saudi
Vision 2030, Strategic Risk
Management*

ABSTRACT

Saudi Arabia's Vision 2030 is one of the world's most powerful national transformation programmes designed to diversify the economy, reform society and speed up technological progress across all sectors of the Kingdom's economy. As organizations become increasingly aware of the many trends that could impact their security, the risk landscape is now as multifaceted, from regulatory, technological, geopolitical, and operational perspectives, as ever before. The authors proposed a blended Strategic Risk and Compliance Planning (SRCP) framework that combines the elements from the COSO Enterprise Risk Management (ERM) framework, the Saudi Data and AI Authority (SDAIA) regulations, and the guidelines from the ISO 31000, along with the Saudi Central Bank (SAMA), Capital Market Authority (CMA), the National Cybersecurity Authority (NCA), the Zakat, Tax and Customs Authority (ZATCA). The Vision 2030 Annual Report 2025 highlights the scale and direction of these structural changes: SMEs contribute 22.9% to GDP, female labor force participation is 34.5%, and non-oil activities currently account for roughly 55% of GDP. Concurrently, the regulatory environment has been growing as well, incorporating the necessary cybersecurity baselines of the NCA (the Essential Cybersecurity Controls (ECC-2:2024); the strict obligations under the data governance of the PDPL (the Personal Data Protection Law) entered into force from September 2024; and the new tax compliance requirements due to the phased implementation of ZATCA's e-invoicing registration. The vision's transition from 2030 is not only an economic roadmap but a reimagining of the platform where risks and compliance will exist for all entities in Saudi Arabia. The article introduces a unified approach to ensure equivalent international requirements meet Saudi jurisdiction regulatory requirements. It is action-oriented: research findings are paired with strategic recommendations, sector-specific applications are clarified across banking, health care, energy, and technology, and an implementation roadmap provides a comprehensive plan to operationalize the SRCP framework for organizations that wish to.

INTRODUCTION

The Kingdom of Saudi Arabia is changing beyond anything which humanity has seen before. His Royal Highness Crown Prince Mohammed bin Salman initiated the Saudi Vision 2030 in 2016 to reduce the dependence of the Kingdom on oil-based economy, broaden the economy, build up public services, and transform Saudi Arabia into a world-class hub for investment opportunities. Today, nearly 10 years later, reform has started to gain momentum as new regulatory institutions are established, comprehensive legislation first passed and the more recent giga-projects, such as NEOM, Qiddiya and the Red Sea Development will bring a new physical and economic situation.

The issue before the C-suite executive, board member or chief risk officer in such a scenario is straightforward; how can an organization move for aggressive growth and transformation, whilst maintaining strong risk management and regulatory compliance? Traditional, siloed approaches to risk and compliance, with a risk function, compliance team, internal audit, and technology security working in isolation, is not enough. One consistent and coherent way that incorporates principles of risk management into risk strategy formulation and links it to the particular

regulatory framework of the Saudi jurisdiction is required. This article aims to answer that question. It starts with an overview of the strategic context: Vision 2030 transformation, and the new risk landscape it has created. It then presents the SRCP framework, and how the COSO ERM and ISO 31000 frame works can be integrated and adapted to the Saudi regulatory context. The following sector-specific applications are followed by an implementation roadmap and illustrative case-studies. The article ends with important tips for leaders who are entering this voyage.

The Strategic Context: Vision 2030 and the New Risk Landscape

Vision 2030: Transformation at Scale

The vision is developed from 3 pillars: A Vibrant Society, A Thriving Economy, and An Ambitious Nation. Specific strategic goals and key performance indicators are tracked under each pillar and reported each year. The Council of Economic and Development Affairs' 2025 Annual Report capture significant gains on various fronts.

Based on data from the Vision 2030 Annual Report 2025, the following indicators illustrate the scale of transformation:

¹ International Business Academy of Switzerland (IBAS), Switzerland

* Corresponding author's e-mail: mohamedabdelhalimmostafasoliman@researchpublication.co

Table 1: Based on data from the Vision 2030 Annual Report 2025, the following indicators illustrate the scale of transformation:

Indicator	Vision 2030 Target	2025 Reported Achievement
Non-oil GDP share	By 2030: diversified economy	~55% of GDP from non-oil activities
GDP growth	Sustained growth above G20 average	4.5% GDP growth reported
Female labor force participation	30% by 2030	34.5% achieved (exceeded target)
SME contribution to GDP	35% by 2030	22.9% (progressing toward target)
Foreign direct investment (FDI)	Increase to 5.75% of GDP	2.8% of GDP (improving)
TVET graduate employment	Aligned with market needs	47.41% employment rate reported
Foreign visitors (annual)	150 million by 2030	~30 million (Q1 2025 average, +3.8% YoY)

These are clear indicators that the Vision 2030 transformation is showing tangible economic results, rather than just talking-up the idea. There are however, some risks which accompany each of these achievements. The diversification of margin to non-oil activities creates additional risks from markets. Given the presence of more women in the workforce, HR policies and workplace safety plans must be adjusted. This expansion also presents supply-chain and counterparty risk issues for bigger businesses relying upon small and medium-sized companies, many of which are in the early stages

of development. Foreign tourists broaden the exposure of risks arising from infrastructure, security and public health.

The Expanding Regulatory Architecture

With the changing economy, the regulatory framework has undergone transformation. Saudi Arabia has created, or empowered several regulatory bodies that all have strict requirements and standards to abide by. The table below shows the main regulators and their key instruments that are relevant for risk and compliance planning.

Table 2: Key Saudi Arabian Regulatory Authorities, Primary Instruments, and Requirements for Risk and Compliance Planning

Regulator	Primary Instrument	Key Requirements
Saudi Central Bank (SAMA)	SAMA Rulebook — Risk Management Framework	Enterprise risk management policies, operational risk controls, cyber risk control framework, AML/CFT compliance, business continuity requirements for financial institutions
Capital Market Authority (CMA)	Corporate Governance Regulations (2017)	Board composition and independence, audit committee requirements, internal control systems, risk management committee mandate, disclosure and transparency obligations for listed companies
National Cybersecurity Authority (NCA)	Essential Cybersecurity Controls ECC-2:2024	Mandatory cybersecurity baseline for national entities and private sector; covers governance, asset management, access control, incident response, and third-party risk
Saudi Data & AI Authority (SDAIA)	Personal Data Protection Law (PDPL) — enforced Sept 2024	Lawful basis for processing, consent management, data controller registration, cross-border transfer restrictions, breach notification within 72 hours, data subject rights
Zakat, Tax & Customs Authority (ZATCA)	E-Invoicing (Fatoorah) Regulations — Phases 1 & 2	Phase 1: generation of compliant e-invoices (since Dec 2021); Phase 2: integration with ZATCA systems for real-time invoice submission and clearance for targeted taxpayer groups

Regulatory framework is not a fixed place; it is moving! After the original ECC-1:2018 controls, the NCA has updated and expanded these controls in the current ECC-2:2024 to address the rapidly changing threat environment. SDAIA issued Implementation Guidelines and Registration requirements in order to bring operational detail to the principles of the PDPL. ZATCA's Phase 2 integration process works in stages, gradually gaining access to more and more taxpayers. Compliance is thus an ever-evolving conversation on the agenda for businesses, not a project to complete once.

The Convergence of Risk Domains

One of the characteristics of the Saudi risk landscape is the fusion of risk domains, each of which is traditionally handled separately. Now, there is a strong intertwining of cybersecurity risk, data protection risk, financial reporting risk, tax compliance risk, and strategic risk. A cybersecurity incident can bring about PDPL notification requirements, financial reporting obligations, reputational harm and regulatory fines at the same time. A breach of e-invoicing compliance regulation can also lead to tax penalties, audit consequences and disruption in the

supply chain. The SRCP framework outlined in the next section will deliver an enterprise-wide approach to risk and compliance that is needed for this convergence.

MATERIALS AND METHODS

Research Approach and Scope

Analytical Procedure and Limitations

The review proceeded in three stages. First, the source materials were organized by strategic objective, risk domain, regulatory authority, and implementation requirement. Second, the COSO ERM components and ISO 31000 principles were compared with the obligations and control expectations identified in the Saudi instruments. Third, the recurring integration points were synthesized into the five SRCP domains and then tested conceptually against the needs of banking, healthcare, energy, and technology organizations. The analysis is interpretive and implementation-oriented; it does not estimate causal effects or claim statistical generalizability. Regulatory requirements may also change, so organizations should verify current official guidance before implementation.

The purpose of this article is a synthesis that is only able to address questions from a practitioner perspective, rather than a quantitative empirical study. The research methodology included a systematic review of the following: (1) official Vision 2030 documents and the Council of Economic and Development Affairs annual reports; (2) regulatory instruments published on SAMA, CMA, NCA, SDAIA, and ZATCA official websites; (3) COSO Enterprise Risk Management - Integrating with Strategy and Performance framework (2017), and ISO 31000:2018 Risk Management Guidelines; and (4) peer-reviewed academic literature related to ERM implementation, compliance governance and risk management in the Saudi and GCC region. The analysis was done through qualitative synthesis, which identified the convergences, gaps, and integration points that exist between the international frameworks and the Saudi regulatory requirements. The following SRCP is the output of the analytical process of the synthesis. The figures referenced are based on the NC State 2025 State of Risk Oversight Report (16th Edition) and the Vision 2030 Annual Report 2025. Illustrative case studies are composite stories based on the reported development within a sector that are clearly identified as illustrative - not specific named organizations.

RESULTS AND DISCUSSION

The qualitative synthesis produced an integrated framework rather than a new statistical model. The principal result is that strategic risk management and regulatory compliance should be designed as one decision system for organizations operating in the Vision 2030 environment. Across the reviewed sources, five findings were consistent: governance must assign clear accountability; risk appetite must inform strategic choices; risk assessment must combine enterprise and

regulatory exposures; compliance obligations must be linked to controls and monitoring; and technology and data assurance must be treated as strategic capabilities rather than isolated technical functions.

The findings also explain why a unified approach is necessary. Vision 2030 expands the scale and speed of organizational change, while the Saudi regulatory architecture increasingly places overlapping demands on governance, cybersecurity, personal-data protection, tax administration, and operational resilience. A single event can therefore create strategic, financial, operational, legal, and reputational consequences at the same time. The sections that follow discuss how the SRCP framework responds to this convergence and what the synthesis implies for implementation in different sectors.

The SRCP Framework

Finding 1: Integrated SRCP Framework

Framework Contribution and Interpretation

This article proposes one synthesis Strategic Risk and Compliance Planning (SRCP) framework, obtained through combining the COSO Enterprise Risk Management (ERM) framework (2017), the risk management guidelines of ISO 31000:2018 and the Saudi regulatory requirements adopted by SAMA, CMA, NCA, SDAIA, and ZATCA. The SRCP framework brings together five interconnected domains—that of Governance and Culture, Strategy Alignment, Risk Identification and Assessment, Compliance Integration, and Technology and Data Assurance—in one operational framework customized for the Vision 2030 transformation context. This is the first published framework of international risk management standards mapping the complete range of Saudi regulatory instruments, all in one location and in a format ready for implementation.

Framework Architecture

The five interrelated domains in the SRCP framework are based on certain aspects of the COSO ERM and the ISO 31000 frameworks and correspond to specific Saudi regulatory needs. The framework is not COSO or ISO, but a specially designed synthesis that builds on both COSO's focus on governance and strategic alignments, and the principles-based process architecture of ISO 31000, bringing in the compliance-specific obligations of the Saudi jurisdiction.

Domain 1: Governance and Culture

Governance and culture drives the organization's tone at the top, laying the ground mold and defining the structures, ethical standards, and accountability responsibilities for the conduct of all risk management activity, based on the COSO ERM framework. Within the Saudi context, this stands on the shoulders of the CMA Corporate Governance Regulations (2017), which mandate the presence of independent directors on the boards of listed companies, the formation of audit and risk management committees, as well as internal control systems. The

CMA rules prescribe that the board of directors shall be responsible for overseeing the company's systems of risk management and of internal control, while the risk management committee (or the audit committee doing the job) is required to have members who are experts in the area.

Organizations that are listed or non-listed operating in Saudi Arabia should consider adopting governance arrangements at a minimum that meet or exceed the standards of the CMA Corporate Governance Regulations. This encompasses setting up a board-level risk management committee, appointing a board-level Chief Risk Officer (CRO), and integrating risk culture into executive performance reviews. Governance maturity is shown to be the most critical gap across the board. Of the executives surveyed, only 32% rated their state of risk oversight as "mature" or "robust" in the NC State 2025 State of Risk Oversight Report; only 11% said their ERM processes provide a strategic advantage.

Domain 2: Strategy Alignment

Risk management integration with strategy-setting is key in both COSO ERM and ISO 31000. COSO's second element, Strategy and Objective-Setting, involves analyzing the business environment, establishing a risk appetite, and establishing objectives that are consistent with that appetite. The principle of integration, which is the central theme of ISO 31000, requires the integration of risk management into governance and organizational activities. Within the Saudi context, it involves the explicit reliance on risk appetite alongside Saudi Vision 2030 Strategic Objectives, in situations such as going for Saudization goals, exploration of new sectors, or working in Saudi giga-projects supply chains. The organizations are encouraged to have a written Risk Appetite Statement with clear reference to Vision 2030 strategic priorities relevant to the organization's sector and business model. The intent of this statement is to establish quantitative limits for financial, operational, regulatory and reputational risk and should be assessed at least once per year by the board. More critically, the

NC State report revealed that just 30% of organizations incorporate risk exposure information into the capital planning process, and the NC State report explicitly recognizes this through the mandate for "risk-adjusted capital planning.

Domain 3: Risk Identification and Assessment

ISO 31000 introduces a systematic approach for identifying, analyzing and assessing risks whilst COSO's Performance component focuses on prioritizing risk severity and having a portfolio view. The SRCP framework calls for organizations to keep a detailed Enterprise Risk Register, which is updated at least quarterly, and which is specific enough to clearly and specifically contain regulatory compliance risks for all applicable Saudi regulators. Risk assessment must be qualitative and quantitative; heat maps and detailed scoring for operational management, board-level.

Responding executives, according to the 2025 State of Risk Oversight Report, are concerned about increasing risk complexity (61%) and competition for priorities and limited resources (41%) to further the evolution of risk management. The SRCP approach tackles these challenges by integrating risk identification into go/no-go decision-making processes, for example, as embedded in strategic planning cycles, in project approval gates, and in regulatory change monitoring, rather than as a stand-alone, resource-heavy activity.

Domain 4: Compliance Integration

The COSO and ISO frameworks provide the foundation for this domain, and it is in this domain that the SRCP framework contributes the most. Although compliance assessment is part of the COSO ERM objectives, regulatory risk is recognized in ISO 31000; neither standard contains the necessary compliance architecture for Saudi organizations. The SRCP framework brings together compliance obligations of five key Saudi regulators in the risk management process, so that Saudi regulatory requirements aren't just recorded in a compliance register but also connected to risk assessments, controls and monitoring.

Table 3: Institutional Affiliations and Designations of Academic Experts

Regulator	Key Obligation	Integration Point in SRCP
SAMA	Risk management policies and cyber risk controls for financial institutions	Domain 1 (Governance) and Domain 3 (Assessment) — ERM policy must align with SAMA Rulebook risk management framework
CMA	Board oversight, risk committee, internal controls, disclosure	Domain 1 (Governance) — Board and committee structure must satisfy CGR 2017 requirements
NCA	ECC-2:2024 mandatory cybersecurity controls	Domain 5 (Technology & Data) — Cybersecurity control baseline mapped to ECC-2:2024 domains
SDAIA	PDPL data protection compliance	Domain 5 (Technology & Data) — Data governance, consent management, breach notification protocols
ZATCA	E-invoicing Phases 1 & 2, VAT compliance	Domain 4 (Compliance) — Tax compliance processes integrated with financial systems and audit trails

Domain 5: Technology and Data Assurance

Technologies and data assurance has become a space unto itself because it has become a strategic risk domain crossing the cybersecurity, data protection and digital transformation fields. The NCA's ECC-2:2024 provides a comprehensive cybersecurity control baseline which has now become mandatory for the private sector as well as government entities. The PDPL, which took effect across all of SDAIA from the 1st of September 2024, applies to all organisations processing personal information of any individual in the Kingdom. In addition, the SRCP framework invites organisations to have a consolidated technology and data risk register for both ECC-2:2024 and PDPL, and to establish control testing and response procedures for data breaches that meet the PDPL notification requirement of 72 hours.

Organizations should be performing a gap assessment versus ECC-2:2024 in the first 90 days of SRCP to identify those areas with controls that have not yet been set up, including governance, access management, and incident response controls. To meet the PDPL requirements, we suggest that a data inventory and mapping exercise be performed to locate all recorded personal data activities, legal bases, and cross-border transfers, followed by the registration of a personal data controller, when required, with SDAIA.

Discussion of Findings

Taken together, the framework domains indicate that compliance maturity is not separate from organizational performance. The reported maturity gap in enterprise risk oversight, the limited use of risk information in capital planning, and concerns about risk complexity and constrained resources point to a practical governance problem: risk information is often available but is not consistently translated into investment, project, and operating decisions. The SRCP framework addresses this problem by assigning ownership, linking regulatory obligations to enterprise risks, and establishing recurring evidence through risk indicators, control testing, management reporting, and independent assurance. These are analytical implications of the reviewed evidence, not measured outcomes from a field trial; their effectiveness should therefore be validated through organization-level implementation and follow-up assessment.

Sector-Specific Applications

At its core, the SRCP is sector agnostic, yet each specific sector should consider how to shape the application of the framework to their unique risk profile, regulatory responsibilities, and strategic goals. The framework is explained below in relation to four important clusters of the Saudi economy.

Banking and Financial Services

Saudi Arabia has one of the most regulated industry sectors, that of banking and financial services, over which SAMA has wide regulatory authority. SAMA's

Rulebook contains comprehensive requirements for risk management in relation to credit risk, market risk, operational risk, liquidity risk, and cyber risk. Financial institutions are required to demonstrate to SAMA that their proposed policy regarding risk management and control is sufficient and appropriate for monitoring and controlling all material risks. Listed financial institutions are also subject to standards on board composition and disclosure in the CMA's Corporate Governance Regulations.

The SRCP framework for financial services organizations should prioritize the following: (1) An extensive enterprise risk management policy conforming to the SAMA Risk Management Framework (2) Board-level risk and audit committees with members with a good level of financial literacy (3) The integration of SAMA cyber risk control requirements into the technology and data assurance domain (4) AML/CFT compliance monitoring integrated into operational risk processes (5) Stress testing and scenario analysis integrated with risk appetite statement.

Healthcare

Saudi Arabia is experiencing significant change within the healthcare industry across the country, including the implementation of various privatization programs, the creation of new regulations, and the Private Health Holding Company. Healthcare organizations have a unique risk profile: clinical risk, patient safety risk, data protection, and regulatory compliance risk. The PDPL is especially so because health data is considered sensitive and the NCA's ECC-2024 seems to be applicable to healthcare organizations as national infrastructure.

It is recommended that the healthcare organization that adopts the SRCP framework expand the risk register to contain a list of clinical risk categories: patient safety incidents, medication errors and quality of care indicators, with the basic enterprise risk categories. Health data should be treated as a special category under PDPL, and breach response procedures should take into account the greater sensitivity of case presentation as medical records.

Energy and Petrochemicals

The energy and petrochemicals industry represents a pivotal sector within the Saudi economy, where severe risks are being created from the global energy transition, energy price volatility, geopolitical risk and the Kingdom's own agenda of diversification. In the Journal of Intelligent Decision Making and Information Sciences, Ali (2026) has researched risk governance and the resilience of insurance markets in the Saudi energy sector for sustainable development in the post-Vision 2030 era, reflecting ESG's, regulatory compliance's and the capacity of reinsurers' importance in energy. Furthermore, integrated risk management models in large-scale infrastructure projects in Saudi Arabia (Jafri, 2026) reveals that risk management is a strategic support rather than a compliance purpose for significant energy and infrastructure projects.

Energy sector organizations applying the SRCP framework are encouraged to include environmental risk and transition risk (as part of the shift away from hydrocarbons globally) in the SRCP strategy alignment domain. Operational risk assessments should include process safety, asset integrity and supply chain resilience; compliance integration should cover any obligations from the ZATCA compliance on taxes for energy sector and customs duties of imported equipment and materials.

Technology and Digital Services

The vision 2030 can also be applied to the technology sector, which encompasses various initiatives, including the Generative AI Accelerator (GAIA), the National Data Quality Programme, and SDAIA's overarching vision to promote AI and data competencies. In addition to the NCA and SDAIA regulatory framework, companies in the technology sector in the Kingdom are also subject to various other regulatory requirements, including those related to intellectual property, cross-border data transfer, and new international legal considerations regarding AI governance.

For technology organizations implementing the SRCP

framework, the NCA ECC-2:2024 and the SDAIA PDPL are the main compliance anchors for Domain 4 and Domain 5, especially with respect to cloud security controls (the NCA has published Cloud Cybersecurity Controls: CCC-2:2024) and requirements for data location. The risk register should capture emerging technology risks, such as AI model bias, algorithmic transparency and third party API dependencies, while the domain of technology and data assurance should capture ongoing monitoring of cloud infrastructure configurations.

Implementation Roadmap

The SRCP framework is intended to be implemented in a phased manner for 18 months. The following roadmap is broken down into three six month buckets of deliverables and success criteria. The timeline should be adjusted based on the maturity of the organization, sector-specific needs and resources.

Phase 1: Foundation (Months 1–6)

The foundation phase establishes the governance structures, policies, and baseline assessments required for SRCP implementation.

Table 4: SRCP Implementation Roadmap: Phase 1—Foundation (Months 1–6)

Month	Activity	Deliverable
1–2	Secure board and executive sponsorship; designate CRO and risk committee	Board resolution, CRO appointment, risk committee charter
2–3	Conduct current-state risk maturity assessment (using RIMS RMM or equivalent)	Maturity assessment report with gap analysis
3–4	Develop enterprise risk management policy aligned with COSO ERM and ISO 31000	Approved ERM policy document
4–5	Conduct ECC-2:2024 gap assessment and PDPL data inventory	Cybersecurity gap report; data processing inventory
5–6	Draft Risk Appetite Statement linked to Vision 2030 strategic objectives	Board-approved Risk Appetite Statement

Phase 2: Integration (Months 7–12)

The integration phase operationalizes the framework by building risk and compliance processes into day-to-day

operations and establishing monitoring and reporting mechanisms.

Table 5: Integration Phase Implementation Plan (Months 7–12)

Month	Activity	Deliverable
13–14	Develop comprehensive enterprise risk register with regulatory risk mapping	Live risk register with risk owners and scoring
14–15	Design and implement compliance monitoring for SAMA, CMA, NCA, SDAIA, ZATCA obligations	Compliance monitoring dashboard
15–16	Implement Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs)	KRI/KPI framework with thresholds and escalation protocols
16–17	Conduct organization-wide risk workshops to validate risk assessments	Updated risk assessments; risk heat maps
17–18	Establish board-level risk reporting cadence and formats	Board risk reporting template and schedule

Phase 3: Optimization (Months 13–18)

The optimization phase focuses on continuous improvement, technology enablement, and embedding

risk-aware decision-making into the organizational culture.

Table 5: Optimization Roadmap (Months 13–18): Activities and Deliverables

Month	Activity	Deliverable
13–14	Evaluate and select GRC technology platform for integrated risk and compliance management	Platform selection decision and implementation plan
14–15	Conduct first comprehensive SRCP framework effectiveness review	Effectiveness review report with improvement recommendations
15–16	Implement risk culture training programme across all organizational levels	Training completion metrics; culture survey results
16–17	Integrate risk-adjusted capital allocation into strategic planning cycle	Updated capital allocation framework
17–18	Conduct external assurance review of SRCP implementation	Independent assurance report; certification roadmap

Illustrative Case Studies

Case Study 1: A Regional Bank Adopting the SRCP Framework

The mid-sized regional bank operating in the Kingdom of Saudi Arabia was under growing regulatory stress due to SAMA's new risk management expectations, as well as SAMA ECC-2:2024 cybersecurity controls and SDAIA's PDPL for customer data. The bank's risk management operational processes were historically compartmentalized: operational risk management, credit risk management, and compliance are managed separately from one another, and there was little visibility on the risk profile at the board level.

The bank started with making a risk management committee at the board level, comprising independent directors who have risk management expertise (Domain 1). The risk appetite statement was updated to clearly include the bank's financial sector development targets as set out by Vision 2030 (Domain 2). The enterprise risk register resulted from identifying and categorizing the risks faced by the enterprise and documenting their probability of occurrence and potential impact. This included incorporating into a single view SAMA regulatory requirement, the NCA cyber security controls, and the data protection obligations under SDAIA (Domains 3 and 4). The technology and data assurance domain was enhanced by adding priority areas identified in a gap assessment on ECC-2:2024 (which includes areas related to access control and incident response, Domain 5).

Key outcome: The bank gained a Board-level risk reporting view, and its compliance monitoring do-overs were trimmed by around 30%, having transitioned to such a degree that it is now ready for SAMA examinations with documented evidence of integrated risk and compliance management within the 12 months. The bank has strengthened its risk maturity level from Level 2 (Emerging) to Level 3 (Conforming) based on the RIMS Risk Maturity Model.

Case Study 2: A Healthcare Provider Navigating PDPL and ECC-2:2024

In a multi-facility healthcare organization in the Kingdom (KK), requirements were identified to deal with PDPL

compliance for sensitive patient health-related data, as well as the ECC-2:2024 cybersecurity baseline requirement. Its existing data protection measures were scattered among facilities, and there wasn't any centralized data inventory or breach response approach.

The provider mapped out a comprehensive overview of all its processing activities, lawful bases, and cross-border transfers, using the SRCP framework (Domain 5). A single breach notification process was put in place to comply with the PDPL requirements for notification within 72 hours and roles were assigned to the officers responsible for data protection at each facility. The ECC-2:2024 gap assessment focused on key vulnerabilities in the healthcare sector, including those related to security in medical devices, access to electronic health records, and risks associated with third-party vendors. The governance domain was bolstered with the appointment of Senior Management, with a Chief Data Protection Officer reporting directly to the board's risk committee (Domain 1).

Key outcome: The healthcare provider is registered as a PDPL with SDAIA, had measurable improvements in cybersecurity control coverage, and implemented a repeatable annual review cycle for data protection and cybersecurity compliance. The organization decreased the average detection time when it introduced monitoring controls, but this exact value needs to be quantified through a more longitudinal measurement.

Case Study 3: An Energy Company Integrating ESG and Transition Risk

A key energy firm understood the necessity for a land grab with the arrival of the worldwide energy shift and the diversification coverage it sought for Vision 2030. In addition, there was a need to add two other new categories of risk: environmental, social and governance (ESG) risk and energy transition risk, which were not traditional risk categories.

The SRCP framework was used, with particular focus given to Domain 2 (Strategy Alignment), and the use of Transition Risk scenarios was included in the strategic planning cycle. The risk appetite statement was extended to include direct commitments for ESG Saudi targets. Increased new carbon reporting requirements and

environmental regulation requirements were added to Domain 4 (Compliance Integration). The company also took advantage of Domain 5 (Technology and Data Assurance) for installing emissions monitoring equipment and environmental data management platforms.

Key outcome: The energy company linked ESG risk to its enterprise risk register and put it under board-level oversight for transition risk, and aligned its capital allocation to Vision 2030 goals and Saudi Green Initiative goals. However, the organization's risk management has moved from compliance to strategy, aligning with the highest level of risk management maturity outlined in the COSO ERM framework.

Key Recommendations for Leaders

As a result of the research conclusions and framework outlined in this article, the following recommendations are presented to the C-suite executives, board members and risk and compliance professionals dealing with these challenges in Saudi Arabia.

For Boards and C-Suite Executives

- Raise risk governance to the board-room. Appoint a board level risk management committee with independent members who have risk management experience, as required by CMA Corporate Governance Regulations (2017).
- Connect risk appetite to Vision 2030. Maintain and regularly review a Risk Appetite Statement, revealing the organization's targets under its Vision 2030 strategy, and establishing clear quantitative limits on three types of risk – financial, operational, regulatory and reputational.
- Integrate risk into decision-making about capital allocation. Implement risk exposure information in capital allocation and strategic investment decisions. Current figures, according to the report by NC State 2025, show that just 30% of organizations currently do this, offering a competitive edge opportunity to those that embrace it.
- Make investments in risk leadership. Designate a Chief Risk Officer whose role is to have direct access to the board and be cross-functional with risk, compliance and technology assurance responsibilities.

For Risk and Compliance Professionals

- Standardize risk and compliance registers. Create a single, comprehensive risk and compliance register, connecting the COSO ERM components, the ISO 31000 principles, and Saudi regulatory requirements from SAMA, CMA, NCA, SDAIA, and ZATCA.
- Focus on compliance with cybersecurity basics. Do a gap assessment for NCA ECC-2:2024 in the first 90 days of implementation of the framework, focusing on the domains of governance, access control, and incident response.
- Achieve PDPL compliance. Perform a PDPL data inventory and mapping process and register with SDAIA as a data controller if applicable, and implement a breach notification plan that complies with the 72-hour standard.

- Set up KRIs and reporting schedule. Adopt Key Risk Indicators (KRIs) along with thresholds and escalation procedures. Implement regular board risk reporting cadence (at least quarterly) and Key Risk Indicators (KRIs) with defined thresholds and escalation procedures.

- Adopt GRC technology. Review and deploy a GRC technology platform that offers a consistent view of risk, compliance, and audit administration, eliminating disparate spreadsheets and point technologies.

For Sector Leaders

- Banking: Ensure alignment of ERM policy with SAMA Risk Management Framework; establish integration of AML/CFT monitoring in operational risk processes; implement SAMA cyber risk control requirements.
- Healthcare: Add clinical risk categories to the risk register; add a PDPL control for medical data; add controls to ECC-2:2024 for medical device security.
- Energy: Include environmental, social, and governance (ESG) and transition risk within the scope of strategy alignment; include process safety and asset integrity within operational risk assessments; align with Saudi Green Initiative goals.
- Technology: Utilize NCA ECC-2:2024 as primary compliance anchor and SDAIA PDPL, Monitor Cloud Security Controls (CCC-2:2024), and address Risks from AI Governance and Algorithmic Transparency.

CONCLUSION

The Vision 2030 transformation has transformed the risk and compliance landscape of every organization operating in Saudi Arabia's Kingdom. Together with the emerging risk landscape surrounding rapid economic diversification, a growing regulatory landscape, and the ongoing digital transformation, an integrated, strategic, and forward-looking approach to managing risk is needed, as opposed to the more reactive, siloed thinking of the past.

The Strategic Risk and Compliance Planning (SRCP) framework described in this article provides a potential solution to this challenge. The framework fuses the COSO Enterprise Risk Management framework and the ISO 31000 Risk Management guidelines with the specific requirements of SAMA, CMA, NCA, SDAIA and ZATCA, offering a unified and implementation-ready model specific to the Saudi jurisdiction. The five domains – Governance and Culture, Strategy Alignment, Risk Identification and Assessment, Compliance Integration, and Technology and Data Assurance – encompass all aspects of risk and compliance activity that organizations have to operate.

The 18-month implementation roadmap offers a sequential, attainable process of from foundation to integration to optimization. The sector-specific applications highlight the versatility of the framework in the banking, healthcare, energy and technology sectors. While they are, of course, fictional examples, the illustrative case studies demonstrate real-world issues and

results that organizations will face.

This investment strategy is not done purely for compliance; for leaders ready to invest, the rewards are both significant and plentiful. According to the NC State 2025 State of Risk Oversight Report, just 11% of executives report that their ERM process is providing strategic advantage. Organizations that embrace the SRCP framework can become a part of that minority – moving risk management from defense and deterrence to the strategic corner, to become boldly able to pursue Vision 2030 goals. That ability will likely be the greatest risk investment an organization can make in an environment of unprecedented change. The organizations that will succeed with Vision 2030 won't be those that avoid risk; they'll be the ones that manage it strategically, with integrated processes, and, of course, regulatory intelligence.

REFERENCES

- Ali, M. A. A. (2026). Sustainable Risk Governance and Insurance Market Resilience in Saudi Arabia under Vision 2030: A Review of ESG, Regulation, and Reinsurance Capacity. *Journal of Intelligent Decision Making and Information Sciences*. Available at: <https://www.jidmis.org/index.php/jidmis/article/view/1058>
- Capital Market Authority (CMA). (2017). *Corporate Governance Regulations*. Kingdom of Saudi Arabia. Available at: <https://cma.gov.sa/en/RulesRegulations/Regulations/Pages/details.aspx?code=2>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*. Durham, NC: COSO. Available at: <https://www.coso.org/erm-framework>
- ERM Initiative at NC State University. (2025). *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices* (16th Edition). Raleigh, NC: Poole College of Management. Available at: <https://erm.ncsu.edu/resource-center/2025-the-state-of-risk-oversight-an-overview-of-enterprise-risk-management-practices-16th-edition/>
- International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk Management—Guidelines*. Geneva: ISO. Available at: <https://www.iso.org/iso-31000-risk-management.html>
- Jafri, S. M. D. (2026). Integrated Risk Management and Process Improvement Models for Large-Scale Infrastructure Development in Saudi Arabia. *Global Academic Journal of Economics and Business*, 8(3), 472–480. Available at: https://www.gajrc.com/media/articles/GAJEB_83_472-480.pdf
- National Cybersecurity Authority (NCA). (2024). *Essential Cybersecurity Controls (ECC-2:2024)*. Kingdom of Saudi Arabia. Available at: <https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/>
- Saudi Arabian Monetary Authority / Saudi Central Bank (SAMA). (n.d.). *SAMA Rulebook: Risk Management Framework*. Available at: <https://rulebook.sama.gov.sa/en/risk-management>
- Saudi Data and AI Authority (SDAIA). (2023). *Personal Data Protection Law (PDPL)—English Version, 23 April 2023*. Kingdom of Saudi Arabia. Available at: <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>
- Vision 2030. (2025). *Vision 2030 Annual Report 2025*. Council of Economic and Development Affairs, Kingdom of Saudi Arabia. Available at: <https://www.vision2030.gov.sa/en/annual-reports>
- Wolters Kluwer. (2025). *Risk Management Principles: Understanding ISO 31000 and COSO ERM*. Available at: <https://www.wolterskluwer.com/en/expert-insights/risk-management-principles-understanding-iso-31000-and-coso-erm>
- Zakat, Tax and Customs Authority (ZATCA). (n.d.). *E-Invoicing (Fatoorah) Regulations*. Kingdom of Saudi Arabia. Available at: <https://zatca.gov.sa/en/E-Invoicing/Pages/default.aspx>