Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i05.012

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Integrating Governance, Risk and Compliance (GRC) for Organizational Resilience in Saudi Arabia under Vision 2030

Essam Ali Hassan Abdelaal[1]*
[1]Independent Researcher

***Corresponding Author**
Essam Ali Hassan Abdelaal
Independent Researcher

Article History
Received: 17.07.2026
Accepted: 10.09.2026
Published: 14.09.2026

Abstract: Saudi Arabia's economic diversification and rapid digitalization have increased strategic risks linked to fragmented governance, risk management, and compliance. This integrative review examines how governance, risk, and compliance (GRC) can be structured as an organizational resilience capability within the Vision 2030 framework, rather than as separate control functions. The review synthesizes peer-reviewed research on enterprise risk management, corporate governance, compliance, digital transformation, cybersecurity, RegTech, and organizational resilience, focusing on evidence relevant to Saudi institutions and technology-intensive sectors. A transparent search and quality-assessment protocol prioritizes literature from 2020 to 2025, while retaining key foundational studies and a recent Saudi empirical anchor. The synthesis shows that resilience develops when governance defines decision rights and risk appetite, risk management translates uncertainty into prioritized action, compliance ensures reliable control behavior, and digital GRC enables timely, shared intelligence. These mechanisms strengthen anticipatory capacity, disruption absorption, adaptive coordination, recovery, and organizational renewal. However, integration may fail if GRC becomes overly centralized, metric-driven, technologically opaque, or disconnected from business ownership. Saudi evidence indicates that governance reform, ESG reporting, foreign investment, cyber governance, and digital transformation create mutually reinforcing pressures for integrated assurance. This paper presents a GRC-to-resilience framework and a four-stage maturity model for Saudi organizations. It concludes that resilience relies more on the integration of GRC into strategy, operations, data architecture, learning routines, and board oversight than on the mere existence of GRC functions. The review identifies research priorities including causal measurement, sector comparisons, AI-enabled GRC, regulatory interoperability, and resilience outcomes.

Keywords: Governance, Risk Management, Compliance, Organizational Resilience, Vision 2030, Saudi Arabia Digital GRC.

1. INTRODUCTION

Vision 2030 is reshaping Saudi organizations through diversification, privatization, digital public services, capital-market development, sustainability expectations, and intensified international investment. These changes create opportunities while enlarging the number and interdependence of strategic, operational, cyber, regulatory, reputational, and third-party risks. Early analyses of Vision 2030 emphasized the transition from an oil-dependent

economy to diversified, knowledge-intensive growth, alongside the institutional importance of sustainability and governance (Nurunnabi, 2017; Alshuwaikhat & Mohammed, 2017). More recent evidence shows that governance reforms can influence ESG disclosure and the attractiveness of Saudi firms to foreign investors, suggesting that control quality increasingly affects access to capital and stakeholder legitimacy (Chebbi & Ammer, 2022; Alregab, 2023; Umar *et al*., 2024).

Yet governance, risk, and compliance are still frequently organized as separate functions with different taxonomies, reporting cycles, technologies, and ownership models. Such separation can produce duplicated controls, inconsistent escalation, delayed risk information, and ambiguity over who accepts risk. GRC research therefore argues for coordinated information systems and integrated enterprise-level practices rather than parallel assurance silos (Papazafeiropoulou & Spanaki, 2016; Anton & Nucu, 2020). Enterprise risk management evidence similarly suggests that risk governance adds value when it is connected to board oversight and performance rather than implemented as a ceremonial process (Malik *et al*., 2020). Recent Saudi evidence from technology-driven firms further indicates that governance, risk management, and compliance contribute differently to efficiency and reputation. At the same time, integration and operational mechanisms matter for converting controls into organizational value (Aloulou & Alshohail, 2026).

Organizational resilience provides a more demanding outcome than compliance or short-term performance. Resilience concerns the capacity to anticipate adversity, absorb disruption, adapt during uncertainty, recover critical activities, and learn sufficiently to renew capabilities. Reviews of resilience research warn against reducing the construct to business continuity or post-crisis recovery alone (Duchek, 2020; Conz & Magnani, 2020; Hillmann & Guenther, 2021). This paper therefore asks how integrated GRC can create the decision discipline, sensing capacity, control reliability, and organizational learning needed for resilience in the Saudi transformation context. It extends performance-centered GRC research by connecting GRC mechanisms to resilience capabilities, digital governance, and Vision 2030 implementation.

2. Aim of the Study

This study aims to provide a critically synthesized explanation of how integrated GRC can enhance organizational resilience in Saudi Arabia under Vision 2030. Instead of assuming that additional controls automatically lead to resilience, it evaluates how governance, enterprise risk management, compliance, and digital assurance interact, identifies when integration may become counterproductive, and examines institutional factors affecting transferability to Saudi organizations.

2.1. Research Objectives

1. To synthesize contemporary evidence connecting governance, enterprise risk management, compliance, and organizational resilience, distinguishing integration mechanisms from the simple co-existence of functions.
2. To evaluate how board oversight, risk culture, control architecture, regulatory intelligence, and assurance coordination influence anticipatory, absorptive, adaptive, and recovery capacities.
3. To assess how digital transformation, cybersecurity, RegTech, data integration, and AI governance alter the design and effectiveness of integrated GRC.
4. To contextualize GRC-resilience relationships within Saudi governance reform, ESG expectations, digitalization, investment ambitions, and sector-specific institutional pressures associated with Vision 2030.
5. To develop a conceptual framework and research agenda that can guide empirical testing, managerial implementation, and policy development without overstating the present evidence base.

2.2. Research Questions

RQ1. Through which mechanisms can integrated GRC generate organizational resilience capabilities rather than merely regulatory conformance?
RQ2. How do governance, risk management, and compliance complement or constrain one another when uncertainty becomes operationally disruptive?
RQ3. How are digital transformation, cybersecurity, RegTech, and AI governance changing GRC's resilience contribution?
RQ4. Which Saudi institutional conditions under Vision 2030 are likely to strengthen, weaken, or reshape these relationships?

3. REVIEW METHODOLOGY

3.1. Review Design and Scope

An integrative review design was chosen because the research question spans several mature but only partially connected literatures, including GRC information systems, enterprise risk management, corporate governance, compliance, organizational resilience, digital transformation, cybersecurity governance, RegTech, and Saudi institutional reform. A narrowly focused systematic

review could exclude relevant mechanisms due to differing disciplinary terminology. The integrative approach allows for conceptual comparison across empirical studies, systematic reviews, and theory-building articles, while maintaining explicit decision rules. The synthesis focuses on mechanisms explaining how GRC practices may influence resilience capacity, rather than estimating pooled effects.

3.2. Databases and Search Strategy

Bibliographic searches focused on Scopus and Web of Science Core Collection, with additional retrieval from ScienceDirect, Emerald Insight, SpringerLink, Wiley Online Library, and Taylor & Francis Online for publisher-level access and citation tracing. Search terms included variants of: "governance risk compliance" OR GRC OR "enterprise risk management" OR "risk governance" OR "regulatory compliance"; AND resilien* OR "business continuity" OR adaptability OR agility; AND, where relevant, "Saudi Arabia" OR "Vision 2030" OR digital transformation OR cybersecurity OR RegTech OR "AI governance". The main publication window was 2020-2025. Earlier studies were included only if they provided foundational concepts in GRC, ERM, resilience, or Vision 2030 not addressed by recent work. The 2026 Saudi study served as a contextual anchor, not as a methodological template.

Table 1: Integrative review protocol and decision rules

Protocol component	Specification	Analytical rationale
Review design	Integrative, mechanism-oriented review across GRC, ERM, resilience, digital transformation, cybersecurity, and Saudi governance.	Accommodates fragmented terminology while preserving explicit evidence-selection rules.
Primary period	2020-2025, with selected earlier foundational studies and one 2026 Saudi empirical anchor.	Prioritizes contemporary evidence without discarding concepts that remain foundational.
Discovery sources	Scopus; Web of Science Core Collection; ScienceDirect; Emerald Insight; SpringerLink; Wiley Online Library; Taylor & Francis Online.	Combines multidisciplinary bibliographic coverage with publisher-level retrieval.
Search concepts	GRC / governance-risk-compliance / ERM / risk governance / regulatory compliance + resilience / continuity / adaptability + Saudi Arabia / Vision 2030 / digital transformation / cybersecurity / RegTech / AI governance.	Captures both direct GRC-resilience studies and adjacent mechanism evidence.
Inclusion criteria	Peer-reviewed English-language journal articles with explicit relevance to GRC mechanisms, resilience capabilities, or Saudi institutional conditions.	Retains analytically comparable and verifiable scholarship.
Exclusion criteria	Practitioner commentary, dissertations, promotional material, non-peer-reviewed reports, duplicates, and narrowly technical studies lacking organizational governance relevance.	Reduces unsupported or non-transferable evidence.
Quality assessment	Topical relevance; methodological transparency; construct clarity; outlet credibility; contextual transferability; explanatory contribution.	Prevents simple citation accumulation from substituting for critical appraisal.
Synthesis approach	Thematic coding and mechanism mapping; conflicting and conditional findings retained.	Supports conceptual integration without inappropriate effect-size pooling.
Verification	Bibliographic details and DOI strings checked against publisher pages or Crossref-linked records.	Strengthens reference integrity and reproducibility.

3.3. Inclusion, Exclusion, and Screening

Eligible sources were peer-reviewed journal articles in English that addressed at least one link between GRC architecture, resilience mechanisms, or Saudi institutional conditions. Priority was given to studies with explicit constructs, transparent methods, publication in recognized journals, and findings suitable for cross-setting comparison. Excluded sources included practitioner commentary, dissertations, promotional GRC material, non-peer-reviewed reports, duplicates, or papers referencing "governance" without an organizational control or accountability focus. Studies focused solely on technical cyber controls were excluded unless they addressed governance, organizational response, or policy integration. Screening was iterative, starting with title and abstract relevance, followed by full-text review, reference checking, and alignment with the emerging thematic map. No unsupported numerical search or exclusion counts are reported.

3.4. Quality Assessment, Synthesis, and Verification

Quality assessment addressed six dimensions: topical relevance, methodological transparency, construct clarity, journal credibility, contextual transferability, and explanatory contribution. Empirical findings were interpreted according to study design, so cross-sectional associations were not treated as causal evidence. The synthesis used thematic coding and mechanism mapping across governance and risk culture, ERM and compliance integration, digital GRC, Saudi institutional context, and resilience outcomes. Contradictory findings were retained to avoid one-sided conclusions. Bibliographic details and DOIs were checked against publisher or Crossref records. Heterogeneous constructs and designs justified theory-oriented synthesis; exhaustive coverage of studies is not claimed.

4. Thematic Literature Review and Critical Analysis

4.1. GRC Integration as a Resilience Capability

The central distinction in the literature is between possessing governance, risk, and compliance functions and integrating them into a coherent decision system. Early GRC information-systems research showed that integration depends on shared information, process alignment, and expert interpretation rather than on a software label alone (Papazafeiropoulou & Spanaki, 2016). ERM scholarship makes a parallel argument: formal frameworks can become symbolic unless risk information reaches strategic decisions and senior oversight (Bromiley *et al*., 2015; Anton & Nucu, 2020). Malik *et al*., (2020) demonstrate that ERM effectiveness is strengthened by risk governance arrangements such as board-level risk committees, reinforcing the importance of decision architecture.

Resilience research clarifies why this integration matters. Duchek (2020) conceptualizes resilience through anticipation, coping, and adaptation, while Conz and Magnani (2020) emphasize its dynamic and temporal nature. Hillmann and Guenther (2021) similarly caution that resilience is multidimensional and difficult to measure consistently. These perspectives imply that GRC supports resilience only when it generates usable capabilities across time: foresight before disruption, coordinated authority during disruption, control flexibility during adaptation, and learning after recovery. A compliance checklist may improve rule adherence without improving any of these capabilities.

The recent Saudi evidence is instructive because it shows differentiated pathways among GRC dimensions rather than a single undifferentiated effect. Governance and compliance exhibited clearer links to reputation through operational efficiency than risk management, suggesting that internal GRC components may create value through different mechanisms (Aloulou & Alshohail, 2026). The resilience implication is that integration should preserve functional specialization while connecting information, escalation, and accountability. Over-integration can be as problematic as fragmentation if centralized controls suppress local sensing or delay emergency decisions. Figure 1 therefore represents GRC as a coordinated capability system, not a merged department.

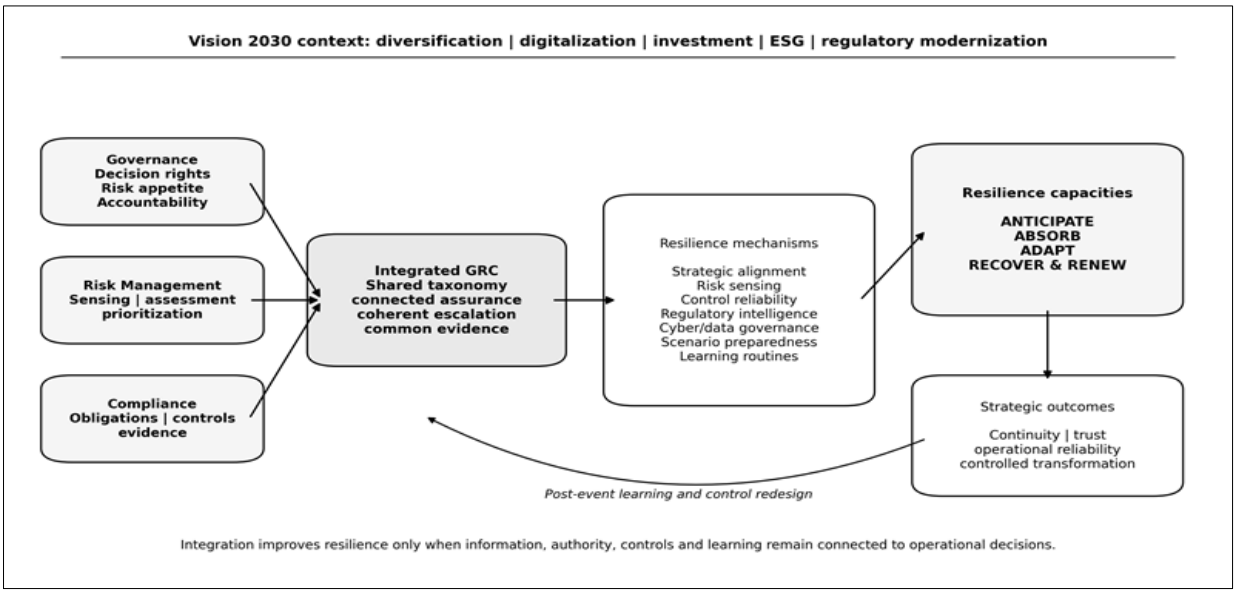

Figure 1: Integrated GRC-to-resilience framework for the Vision 2030 context. Source: developed for this review from the synthesized literature

4.2. Governance Architecture, Risk Culture, and Accountable Decision-Making

Governance contributes to resilience by determining who may decide, which risks are acceptable, how exceptions are escalated, and whether boards receive decision-relevant information. Risk governance becomes especially consequential when organizations confront ambiguity rather than quantifiable routine risks. Bianchi *et al*., (2021) find that sound risk culture is associated with stronger bank outcomes, indicating that formal policies require reinforcing behavioral norms. Derouiche *et al*., (2021) likewise link risk disclosure to operational efficiency, supporting the view that transparency can improve internal discipline rather than serve only external communication.

The governance-resilience relationship is nevertheless conditional. More oversight can reduce opportunism and clarify accountability, but excessive approval layers may impair speed. Resilience therefore requires "bounded autonomy": strategic risk appetite and non-negotiable controls are set centrally, while operational teams retain predefined authority to respond within tolerances. This logic is consistent with evidence that governance quality and reporting shape reputation and stakeholder assessments (Ghuslan *et al*., 2021; Eriqat *et al*., 2023). Reputation matters for resilience because stakeholder trust affects the organization's access to cooperation, capital, and legitimacy during disruption, although reputational outcomes should not be treated as resilience itself.

Saudi studies make this mechanism contextually salient. Governance reforms have been associated with ESG disclosure patterns, and board characteristics can influence reporting practices (Chebbi & Ammer, 2022; Bamahros *et al*., 2022). Ebaid (2022) also shows that governance mechanisms influence corporate social responsibility disclosure in an emerging-market setting, while Umar *et al*., (2024) provide updated Saudi evidence on governance mechanisms and ESG disclosure. The critical implication is that board structure alone is insufficient. Under Vision 2030, governance must connect disclosure, risk appetite, strategic investment, cyber accountability, and crisis authority; otherwise, organizations may become transparent about risks without becoming better able to manage them.

4.3. Enterprise Risk Management, Compliance, and Continuity

ERM supplies the portfolio logic needed to compare uncertainties across strategic and operational domains. The literature review by Anton and Nucu (2020) shows that ERM research increasingly connects risk management with performance and governance, but also reveals persistent variation in definitions and measures. Bromiley *et al.*, (2015) earlier warned that ERM research needs stronger theory and more careful treatment of implementation. These concerns are directly relevant to resilience: a risk register is not a resilience capability unless it changes resource allocation, preparedness, stress testing, or response design.

Compliance adds a different form of value. It translates external obligations and internal policy into repeatable controls, evidence, monitoring, and corrective action. When compliance is detached from risk, organizations can spend heavily on low-consequence requirements while underinvesting in high-impact vulnerabilities. When risk is detached from compliance, organizations may normalize significant legal or conduct exposures as operational trade-offs. Integrated GRC therefore requires a common taxonomy linking obligations, risks, controls, assets, owners, incidents, and assurance results. RegTech research shows how data and technology can reduce compliance friction and improve monitoring, while also introducing cyber, algorithmic, and data-governance risks that themselves require oversight (Grassi & Lanfranchi, 2022).

From a resilience perspective, the most important interface is continuity. Controls should be designed not only for normal operations but for degraded states: supplier failure, cyber incidents, regulatory change, workforce disruption, or technology outages. The best control may change during a crisis, but the principles governing temporary exceptions must be predetermined. Malik *et al*., (2020) and Bianchi *et al.,* (2021) imply that board-level risk governance and culture shape whether such judgments are disciplined. Thus, resilient compliance is neither rigid adherence nor improvisation; it is controlled adaptability, supported by documented tolerances, delegated authority, alternative controls, and post-event review.

Table 2: Critical synthesis of GRC-resilience mechanisms and Vision 2030 implications

Theme	Evidence pattern	Critical tension	Vision 2030 implication	Indicative sources
GRC integration	Shared information, risk ownership, control mapping, coordinated assurance.	Integration vs. functional independence.	Use common architecture without collapsing challenge roles.	Papazafeiropoulou & Spanaki (2016); Malik *et al*., (2020); Aloulou & Alshohail (2026)
Governance and risk culture	Decision rights, transparency, risk appetite, board oversight, escalation norms.	Control reliability vs. decision speed.	Design bounded autonomy for rapid transformation.	Bianchi *et al*., (2021); Ghuslan *et al.,* (2021); Eriqat *et al*., (2023)
ERM and compliance	Portfolio prioritization, obligations-to-controls traceability, disciplined exceptions.	Checklist compliance vs. risk significance.	Link obligations to critical services and continuity tolerances.	Anton & Nucu (2020); Derouiche *et al*., (2021); Grassi & Lanfranchi (2022)
Digital GRC, cyber, and AI	Continuous monitoring, integrated telemetry, automation, regulatory intelligence.	Automation efficiency vs. accountability and opacity.	Integrate cyber, data, third-party, and AI governance with enterprise GRC.	Hanelt *et al*., (2021); Rawindaran *et al*., (2023); Camilleri (2024); Bernardelli & Giudici (2025)
Saudi institutional context	Governance reform, ESG disclosure, investment credibility, digital public services.	Disclosure quality vs. operational resilience.	Use GRC to support credible controlled acceleration under Vision 2030.	Chebbi & Ammer (2022); Bamahros *et al*., (2022); Alregab (2023); Umar *et al*., (2024)
Resilience outcomes	Anticipation, absorption, adaptation, recovery, learning and renewal.	Proxy indicators vs. event-based capability measures.	Measure detection latency, recovery, adaptation, and control learning.	Duchek (2020); Hillmann & Guenther (2021); Zhang *et al*., (2021); He *et al*., (2023)

4.4. Digital GRC, Cybersecurity, RegTech, and AI Governance

Digital transformation changes both the risk landscape and the GRC operating model. Hanelt *et al*., (2021), Verhoef *et al*., (2021), and Kraus *et al*., (2022) show that digital transformation is organizational and strategic, not merely technological. As processes become platform-based, data-intensive, automated, and ecosystem-dependent, GRC must monitor risks that cross organizational boundaries and evolve faster than annual control cycles. This creates a need for continuous control monitoring, machine-readable obligations, integrated data lineage, cyber-risk telemetry, and faster exception management.

Digital capability can also strengthen resilience. Zhang *et al*., (2021) link digital transformation to organizational resilience, while He *et al*., (2023) describe how digital transformation can help build resilience through organizational mechanisms. Forliano *et al*., (2023) add that strategy's digital maturity mediates the relationship between technological orientation and resilience. Together, these findings suggest that technology creates resilience only when governance and strategy determine how information is interpreted and acted upon. Automated dashboards that accelerate weak decisions merely digitize fragility.

Cybersecurity illustrates the integration problem sharply. Saudi-focused research emphasizes that cybersecurity governance, policy, and organizational arrangements matter alongside technical protection (Rawindaran *et al*., 2023). Al-Hawamleh (2024) similarly connects cybersecurity practices with the quality of Saudi e-government services, highlighting the operational consequences of security governance. Cyber incidents can simultaneously trigger service disruption, privacy obligations, executive accountability, reputational exposure, and third-party risk; siloed GRC therefore fragments a single event into multiple reporting chains.

AI intensifies these challenges. Camilleri (2024) argues that AI governance requires ethical and social-responsibility considerations, while Bernardelli and Giudici (2025) show the rapid development of AI risk-management research. AI-enabled GRC may improve anomaly detection, policy mapping, control testing, and scenario analysis, but opaque models can create explainability, bias, privacy, and accountability risks. The appropriate direction is governed augmentation: automation expands sensing and analytical capacity, while human owners retain explicit responsibility for risk

acceptance, material judgments, and contested exceptions.

4.5. Saudi Vision 2030 as an Institutional Setting for GRC Resilience

Saudi Arabia is not simply another geographic setting for GRC. Vision 2030 combines economic diversification, state-enabled transformation, capital-market development, digital government, private-sector growth, localization, and sustainability ambitions. Foundational analyses describe this transition as a move toward a knowledge-based and more diversified economy in which institutional quality and sustainability matter to national development (Nurunnabi, 2017; Alshuwaikhat & Mohammed, 2017). Such transformation raises the premium on organizations that can change rapidly without losing control.

Corporate-governance evidence reinforces this point. Alregab (2023) links governance to foreign-investment attraction among Saudi-listed firms, while Saudi ESG studies show that governance reforms and board mechanisms affect non-financial disclosure (Chebbi & Ammer, 2022; Bamahros *et al*., 2022; Umar *et al*., 2024). These findings do not prove organizational resilience, but they demonstrate that governance quality influences the external trust environment in which resilience is exercised. Organizations seeking international capital, partnerships, or public mandates must show that strategic transformation is governed credibly.

The digital dimension is equally important. Saudi cyber-governance studies indicate that policy, organizational practice, and service quality are intertwined (Rawindaran *et al*., 2023; Al-Hawamleh, 2024). Meanwhile, recent Saudi GRC evidence suggests that operational efficiency is one pathway through which governance and compliance contribute to reputation (Aloulou & Alshohail, 2026). Taken together, the literature supports a Vision 2030-specific proposition: integrated GRC becomes most valuable when it enables controlled acceleration. Its purpose is not to slow transformation until uncertainty disappears, but to make risk ownership, evidence, escalation, and recovery sufficiently reliable that organizations can pursue ambitious change without accumulating hidden fragility.

5. DISCUSSION

The review identifies organizational resilience as an emergent property of GRC integration rather than a direct product of any single governance mechanism. Governance creates strategic coherence by defining risk appetite, accountability, and escalation. ERM creates portfolio awareness by translating uncertainty into comparable priorities. Compliance creates control discipline and evidence. Digital GRC shortens the interval between signal, interpretation, and response. These elements become resilience capabilities when they are connected to operations and learning. This interpretation bridges ERM research, which emphasizes governance and implementation quality (Anton & Nucu, 2020; Malik *et al*., 2020), with resilience theory, which emphasizes anticipation, coping, adaptation, and renewal (Duchek, 2020; Hillmann & Guenther, 2021).

The synthesis also exposes three tensions. First is the control-agility tension. Formalization can improve reliability but may increase decision latency. Resilient GRC therefore differentiates between non-negotiable boundaries and delegated response authority. Second is the integration-independence tension. Combining risk and compliance data reduces duplication, yet assurance functions still require sufficient independence to challenge management. Integration should mean common architecture and coordinated evidence, not elimination of professional judgment or the "three lines" logic of differentiated responsibility. Third is the automation-accountability tension. RegTech and AI can improve monitoring, but automated classification and recommendations may obscure assumptions or redistribute responsibility without explicit governance (Grassi & Lanfranchi, 2022; Camilleri, 2024).

The Saudi context makes these tensions strategically significant. Vision 2030 requires organizations to innovate, scale, localize capabilities, attract investment, and digitize services while meeting rising expectations for governance and transparency. Saudi governance and ESG research suggests that formal reforms alter reporting and stakeholder-facing practices (Chebbi & Ammer, 2022; Bamahros *et al*., 2022; Alregab, 2023). However, disclosure and board structure are not substitutes for operational resilience. The critical research and management question is whether governance reforms penetrate daily decision processes: project gates, technology architecture, vendor selection, model approval, crisis escalation, and post-incident learning.

Figure 2 converts this argument into a maturity path. The model deliberately avoids equating maturity with more controls. Movement from fragmented compliance to adaptive resilience requires better integration of data and assurance, faster learning, clearer risk ownership, and calibrated autonomy. A digitally sophisticated organization can remain immature if its analytics are disconnected from decisions; conversely, a less automated organization can be resilient if its accountabilities, scenarios, and recovery routines are coherent.

Digitalization is therefore an accelerator of GRC maturity, not its definition.

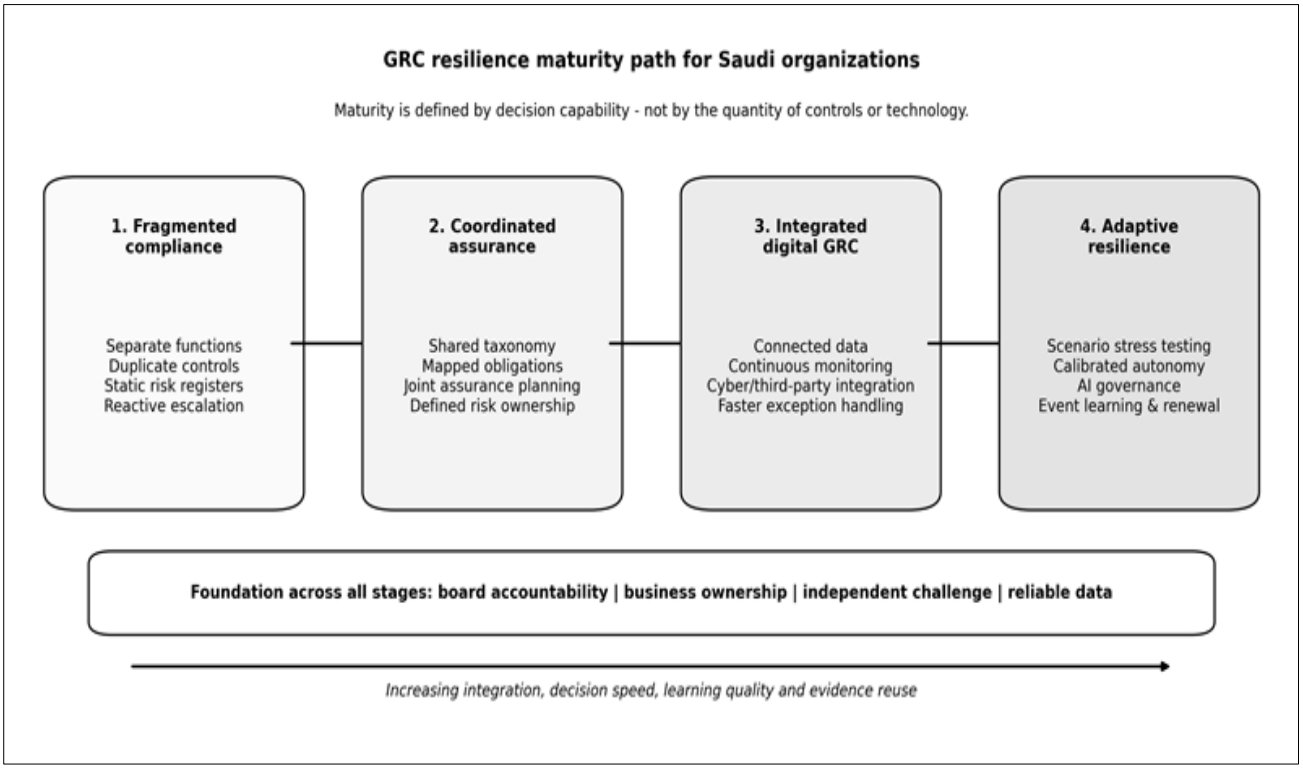

Figure 2: GRC resilience maturity path for Saudi organizations. Source: developed for this review from the synthesized literature

A further implication concerns measurement. Much existing evidence uses performance, disclosure, reputation, or self-reported GRC maturity as outcomes. These are useful but incomplete proxies. Resilience should be tested through observable capabilities and event-based outcomes: time to detect material change, decision latency, duration of critical-service interruption, recovery-time variance, control effectiveness under degraded conditions, speed of regulatory adaptation, concentration of third-party dependencies, and evidence that post-event learning changes controls. Without such measures, organizations may report improving GRC scores while remaining brittle under stress.

A final interpretive point concerns organizational ownership. Integrated GRC is sometimes designed as a specialist platform administered by risk or compliance teams, yet resilience requires information to travel both vertically and horizontally. Front-line teams must recognize emerging signals, control owners must understand the business consequences of failure, and executives must distinguish transient exceptions from shifts in the risk profile. This distributed ownership is consistent with the resilience literature's emphasis on adaptive capacity and learning (Conz & Magnani, 2020). It also explains why risk culture matters: employees need incentives to escalate weak signals before they become reportable incidents (Bianchi *et al.*, 2021). In Saudi organizations undergoing rapid growth, acquisition, localization, or digital redesign, integration should therefore be tested through decision exercises rather than system demonstrations. Scenario simulations can reveal whether data are trusted, authorities are understood, alternative controls are available, and lessons reach investment and design decisions. Such exercises convert GRC from a documentation architecture into a practiced organizational capability.

6. Research Gaps and Future Research

The first gap is causal. Cross-sectional governance and GRC studies can identify associations but cannot establish whether integration causes resilience or whether capable organizations simply invest more in GRC. Longitudinal designs should examine GRC changes before and after regulatory shifts, cyber events, mergers, major projects, or digital transformations. Event studies and matched organizational comparisons could test whether integrated risk intelligence shortens disruption duration or improves recovery quality. Saudi sectors

undergoing rapid transformation provide unusually relevant settings for this work.

Second, the field lacks validated GRC-resilience measures. Resilience reviews already identify conceptual and measurement inconsistencies (Hillmann & Guenther, 2021). Future research should distinguish preparedness, absorption, adaptation, recovery, and renewal, then test which GRC capabilities predict each dimension. This would clarify why risk management may enhance internal efficiency without producing the same reputational pathway as governance or compliance, as suggested by Aloulou and Alshohail (2026).

Third, sectoral contingency is underdeveloped. Banking, energy, healthcare, telecommunications, logistics, public services, and giga-project ecosystems face different risk velocities, regulatory intensity, safety consequences, and dependency structures. Comparative Saudi research should test whether a common GRC architecture requires sector-specific operating models. Particular attention should be paid to supply-chain and third-party concentration because Vision 2030's localization and ecosystem-building agendas create both resilience opportunities and transition dependencies.

Fourth, digital GRC needs governance research rather than technology optimism. Studies of digital transformation and resilience indicate that organizational mechanisms and digital maturity matter (Zhang *et al*., 2021; He *et al*., 2023; Forliano *et al*., 2023). Future studies should evaluate continuous control monitoring, knowledge graphs, machine-readable regulation, AI-assisted risk sensing, and automated evidence collection against false positives, model drift, privacy, cyber exposure, and automation bias. AI risk-management research should also test accountability when machine-generated GRC recommendations influence material decisions (Bernardelli & Giudici, 2025).

Finally, regulatory interoperability deserves attention. Saudi organizations increasingly operate across overlapping financial, cyber, data, ESG, sector, and international requirements. Research should examine whether common control frameworks and shared evidence repositories reduce compliance burden while improving resilience, or whether they create systemic dependence on centralized taxonomies and technology platforms. The next generation of GRC research should therefore study architectural choices, not merely adoption levels.

7. Practical, Managerial, and Policy Implications

For boards, the priority is to govern GRC as a decision system. Risk appetite should be translated into operational thresholds, exception authorities, and escalation triggers that remain usable during disruption. Board reporting should focus on changes in exposure, control deterioration, dependency concentration, unresolved exceptions, and recovery readiness rather than large inventories of static risks. Risk committees can add value when they connect ERM to performance and strategic oversight, consistent with Malik *et al*., (2020), but accountability must remain with business owners rather than being transferred to the risk function.

For executives, integration should begin with architecture before technology. Organizations need a common taxonomy connecting objectives, obligations, risks, controls, assets, processes, third parties, incidents, and assurance findings. Compliance testing, internal audit evidence, cyber telemetry, and operational indicators should be reusable where appropriate, reducing duplicate requests while preserving independent challenge. Digital tools should then automate traceability and monitoring. RegTech evidence supports efficiency gains from technology-enabled compliance, but the associated data and algorithmic risks require governance from the outset (Grassi & Lanfranchi, 2022).

For Saudi transformation programs, GRC should be embedded into investment gates, digital-product design, procurement, localization decisions, and major-project governance. This is particularly important where rapid scaling can create hidden dependencies or control debt. The objective is controlled acceleration: predictable boundaries combined with faster risk-informed decisions. Cybersecurity and AI governance should be integrated with enterprise GRC because digital incidents can create simultaneous operational, legal, reputational, and strategic consequences (Rawindaran *et al*., 2023; Camilleri, 2024).

For policymakers and regulators, interoperability is preferable to proliferating disconnected compliance regimes. Common definitions, machine-readable requirements, proportional assurance expectations, and reusable evidence models can reduce administrative burden while improving supervisory visibility. Policy should also encourage resilience testing, scenario exercises, and post-incident learning rather than treating documented compliance as sufficient proof of preparedness. Saudi governance research indicates that reforms can influence corporate behavior and disclosure (Ebaid, 2022; Umar *et al*., 2024); the next

step is to align those incentives with demonstrable adaptive capacity.

8. Limitations

This review is intentionally integrative and concept-driven. It does not estimate pooled effects, and the heterogeneity of GRC definitions, resilience measures, sectors, and national settings limits direct comparison. The evidence base is also stronger for governance, ERM, disclosure, digital transformation, and performance than for studies directly testing integrated GRC against event-based resilience outcomes. Saudi-specific peer-reviewed evidence remains uneven across sectors, so some mechanisms are transferred cautiously from international research. Finally, restricting the reference corpus for recency and conceptual focus may omit useful specialist studies. These limitations support the proposed empirical agenda rather than invalidating the synthesis.

9. CONCLUSION

Integrated GRC can contribute to organizational resilience in Saudi Arabia when it moves beyond administrative control and becomes part of how strategy, operations, technology, and learning are governed. The review shows that governance supplies decision rights and risk appetite; ERM creates prioritized awareness of uncertainty; compliance embeds disciplined, evidence-based control; and digital GRC accelerates sensing, traceability, and coordination. Their resilience value emerges through integration, not mere presence. The strongest configuration combines common data and assurance architecture with differentiated professional roles, delegated authority, and explicit board accountability.

Under Vision 2030, this capability is strategically important because organizations are expected to transform quickly while remaining trustworthy, investable, secure, and operationally reliable. Saudi evidence on governance reform, ESG disclosure, foreign investment, cybersecurity, and GRC performance points in the same direction: formal structures matter, but their value depends on how deeply they shape operational behavior. The proposed framework therefore treats resilience as controlled adaptability rather than resistance to change.

Future progress requires better measurement and stronger causal designs. Researchers should test whether integrated GRC reduces detection and decision latency, improves recovery performance, accelerates regulatory adaptation, and converts incident learning into changed controls. Managers and policymakers should likewise judge GRC by its ability to sustain critical objectives under uncertainty, not by the volume of policies, dashboards, or audit evidence produced. In that sense, resilient GRC is best understood as an organizational capability for governing transformation itself.

REFERENCES

- Al-Hawamleh, A.M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. Digital Policy, Regulation and Governance, 26(3), 317-336. https://doi.org/10.1108/DPRG-11-2023-0168
- Aloulou, W.J. and Alshohail, N.F. (2026). From Control to Value: How Governance, Risk Management and Compliance Improve Operational Efficiency and Company Reputation in Saudi Technology-Driven Firms. Risks, 14(1), 19. https://doi.org/10.3390/risks14010019
- Alregab, H. (2023). The role of corporate governance in attracting foreign investment: An empirical investigation of Saudi-listed firms in light of Vision 2030. International Journal of Finance & Economics, 28(1), 284-294. https://doi.org/10.1002/ijfe.2420
- Alshuwaikhat, H.M. and Mohammed, I. (2017). Sustainability Matters in National Development Visions-Evidence from Saudi Arabia's Vision for 2030. Sustainability, 9(3), 408. https://doi.org/10.3390/su9030408
- Anton, S.G. and Afloarei Nucu, A.E. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. Journal of Risk and Financial Management, 13(11), 281. https://doi.org/10.3390/jrfm13110281
- Bamahros, H.M., Alquhaif, A., Qasem, A., Wan-Hussin, W.N., Thomran, M., Al-Duais, S.D., Shukeri, S.N. and Khojally, H.M.A. (2022). Corporate Governance Mechanisms and ESG Reporting: Evidence from the Saudi Stock Market. Sustainability, 14(10), 6202. https://doi.org/10.3390/su14106202
- Bernardelli, A.E. and Giudici, P. (2025). AI Risk Management: A Bibliometric Analysis. Risks, 13(7), 131. https://doi.org/10.3390/risks13070131
- Bianchi, N., Carretta, A., Farina, V. and Fiordelisi, F. (2021). Does espoused risk culture pay? Evidence from European banks. Journal of Banking & Finance, 122, 105767. https://doi.org/10.1016/j.jbankfin.2020.105767
- Bromiley, P., McShane, M., Nair, A. and Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. Long Range Planning, 48(4), 265-276. https://doi.org/10.1016/j.lrp.2014.07.005
- Camilleri, M.A. (2024). Artificial intelligence governance: Ethical considerations and implications for social responsibility. Expert Systems, 41(7), e13406. https://doi.org/10.1111/exsy.13406

- Chebbi, K. and Ammer, M.A. (2022). Board Composition and ESG Disclosure in Saudi Arabia: The Moderating Role of Corporate Governance Reforms. Sustainability, 14(19), 12173. https://doi.org/10.3390/su141912173
- Conz, E. and Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. European Management Journal, 38(3), 400-412. https://doi.org/10.1016/j.emj.2019.12.004
- Derouiche, I., Manita, R. and Muessig, A. (2021). Risk disclosure and firm operational efficiency. Annals of Operations Research, 297, 115-145. https://doi.org/10.1007/s10479-020-03520-z
- Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. Business Research, 13(1), 215-246. https://doi.org/10.1007/s40685-019-0085-7
- Ebaid, I.E.-S. (2022). Corporate governance mechanisms and corporate social responsibility disclosure: evidence from an emerging market. Journal of Global Responsibility, 13(4), 396-420. https://doi.org/10.1108/JGR-12-2021-0105
- Eriqat, I.O.A., Tahir, M. and Zulkafli, A.H. (2023). Do Corporate Governance Mechanisms Matter to the Reputation of Financial Firms? Evidence of Emerging Markets. Cogent Business & Management, 10(1), 2181187. https://doi.org/10.1080/23311975.2023.2181187
- Forliano, C., Bullini Orlandi, L., Zardini, A. and Rossignoli, C. (2023). Technological orientation and organizational resilience to Covid-19: The mediating role of strategy's digital maturity. Technological Forecasting and Social Change, 188, 122288. https://doi.org/10.1016/j.techfore.2022.122288
- Ghuslan, M.I., Jaffar, R., Saleh, N.M. and Yaacob, M.H. (2021). Corporate Governance and Corporate Reputation: The Role of Environmental and Social Reporting Quality. Sustainability, 13(18), 10452. https://doi.org/10.3390/su131810452
- Grassi, L. and Lanfranchi, D. (2022). RegTech in public and private sectors: the nexus between data, technology and regulation. Journal of Industrial and Business Economics, 49(3), 441-479. https://doi.org/10.1007/s40812-022-00226-0
- Hanelt, A., Bohnsack, R., Marz, D. and Antunes Marante, C. (2021). A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. Journal of Management Studies, 58(5), 1159-1197. https://doi.org/10.1111/joms.12639
- He, Z., Huang, H., Choi, H. and Bilgihan, A. (2023). Building organizational resilience with digital transformation. Journal of Service Management, 34(1), 147-171. https://doi.org/10.1108/JOSM-06-2021-0216
- Hillmann, J. and Guenther, E. (2021). Organizational Resilience: A Valuable Construct for Management Research? International Journal of Management Reviews, 23(1), 7-44. https://doi.org/10.1111/ijmr.12239
- Kraus, S., Durst, S., Ferreira, J.J., Veiga, P., Kailer, N. and Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. International Journal of Information Management, 63, 102466. https://doi.org/10.1016/j.ijinfomgt.2021.102466
- Malik, M.F., Zaman, M. and Buckby, S. (2020). Enterprise risk management and firm performance: Role of the risk committee. Journal of Contemporary Accounting & Economics, 16(1), 100178. https://doi.org/10.1016/j.jcae.2019.100178
- Nurunnabi, M. (2017). Transformation from an Oil-based Economy to a Knowledge-based Economy in Saudi Arabia: the Direction of Saudi Vision 2030. Journal of the Knowledge Economy, 8(2), 536-564. https://doi.org/10.1007/s13132-017-0479-8
- Papazafeiropoulou, A. and Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts' view. Information Systems Frontiers, 18(6), 1251-1263. https://doi.org/10.1007/s10796-015-9572-3
- Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I. and Hewage, C. (2023). Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. Digital, 3(3), 200-231. https://doi.org/10.3390/digital3030014
- Umar, U.H., Firmansyah, E.A., Danlami, M.R. and Al-Faryan, M.A.S. (2024). Revisiting the relationship between corporate governance mechanisms and ESG disclosures in Saudi Arabia. Journal of Accounting & Organizational Change, 20(4), 724-747. https://doi.org/10.1108/JAOC-01-2023-0011
- Verhoef, P.C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J.Q., Fabian, N. and Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889-901. https://doi.org/10.1016/j.jbusres.2019.09.022
- Zhang, J., Long, J. and von Schaewen, A.M.E. (2021). How Does Digital Transformation Improve Organizational Resilience?-Findings from PLS-SEM and fsQCA. Sustainability, 13(20), 11487. https://doi.org/10.3390/su132011487.