ISSN 2055-0286
Advances in Social Sciences Research Journal; Vol. 13 No. 04 (2026) (84-92)
https://doi.org/10.14738/assrj.1304.20198

The Added Value of Applying Governance, Risk, and Compliance (GRC) in the Healthcare Sector: A Literature Review

Amjad Aldahmashi & Akram Abdulsamad

1. Faculty of Business and Accountancy, Lincoln University College, Malaysia
2. Faculty of Business and Accountancy, Lincoln University College, Malaysia and Faculty of Economics and Political Science, University of Aden, Yemen

Abstract: The healthcare sector faces unique pressures complex regulatory demands, patient safety obligations, escalating cybersecurity threats, and investor expectations making it one of the industries where Governance, Risk, and Compliance (GRC) frameworks offer the greatest potential value. This literature review synthesizes evidence from 25 peer-reviewed studies, systematic reviews, bibliometric analyses, and industry reports published between 2010 and 2026 to answer the question: what added value does applying GRC bring to healthcare organizations? Six distinct value dimensions are identified and examined: (1) firm value and investor confidence, (2) patient safety and care quality, (3) proactive cyber risk management, (4) operational efficiency and cost reduction, (5) regulatory compliance and reputation protection, and (6) strategic resilience and enterprise risk management. Findings indicate that GRC positively affects firm value in healthcare companies, with an explanatory level of 33.8% [14], and that integrated GRC is associated with improved patient safety across multiple health systems [3]. The review also identifies significant barriers to implementation, including cultural resistance, resource constraints, and data privacy concerns, alongside emerging opportunities from artificial intelligence-enabled GRC tools. The evidence consistently demonstrates that GRC value in healthcare is multiplicative rather than additive: governance, risk management, and compliance generate greater combined benefit when integrated than when managed as separate functions.

Keywords: governance, risk, and compliance, GRC, healthcare, firm value, patient safety, enterprise risk management.

INTRODUCTION

The healthcare sector operates at the intersection of complex regulatory demands, high-stakes patient safety obligations, increasing cybersecurity threats, and investor expectations, making it one of the industries where integrated Governance, Risk, and Compliance (GRC) frameworks have the greatest potential impact. While GRC was initially conceived as a corporate governance and financial compliance tool in the early 2000s following the Sarbanes-Oxley Act [10], its scope has since expanded dramatically into healthcare, encompassing patient safety systems, data privacy regulations (HIPAA, GDPR), cybersecurity governance, and enterprise risk management.

This literature review synthesizes evidence from peer-reviewed academic papers, systematic reviews, bibliometric analyses, and industry research to answer the central question: what added value does the application of GRC bring to the healthcare sector? The

review is organized around six evidence-based dimensions of value, supported by more than 25 sources spanning 2010 to 2026.

THEORETICAL BACKGROUND: THE GRC FRAMEWORK

GRC is defined as an integrated framework combining governance, risk management, and compliance into a unified organizational approach. Handoko et al. [10] define each pillar as follows: Governance refers to the rules, processes, and structures by which business operations are run, regulated, and controlled, encompassing both internal policies and external regulatory expectations. Risk encompasses a company's strategy for protecting the value of existing assets and managing uncertainty strategically. Compliance refers to adherence to laws, regulations, and internal policies, including control mechanisms that ensure operations remain within legal and ethical boundaries.

Racz, Weippl and Seufert [20] provided one of the earliest comprehensive frameworks for integrated GRC research, noting that despite its widespread significance, integrated GRC lacked a common research platform and shared definitions. Vicente and Mira da Silva [24] later proposed a conceptual model integrating all three pillars around shared elements, validated using the OCEG capability model. A bibliometric analysis by Handoyo et al. [11] of 429 Scopus-indexed GRC documents confirmed that GRC scholarship has expanded significantly, with dominant themes in corporate governance, risk management, internal controls, and corporate social responsibility, alongside emerging themes in artificial intelligence, blockchain, and sustainability.

Within healthcare specifically, GRC has evolved from a compliance-driven function into a strategic enabler. As Alder [1] explains, a siloed linear approach to compliance results in inconsistencies and deterioration in patient care, whereas an integrated GRC framework enables bidirectional communication between governance, risk, and compliance activities, preventing silos and improving responsiveness.

ADDED VALUE DIMENSION 1: FIRM VALUE AND INVESTOR CONFIDENCE

GRC implementation has a positive and statistically significant effect on firm value in healthcare companies, with the effect becoming stronger during crisis conditions. Kembaren, Endro and Pendrian [14], in a quantitative study of 11 Indonesian healthcare companies listed on the Indonesia Stock Exchange (2018–2021), used Tobin's Q as a proxy for firm value and measured GRC using the Indonesian GRC Award scoring method. Their findings demonstrated that GRC positively affects firm value with an explanatory level of 33.8% in pooled data. Data segregation revealed that this explanatory level was significantly higher during the COVID-19 pandemic period (R^2 = 0.409) compared to the pre-pandemic period (R^2 = 0.348), indicating that the crisis amplified the signalling value of GRC to investors. The mechanism operates through stakeholder and signalling theory: positive and complete GRC information reassures investors about the security of their capital, spurring greater confidence and higher market valuations. The paired sample t-test confirmed significant differences in both GRC scores and firm value across pre-pandemic and pandemic periods, with healthcare firm value actually increasing during the pandemic, consistent with investor confidence in the sector's robust governance foundations [14].

This is corroborated by the systematic literature review of Karthick et al. [13], which synthesized 25 articles and confirmed that GRC exerts a positive and noteworthy impact on a firm's overall value, with its adoption leading to a sustainable strategy and directed focus on priority programs. The review also highlights that this value effect is especially evident in the healthcare industry, where governance pillars strong ethics, reliable risk management, and regulatory compliance directly influence investor behavior.

ADDED VALUE DIMENSION 2: PATIENT SAFETY AND CARE QUALITY

GRC integration is positively associated with improved patient safety outcomes, reduced medical errors, and enhanced quality of care delivery. Alqahtani, Belal and Zakri [3] conducted the most comprehensive healthcare-specific GRC systematic review to date (PROSPERO-registered, PRISMA 2020 compliant), screening 85 records and including 22 studies across the Netherlands, Australia, the UK, Italy, and the USA, spanning primary care institutions to national-level healthcare systems. The thematic synthesis found that GRC integration was positively associated with improved patient safety, care quality, regulatory compliance, organizational efficiency, and financial outcomes. Key success factors identified included leadership support, stakeholder engagement, tailored implementation, and technology adoption, while cultural resistance, limited resources, and data privacy concerns represented the main barriers [3].

McCormack [7] identifies patient safety as the primary mechanism through which GRC creates value: by implementing stringent safety protocols, identifying potential risks proactively, and establishing preventive measures, healthcare GRC reduces medical errors, prevents infections through proper hygiene governance, and minimizes adverse drug events through effective medication management protocols. The Swiss GRC-Association of Zurich Hospitals collaboration [23] further confirms that hospitals implementing structured GRC strategies can create frameworks enabling dynamic regulatory adaptation, robust data protection, and proactive risk-based management, all of which feed directly into patient safety outcomes.

ADDED VALUE DIMENSION 3: PROACTIVE CYBER RISK MANAGEMENT

GRC provides the structural foundation for proactive, integrated cybersecurity in healthcare, where breaches carry the highest costs of any industry sector. Compyl [8] reports that in 2023 alone there were nearly 750 separate data breach incidents in the United States, while the average cost of a healthcare data breach ($9.7 million per incident) is nearly double that of other industries. Censinet [6] recorded 444 cyber incidents targeting healthcare in 2024, including 206 data breaches, with third-party vendors and connected medical devices particularly vulnerable.

GRC provides the response: healthcare networks that adopt integrated GRC apply proactive risk management to reduce vulnerabilities, leverage technology to customize risk strategies, and use ongoing risk monitoring to mitigate the impact of cyberattacks [8]. This is achieved through structured compliance with standards including HIPAA, HITECH, HITRUST, and ISO 27001, and through IT GRC frameworks that integrate cybersecurity into broader governance structures. Alharbi et al. [2] demonstrated that cybersecurity governance must be embedded within broader GRC architecture rather than managed as a

standalone function, drawing on COBIT, ITIL, and CMI standards to create an integrated approach spanning application security, IoT security, network security, and infrastructure security.

McIntosh et al. [17] showed that GPT-4-assisted generation of cybersecurity GRC policies focused on ransomware mitigation represents an emerging application of artificial intelligence within healthcare GRC. Censinet [6] further demonstrated that AI-driven GRC platforms can achieve a 62% improvement in compliance efficiency for healthcare organizations. Mahendra, Prabowo and Hidayanto [15] identified interoperability, data governance, and system integration as the primary IT obstacles to effective GRC, challenges that are particularly acute in healthcare with its fragmented electronic health record systems.

ADDED VALUE DIMENSION 4: OPERATIONAL EFFICIENCY AND COST REDUCTION

Integrated GRC programs systematically reduce compliance costs, eliminate duplicative processes, and free clinical and administrative resources for higher-value activities. Handoko et al. [10] describe this as reducing the total cost of ownership: investments in GRC infrastructure generate returns across multiple regulatory requirements simultaneously rather than requiring separate compliance architectures for each regulation. Swiss GRC [23] identifies resource optimization as a particular benefit for hospitals, noting that a well-structured GRC framework helps optimize processes and reduce the administrative burden, enabling staff and financial resources to be deployed more effectively toward patient care.

Industry research demonstrates compelling financial returns. Censinet and Forrester [6] found that businesses with integrated GRC programs cut their controls by 47% within three years and reduced testing time per control by 60%, saving millions in compliance costs, with overall ROI exceeding 300% over three years. AI-driven regulatory technology was projected to save organizations approximately $1.2 billion in compliance-related expenses by 2023, with 62% of organizations reporting significant improvements in compliance efficiency from AI solutions [6].

Batenburg, Neppelenbroek and Shahim [4], in their maturity model for GRC in Dutch hospitals, demonstrated that hospitals can use structured GRC frameworks to identify and close operational gaps. Their model, validated through interviews with senior executives representing 12.4% of Dutch hospital bed capacity, established 14 dimensions across five maturity levels as a roadmap for progressive GRC improvement. Alder [1] identifies a specific operational mechanism: integrated GRC enables two-way communication between governance, risk, and compliance functions, meaning that changes to policies are communicated more effectively, new risks are mitigated more quickly, and day-to-day compliance violations are avoided.

ADDED VALUE DIMENSION 5: REGULATORY COMPLIANCE AND REPUTATION PROTECTION

GRC provides healthcare organizations with a strategic, adaptive compliance architecture that simultaneously manages current regulatory requirements and positions institutions for future regulatory evolution. Handoko et al. [10] identify five compliance architecture

dimensions that GRC must address in healthcare: strategy, organization, processes, applications and data, and facilities. They note that companies face compliance challenges from the constant creation of new regulations, vague or overlapping regulatory language, and constantly changing interpretations all of which characterize the healthcare regulatory environment.

Karthick et al. [13] synthesized that GRC encourages organizations to approach compliance as a continuous process rather than a one-time event, requiring systematic monitoring, documentation, and improvement. This aligns with what Alqahtani et al. [3] found in their systematic review: healthcare organizations with mature GRC frameworks demonstrate greater regulatory resilience and are better positioned to absorb new compliance requirements without operational disruption. McCormack [7] frames reputation as a direct GRC output, noting that healthcare organizations can preserve trust, attract patients, and maintain positive relationships with stakeholders by adopting best practices, adhering to ethical guidelines, and promptly addressing compliance issues.

The COSO framework, widely applied in healthcare, provides the regulatory compliance architecture that GRC operationalizes, encompassing control environment, risk assessment, control activities, information and communication, and monitoring [16]. In healthcare, HIPAA serves as the defining compliance framework, but GRC allows organizations to manage HIPAA compliance alongside OSHA, accreditation requirements, billing regulations, and state-level privacy laws within a single integrated system. Nurdiani, Alie and Hamid [19] demonstrate how sectoral regulators can use GRC frameworks as both a governance standard and a compliance measurement tool, with the HITRUST CSF serving as the healthcare-specific equivalent.

ADDED VALUE DIMENSION 6: STRATEGIC RESILIENCE AND ENTERPRISE RISK MANAGEMENT

Integrating GRC with Enterprise Risk Management (ERM) creates a holistic risk governance structure that enhances strategic decision-making, organizational resilience, and hospital performance sustainability. The Healthcare Financial Management Association [12] describes five foundational areas for GRC-enabled ERM in healthcare: building a risk culture, formalizing risk governance, identifying risk appetite, leveraging GRC technology, and implementing continuous monitoring. Their analysis demonstrates that when GRC is integrated with ERM, hospitals move from compartmentalized risk silos toward an enterprise-wide risk intelligence function.

Censinet [5] identifies the core ERM integration challenge: too often, ERM is siloed within individual departments with little coordination between different functions. By integrating GRC into ERM efforts, healthcare organizations can gain a more holistic view of risk and make more informed decisions about where to allocate resources. This integration also enables healthcare organizations to adopt new technologies securely, fostering innovation rather than constraining it.

Dihartawan et al. [9], using SEM-PLS analysis of Indonesian hospital risk management, demonstrated that adaptability significantly improves ERM effectiveness in hospitals, and that ERM effectiveness positively correlates with hospital performance and sustainability. Handoyo et al. [11] confirm in their bibliometric analysis that GRC research is increasingly

converging on sustainability themes, with healthcare organizations viewing GRC not merely as a risk control mechanism but as a driver of long-term sustainable performance.

BARRIERS TO GRC IMPLEMENTATION IN HEALTHCARE

Despite the clear evidence of added value, the literature consistently identifies barriers that limit GRC effectiveness in healthcare settings. Alqahtani et al. [3] identify cultural resistance, limited financial and human resources, data privacy concerns, and fragmented implementation approaches as the primary barriers. Censinet [5] adds the perception problem GRC is often viewed as a punitive, reactive function rather than a proactive value driver which reduces organizational buy-in and limits the depth of implementation.

Mahendra, Prabowo and Hidayanto [15] highlight specific IT integration challenges: heterogeneous health information systems, interoperability failures between electronic health records and GRC platforms, and insufficient data governance infrastructure. Batenburg et al. [4] note that GRC maturity varies considerably across hospital contexts and that maturity models must be adapted to each institution's specific operational landscape. Handoko et al. [10] identify regulatory complexity itself as a barrier, noting that vague, overlapping, and constantly changing regulations make compliance architectures difficult to sustain without dedicated GRC infrastructure.

EMERGING TRENDS: AI AND TECHNOLOGY-ENABLED GRC

A growing body of literature identifies artificial intelligence as both an amplifier of GRC value and a source of new GRC challenges in healthcare. Censinet [6] reports that Gartner projects over half of large organizations will use AI and machine learning for continuous regulatory compliance checks by 2025, up from under 10% in 2021. AI-driven GRC solutions in healthcare are being applied to automate compliance monitoring, analyze electronic health records for compliance gaps, conduct real-time risk assessments, and generate ransomware mitigation policies [17].

The MetricStream and GRC Report survey of over 100 global GRC professionals [18] found that 46% highlighted an urgent need to build resilient enterprises for an unpredictable risk landscape, with AI governance frameworks emerging as a top priority. Respondents specifically warned that AI adoption in healthcare is accelerating faster than governance structures can adapt itself creating a new category of GRC risk. Handoyo et al. [11] confirm that AI, blockchain, and sustainability represent the three most significant emerging thematic clusters in GRC research, pointing toward the future evolution of healthcare GRC frameworks.

SUMMARY: LITERATURE MAP OF ADDED VALUE

Table 1 synthesizes the six dimensions of GRC value identified in this review, mapping each to primary evidence and key empirical findings.

Table 1: Summary of the added value dimensions of GRC in the healthcare sector, with corresponding primary evidence and key metrics.

Value Dimension	Primary Evidence	Key Metric / Finding
Firm value & investor confidence	Kembaren et al. [14]; Karthick et al. [13]	GRC explains 33.8% of firm value variation; effect strengthened during COVID-19 pandemic
Patient safety & care quality	Alqahtani et al. [3] (22 studies, PRISMA)	GRC positively associated with patient safety, care quality, and compliance across 5 countries
Cyber risk resilience	Compyl [8]; Censinet [6]; Alharbi et al. [2]	Average breach cost $9.7 M; AI-GRC integration improved compliance efficiency by 62%
Operational efficiency	Censinet / Forrester [6]; Handoko et al. [10]	47% control reduction; 60% testing time reduction; 300%+ ROI over 3 years
Regulatory compliance & reputation	HIPAA Journal [1]; Compliancy Group [7]; Handoko et al. [10]	Integrated GRC eliminates compliance silos and protects institutional reputation
Strategic resilience & ERM	HFMA [12]; Censinet [5]; Dihartawan et al. [9]	GRC-ERM integration improves hospital performance, sustainability, and decision-making

Note: GRC = Governance, Risk, and Compliance; ERM = Enterprise Risk Management; PRISMA = Preferred Reporting Items for Systematic Reviews and Meta-Analyses; ROI = Return on Investment.

CONCLUSION

The converging evidence from academic literature, systematic reviews, bibliometric analyses, and industry research establishes that GRC adds measurable, multi-dimensional value to healthcare organizations, operating across financial, clinical, operational, regulatory, reputational, and strategic dimensions simultaneously. The critical insight emerging from this review is that the value of GRC in healthcare is multiplicative rather than additive: governance, risk management, and compliance create greater value when integrated than when managed as separate functions [3, 12, 14].

The evidence from Kembaren et al. [14], Alqahtani et al. [3], and the HFMA [12] converges on this point: integrated GRC enables healthcare organizations to respond faster, spend less on compliance, sustain higher quality care, maintain investor confidence, and build the organizational resilience needed to navigate continuous disruption. Future research should address the quantification of GRC value in non-financial healthcare outcomes, the role of AI and digital transformation in reshaping GRC architectures, and the cultural and behavioral dimensions that determine whether GRC frameworks achieve their potential or become bureaucratic compliance exercises.

REFERENCES

[1] Alder S. Healthcare governance, risk management, and compliance (GRC). HIPAA Journal. 2024. Available from: https://www.hipaajournal.com/healthcare-governance-risk-management-and-compliance-grc/

[2] Alharbi F, Sabra M, Alharbe N, Almajed A. Towards a strategic IT GRC framework for healthcare organizations. International Journal of Advanced Computer Science and Applications. 2022;13(1). doi:10.14569/IJACSA.2022.0130125

[3] Alqahtani FSA, Belal AAA, Zakri NIM. Impact of governance, risk management and compliance on healthcare system: A systematic review. Journal of Contemporary Dentistry & Practice. 2025;26(9):904–911. doi:10.5005/jp-journals-10024-3943

[4] Batenburg R, Neppelenbroek M, Shahim A. A maturity model for governance, risk management and compliance in hospitals. Journal of Hospital Administration. 2014;3(4):43–52.

[5] Censinet. Key challenges facing GRC in healthcare. 2022. Available from: https://censinet.com/blog/key-challenges-facing-grc-in-healthcare

[6] Censinet. Why 92% of healthcare organizations are failing at GRC integration and how AI changes everything. 2025. Available from: https://censinet.com/perspectives/healthcare-organizations-grc-integration-ai-impact

[7] Compliancy Group (McCormack M). Healthcare governance risk and compliance. 2024. Available from: https://compliancy-group.com/healthcare-governance-risk-and-compliance/

[8] Compyl. Guide to GRC in healthcare. 2026. Available from: https://compyl.com/blog/the-role-of-grc-in-healthcare/

[9] Dihartawan D, Lestari F, Widanarko B, Besral B. Analysis of factors affecting hospital risk management in Indonesia: The SEM-PLS approach. Kesmas. 2024;19(2):135–143.

[10] Handoko BL, Riantono IE, Gani E. Importance and benefit of application of governance risk and compliance principle. Systematic Reviews in Pharmacy. 2020;11(9):510–513.

[11] Handoyo S et al. A bibliometric analysis of governance, risk, and compliance (GRC): trends, themes, and future directions. Humanities and Social Sciences Communications. 2025. Available from: https://www.nature.com/articles/s41599-025-06194-9

[12] Healthcare Financial Management Association (HFMA). ERM: Evolving from risk assessment to strategic risk management. 2022. Available from: https://www.hfma.org/finance-and-business-strategy/enterprise-risk-management/60137/

[13] Karthick V, Prabhakaran J, Banu P, Senthil Kumar US. Systematic literature review on GRC: A study on best practices and implementation strategy in GRC. Samdarshi. 2023;16(4):3558–3570.

[14] Kembaren SYS, Endro G, Pendrian O. Effect of governance, risk management and compliance on a firm's value (healthcare industry). Enrichment: Journal of Management. 2022;12(5):4076–4087.

[15] Mahendra I, Prabowo H, Hidayanto AN. Information technology challenges for integrated governance, risk, and compliance (GRC). In: Proceedings of the 2022 1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS); 2022. p. 79–84. IEEE.

[16] Makas A. Governance, risk and compliance frameworks applicability in the organizations. International Journal of Science and Research Archive. 2023;10(2):716–724.

[17] McIntosh T, Liu T, Susnjak T, Alavizadeh H, Ng A, Nowrozy R, Watters P. Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. Computers & Security. 2023;134:103424.

[18] MetricStream & GRC Report. GRC in 2025: 5 essential survey insights for today's risk and compliance leaders. 2025. Available from: https://www.metricstream.com/blog/essential-survey-insights-grc-risk-compliance-leaders.html

[19] Nurdiani TW, Alie RM, Hamid IR. The fundamentals of competency standards for implementation of governance, risk management, and compliance (GRC). Samdarshi. 2023;16(4).

[20] Racz N, Weippl E, Seufert A. A frame of reference for research of integrated governance, risk and compliance (GRC). In: Communications and Multimedia Security: 11th IFIP TC 6/TC 11 International Conference; 2010. p. 106–117.

[21] Shahim A, Batenburg R, Vermunt G. Governance, risk and compliance: A strategic alignment perspective applied to two case studies. In: ICT Critical Infrastructures and Society: HCC10 2012; 2012. p. 202–212.

[22] Spanaki K, Papazafeiropoulou A. Analysing the governance, risk and compliance (GRC) implementation process: primary insights. In: Proceedings of the 21st European Conference on Information Systems (ECIS); 2013.

[23] Swiss GRC. Ensuring healthcare resilience with governance, risk and compliance (GRC). 2024. Available from: https://swissgrc.com/en/ensuring-healthcare-resilience-with-governance-risk-compliance-grc/

[24] Vicente P, Mira da Silva M. A conceptual model for integrated governance, risk and compliance. In: Advanced Information Systems Engineering: CAiSE 2011; 2011. p. 199–213.

[25] WJARR. AI-driven GRC in cybersecurity: Applications in healthcare compliance monitoring. World Journal of Advanced Research and Reviews. 2024.