Scientific Journal of Informatics
Vol. 13, No. 3, August 2026
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji e-ISSN 2460-0040

An Integrated Cybersecurity Governance Ecosystem for Healthcare: A Quality-Appraised Systematic Review of Governance, Risk, and Compliance Frameworks for AI, Cloud, and Connected Health Technologies

Chipo Miranda Mukwaira[1], Yvonne Chigariro[2], Belinda Ndlovu[3]*
[1,2]Informatics Department, National University of Science and Technology, Zimbabwe
[3]School of Computing, University of South Africa, South Africa

Abstract.
Purpose: The growing use of digital technologies in healthcare has significantly increased exposure to cybersecurity risks, creating a need for governance approaches that go beyond traditional control-based security models. This study reviews how Governance, Risk, and Compliance (GRC) frameworks are applied in healthcare cybersecurity, focusing on their effectiveness, implementation challenges, and integration into organizational governance.
Methods: Using the PRISMA methodology, literature was collected from PubMed, IEEE Xplore, and ScienceDirect, with 20 studies included in the final analysis and individually quality-appraised against six criteria.
Findings: The findings indicate a shift from traditional frameworks to more flexible, integrated governance approaches that account for emerging technologies, including artificial intelligence (AI), cloud computing, and interconnected healthcare systems. While GRC frameworks help improve governance structures, strengthen cybersecurity, and support regulatory compliance, their effectiveness is often limited by factors such as skills shortages, resource constraints, regulatory complexity, and legacy systems. The study also identifies key enablers of successful implementation, including leadership involvement, cross-departmental collaboration, and continuous monitoring.
Novelty: Based on these findings, an integrated healthcare cybersecurity governance framework is proposed that aligns regulatory, organizational, and technological dimensions within a unified model and provides practical insights to strengthen resilience in modern healthcare systems. Unlike prior reviews that examine GRC frameworks in isolation, this study also compares quality-appraised evidence across frameworks to show which approaches work best in different organizational contexts, including those governing AI, cloud computing, and other connected health technologies. For example, control-catalog frameworks such as ISO 27001 and COBIT are best suited to larger, well-resourced organizations, whereas AI governance frameworks succeed only once regulatory uncertainty is resolved internally.

Keywords: Healthcare Cybersecurity Governance, Governance, Risk and Compliance (GRC), Artificial Intelligence Governance, Cloud Computing Security, Digital Health

Received May 2026 / **Revised** June 2026 / **Accepted** August 2026

INTRODUCTION

The application of digital technologies in healthcare service delivery has transformed how services are delivered, managed, and monitored. Modern healthcare organizations rely heavily on technologies such as electronic health records (EHRs), telemedicine, cloud computing, AI solutions, and connected devices, which help improve efficiency and the quality of care [1], [2], [3]. Although the benefits of digital technologies are well known, innovations also introduce new cybersecurity threats, including data breaches, ransomware attacks, and system disruptions [4], [5], [6]. Considering that healthcare services have become more technology- and data-driven today, it is crucial to implement cybersecurity governance to ensure patient safety, maintain uninterrupted operations for healthcare providers, and comply with regulations [7].

Additionally, the use of emerging technologies exacerbates the cybersecurity challenges faced by healthcare organizations. The use of AI algorithms in diagnosis, decision-making, and analysis increases the importance of transparency and accountability in AI-based systems [3],[8],[9],[10]. Furthermore, the

[3]*Corresponding author.
Email addresses: 69970777@mylife.unisa.ac.za (Ndlovu).
DOI: 10.15294/sji.v13i3.49854

implementation of blockchain technology, cloud computing, and the Internet of Medical Things (IoMT) enables enhanced interoperability [11]; however, these distributed systems are prone to cybersecurity breaches [8],[12],[13]. All these factors prove the ineffectiveness of the control-oriented approach to cybersecurity management [14], [15].

In addition, the consequences of cybersecurity failures in healthcare are much more severe compared to those observed in other sectors due to direct impacts on patient safety. Unauthorized access to personal medical information, cyber-attacks leading to the disruption of healthcare services, and any other cybersecurity issue may result in delayed treatment and jeopardize patients' health [16]. Thus, cybersecurity measures in healthcare should be integrated into organizational policies and linked to risk management and compliance [7], [17].

Governance, Risk Management, and Compliance (GRC) frameworks represent methodological approaches to cybersecurity governance that aim at enhancing accountability and risk-based decision-making [18],[19]. GRC frameworks are designed to promote coordination among various stakeholders involved in cybersecurity governance and to align security measures with business strategies and regulatory requirements. However, a vast majority of studies on GRC frameworks focus on specific frameworks or technologies without considering their integration into healthcare organizations [14], [7].

Prior reviews in this space have tended to examine governance in relation to a single framework or a single technology rather than the healthcare governance ecosystem. For example, existing systematic reviews have focused narrowly on blockchain-based digital signature frameworks for healthcare data security [14],[20], privacy-aware cloud governance frameworks [18], and the impact of GRC specifically on healthcare systems [21], AI security governance frameworks for regulated industries in general, rather than healthcare specifically [22], IT GRC maturity and financial reporting outcomes [23], IoT-focused risk management frameworks [24], cloud API security challenges [25], and threat-intelligence-driven risk management [26]. Although all the studies provide insight into their specific frameworks or technologies, none of them attempts to integrate the governance dimensions of regulation, organization, and technology into a single theoretical model. Moreover, there is no comparative analysis of GRC frameworks to explain how they function across the governance dimensions listed above. With respect to governance issues in healthcare organizations related to the use of AI, cloud computing, and IoT technologies, very little research has examined the interaction between conventional, compliance-based frameworks (ISO 27001, HIPAA, NIST Cybersecurity Framework) and these emerging technology domains. This research attempts to fill that gap in literature.

Therefore, it is necessary for scientists to explore approaches that would allow them to apply GRC concepts to cybersecurity governance in the healthcare sector. Considering the above statement, this research paper critically analyzes the existing literature on GRC and healthcare cybersecurity to assess the approach's efficiency, challenges, and potential applications. Contrary to prior studies that analyzed cybersecurity governance issues in isolation, this paper considers the interdisciplinary nature of cybersecurity and treats it as a socio-technical activity requiring collaboration across regulatory, organizational, and technical levels.

This study addresses the following research questions:
1) What Governance, Risk, and Compliance (GRC) frameworks are currently used in healthcare cybersecurity governance?
2) How do GRC frameworks contribute to improving cybersecurity governance and organizational resilience in healthcare settings?
3) What challenges do healthcare organizations face when implementing GRC frameworks for cybersecurity governance?
4) How is cybersecurity governance integrated into broader enterprise governance structures within healthcare institutions?
5) What best practice governance models can be identified for strengthening cybersecurity governance in healthcare?

METHODS

This review adheres to the PRISMA 2020 guidelines to ensure that the research process is transparent, consistent, and replicable. Prior to conducting the review, a protocol was drafted outlining the methodology

for conducting searches, including the criteria for study inclusion and exclusion, quality assessment, data extraction, and thematic analysis. Careful record-keeping and cross-checking of decisions made during the screening phase were conducted to avoid bias.

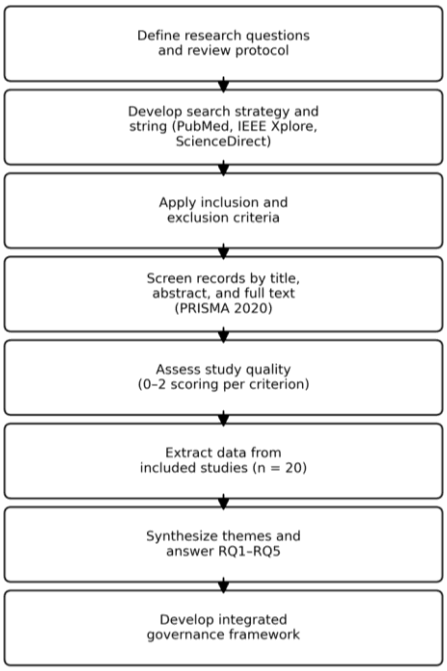

Figure 1. Research workflow of the systematic review

Search Strategy

A systematic search of the literature was conducted on 2 February 2026 across three major databases: PubMed, IEEE Xplore Digital Library, and ScienceDirect. These databases have been selected for their extensive coverage of scholarly publications on healthcare, cybersecurity, and information systems. In this regard, three core concepts have been considered, namely governance and compliance, healthcare, and cybersecurity. All the concepts were linked with each other using Boolean operators (AND, OR). A consistent search string was formed, with only slight modifications for each database.

The final search string used in the study is presented below:
("governance" OR "risk management" OR "compliance" OR "GRC") AND ("healthcare" OR "health care" OR hospital OR clinic) AND ("cybersecurity" OR "information security" OR "security management" OR "cyber risk").

Inclusion and Exclusion Criteria

The inclusion criteria for the articles whose major theme is cybersecurity governance in the healthcare sector, with special emphasis on cybersecurity governance implementation, included peer-reviewed articles providing information related to at least one of the following domains: governance mechanism implementation, effectiveness of governance, problems associated with implementation, governance mechanisms for enterprise environments, and best practices for governance. Peer-reviewed articles written in English and published between 2020 and 2026 were eligible if they provided significant information about cybersecurity governance mechanisms in the healthcare industry that include hospitals, clinics, or digital healthcare systems. The exclusion criteria were articles whose major theme was limited to cybersecurity measures with no mention of cybersecurity governance measures; articles dealing with cybersecurity governance in any field other than healthcare; and non-peer-reviewed articles

Screening and Selection Process

Inclusion of studies was done using the PRISMA guideline. Searches in the databases PubMed, IEEE Xplore, and ScienceDirect identified 9,820 publications. Removing 2,870 duplicates left 6,950 records, which were screened based on their titles and abstracts; 6,700 were rejected as irrelevant to the theme of healthcare cybersecurity governance and GRC methodologies, leaving 250 reports to be retrieved. 10 of them could not be retrieved; therefore, 240 reports were left for full-text screening. In the screening process,

220 reports were excluded (210 for inadequate relevance and detail and 10 for not being peer-reviewed or being opinionated), leaving 30 reports for further screening. Finally, 10 reports were discarded after quality screening because they did not meet the quality requirements discussed below; hence, 20 studies were included in the review, in accordance with the PRISMA flow diagram shown in Figure 1.

Included studies

This literature review is based on 20 studies. The studies include both theoretical and empirical studies, along with governance framework analysis related to healthcare cybersecurity. The results from selected research articles shed light on governance methods, the efficiency of GRC frameworks, implementation issues, and integration techniques in healthcare cybersecurity.

Quality Assessment and Risk of Bias

Six quality criteria served as standards for evaluating all research papers: clarity of purpose, quality of methods, pertinence to healthcare cybersecurity governance, correctness, value to science, and recognition of the paper's limitations by its authors. The rating for each criterion was set on a 0-2 scale, resulting in a maximum score of 12 points. Depending on the total score, research papers were divided into high-quality papers (scores of 8 points or higher), medium-quality papers (scores from 5 to 7 points), and low-quality papers (scores below 4 points).

Table 1. Quality assessment criteria for included studies

Criterion	Description	Scoring Guide
Clarity of objectives	Evaluates whether the study clearly states its research aim and purpose	0 = unclear, 1 = partially clear, 2 = clearly defined
Methodological transparency	Assesses how well the study explains its research methods and procedures	0 = not described, 1 = limited detail, 2 = clearly explained
Relevance to healthcare cybersecurity governance	Determines how closely the study relates to the research topic	0 = not relevant, 1 = somewhat relevant, 2 = highly relevant
Validity of findings	Examines whether the results are supported by appropriate evidence or analysis	0 = weak evidence, 1 = moderate support, 2 = strong support
Contribution to knowledge	Considering the extent to which the study adds new insights or understanding	0 = minimal contribution, 1 = moderate contribution, 2 = significant contribution
Identification of limitations	Checks whether the study acknowledges its own limitations	0 = not mentioned, 1 = partially discussed, 2 = clearly discussed

Table 2 summarizes the individual quality score of the 20 selected articles against each of the six criteria listed in Table 1, as well as their classification and total score of 12. 15 studies (75%) have received a high-quality rating (8 to 12 points). The other five studies [27], [17], [28], [24], and [26] belong to the category of medium quality (5 to 7 points), but they are all conceptual or practice frameworks, and not empirical or systematic review articles. These five studies received low scores due to a lack of methodological transparency and a lack of discussion of limitations, as they do not report a reproducible search or data collection procedure. Nevertheless, these five studies are included in the synthesis because they offer a unique conceptual framework or governance approach not found in the other selected articles (see Table 4). Hence, the findings in these five studies should be viewed merely as illustrations, not as empirical research, and conclusions based primarily on this set of studies are marked accordingly in the discussion. No study is classified as low quality (≤ 4 points), and thus none is omitted from the synthesis due to quality issues.

Table 2. Quality scores for included studies (N = 20)

Ref	Clarity	Methodology	Relevance	Validity	Contribution	Limitations	Total (/12)	Category
[4]	2	1	2	1	2	1	9	High
[7]	2	1	2	1	1	1	8	High
[14]	2	2	2	2	2	1	11	High
[27]	1	0	2	1	1	0	5	Medium
[21]	2	2	2	2	2	2	12	High
[29]	2	1	2	1	2	1	9	High
[17]	1	0	2	1	2	1	7	Medium
[15]	2	2	2	2	2	1	11	High
[22]	2	2	2	2	2	2	12	High
[23]	2	2	2	2	1	1	10	High

Ref	Clarity	Methodology	Relevance	Validity	Contribution	Limitations	Total (/12)	Category
[30]	2	2	2	2	2	2	12	High
[19]	2	2	2	2	2	1	11	High
[28]	1	0	2	1	2	1	7	Medium
[24]	1	0	2	1	2	1	7	Medium
[2]	2	2	2	2	2	2	12	High
[25]	2	2	2	2	1	1	10	High
[31]	2	1	2	2	2	1	10	High
[26]	1	0	2	1	2	1	7	Medium
[5]	2	2	2	2	2	2	12	High
[1]	2	2	2	2	2	1	11	High

The rationale for including each of the 20 selected studies in the current review is detailed in Table 3. It indicates the nature of the study in terms of the theme it addresses, how it answers the research questions posed and why it is relevant. This format ensures that the selected studies are useful in answering the questions on the GRC framework in healthcare cybersecurity.

Table 3: Justification for included studies (N = 20)

Source	Study Focus	Relevance to Research Questions	Justification for Inclusion
[4]	Strategic management approaches to healthcare system resilience	Relates to governance structures that support healthcare system resilience and risk management	Included for its discussion of strategic governance approaches applicable to healthcare cybersecurity management
[7]	Cyber risk management frameworks and strategies	Examine frameworks used to manage cybersecurity risks	Included due to its focus on structured cyber risk management frameworks relevant to GRC
[14]	Blockchain digital signature frameworks for healthcare data security	Addresses technological frameworks protecting healthcare data	Included for its insights into security frameworks used in healthcare information systems
[27]	Governance and lifecycle management of Agentic AI in healthcare	Explores governance mechanisms for AI technologies in healthcare	Included for its relevance to governance structures managing emerging digital technologies
[21]	Governance, Risk Management and Compliance in Healthcare Systems	Directly examine the impact of GRC frameworks in healthcare environments	Included as a core study addressing healthcare GRC implementation
[29]	Strategic IT GRC framework for healthcare organizations	Proposes a governance framework integrating IT governance and risk management	Included for presenting a healthcare-specific GRC governance model
[17]	Governance-centric cybersecurity framework for healthcare	Introduces governance-based approaches to healthcare cybersecurity	Included due to its focus on governance integration within healthcare cybersecurity
[15]	Artificial intelligence and data governance in African healthcare	Examines governance and regulatory considerations for AI-driven healthcare systems	Included for its insights on data governance and emerging technologies in healthcare
[22]	AI security governance frameworks for regulated industries	Reviews governance models for AI risk management	Included due to its relevance to governance frameworks applicable to healthcare environments
[23]	IT GRC maturity and organizational performance	Investigate the maturity of GRC practices and their impact on organizational performance	Included for insights into governance maturity models within GRC systems
[30]	Data governance frameworks for healthcare data security	Evaluates regulatory frameworks such as ISO standards, GDPR, and HIPAA	Included for its analysis of compliance and regulatory governance in healthcare cybersecurity
[19]	Privacy-aware cloud frameworks for healthcare data governance	Examines governance mechanisms for secure healthcare cloud environments	Included because it addresses governance for cloud-based healthcare data systems
[28]	Human oversight and AI automation in GRC practices	Explores governance mechanisms balancing AI automation and human oversight	Included due to its relevance to governance integration in GRC environments
[24]	Risk management frameworks for healthcare IoT security	Investigate cybersecurity frameworks for healthcare Internet of Things devices	Included because it addresses emerging technological risks in healthcare cybersecurity

Source	Study Focus	Relevance to Research Questions	Justification for Inclusion
[2]	Healthcare AI governance maturity model	Develop maturity models for AI governance in healthcare	Included for its contribution to governance maturity assessment in healthcare systems
[25]	Security challenges in healthcare cloud APIs	Reviews of vulnerabilities and governance challenges in healthcare cloud infrastructures	Included due to its focus on cybersecurity risks in healthcare digital infrastructure
[31]	Risk management best practices for healthcare data security	Discusses best practice strategies for healthcare cybersecurity governance	Included for its practical insights into risk management and security governance
[26]	Threat intelligence-driven risk management frameworks	Examines intelligence-driven cybersecurity risk governance for healthcare cloud systems	Included for its discussion of advanced risk management frameworks
[5]	Governance frameworks for safe and responsible AI in healthcare	Reviews governance models supporting responsible AI adoption	Included due to its relevance to governance mechanisms in healthcare technologies
[1]	Ethical and governance frameworks for artificial intelligence	Explores ethical governance structures for AI systems	Included for its contribution to governance principles relevant to healthcare technology oversight

To improve the review's validity, a systematic screening method based on the PRISMA criteria was used. The search method was designed to identify relevant literature focused on healthcare cybersecurity governance. Screening was conducted using a systematic process in which the article title was screened first, followed by the abstract, and finally the full text.

RESULT AND DISCUSSION

Figure 2 shows the PRISMA flow diagram used to illustrate how studies were selected for this SLR.

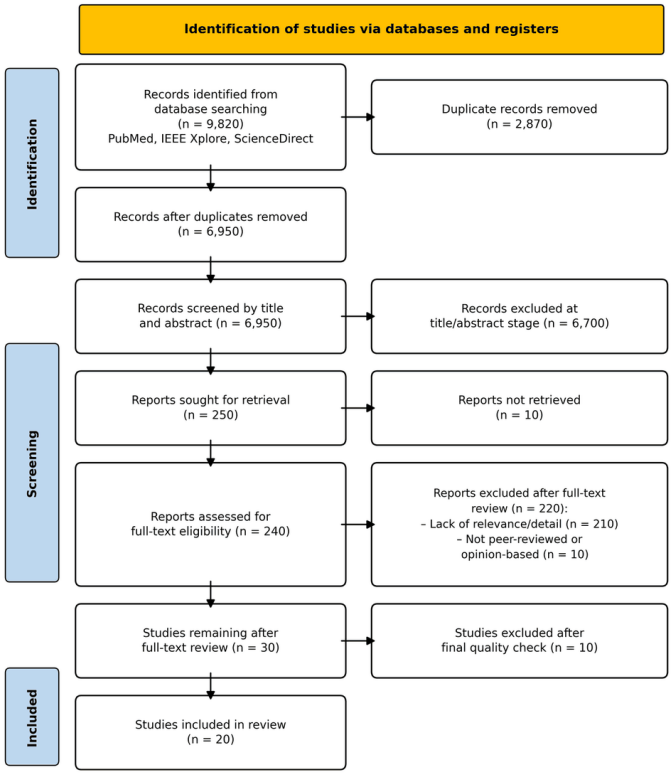

Figure 2. PRISMA screening results

Table 4 summarizes the 20 articles included in the review, detailing each article's main features and results. This table contains details about the country background, the theories used, the outcomes mentioned, the issues faced, and the best practices identified. The organization of this table follows the order of the research questions posed.

Table 4. Summary of articles included in the review

Ref	Country	Framework	Key Findings	Sample / Scope	Best Practice
[4]	Indonesia	Strategic Governance / Policy Frameworks	Proposes a strategic governance model linking healthcare resilience planning to organizational policy; finds that resilience improves when governance structures are embedded at the board level rather than delegated solely to IT.	Single-country conceptual analysis (Indonesia); no fixed sample size reported	Risk-based continuous improvement
[7]	South Africa	NIST CSF	NIST CSF case studies apply to healthcare-adjacent settings; reports that organizations using staged NIST CSF implementation close more skills gaps than those attempting full adoption at once.	Multiple case studies; sample size not numerically reported	Unified policy frameworks
[14]	China	Blockchain governance frameworks	Reviews blockchain-based digital signature frameworks for healthcare data; finds compliance and audit readiness improve but integration complexity rises sharply with legacy EHR systems.	primary study count not separately reported	Zero-trust and modern architecture models
[27]	Sweden	AI governance frameworks	Proposes a lifecycle model for agentic AI governance in healthcare; highlights regulatory uncertainty as the dominant barrier to adoption across the AI lifecycle stages studied.	Conceptual framework paper; no empirical sample	Unified policy frameworks
[21]	Saudi Arabia	ISO 27001 / ISMS	Systematically reviews the impact of GRC on healthcare systems; finds ISO 27001-aligned ISMS implementations improve compliance and audit readiness but increase documentation burden on clinical staff.	Primary study count is not separately reported	Standardization via control mapping
[29]	Saudi Arabia	IT GRC Framework	Proposes a healthcare-specific IT GRC framework based on a single-site case study; reports governance maturity gains constrained by limited resourcing for ongoing control monitoring.	Single-site case study (King Fahad Medical City, Saudi Arabia)	Risk-based continuous improvement
[17]	United States	NIST CSF	Introduces a governance-centric, systems-level cybersecurity framework; finds security incident counts fall most where skills gaps in security operations are addressed directly through training.	Conceptual systems-perspective framework; no fixed empirical sample	Workforce training & cybersecurity culture

Ref	Country	Framework	Key Findings	Sample / Scope	Best Practice
[15]	Kenya	Strategic Governance / Policy Frameworks	Reviews AI and data governance approaches across African healthcare systems; finds regulatory complexity and cross-border data rules are the most cited obstacle to governance maturity.	review of African healthcare AI/data governance studies	Unified policy frameworks
[22]	United States	AI governance frameworks	Reviews AI security governance frameworks across regulated industries including healthcare; finds risk analysis and control selection improve when framework complexity is reduced to a small core control set.	review spanning healthcare, financial services, and gaming sectors	Risk-based continuous improvement
[23]	Indonesia	COBIT	Systematically reviews IT GRC maturity in relation to organizational and financial-reporting performance; finds governance maturity gains are constrained chiefly by resource limitations rather than framework choice.	review; primary study count not separately reported	Standardization via control mapping
[30]	International	ISO 27001 / HIPAA / GDPR	Quantitatively analyzes ISO 27001, GDPR, and HIPAA-aligned data governance frameworks in blockchain-enabled healthcare systems; finds combined-standard approaches improve compliance but raise regulatory complexity.	Quantitative analysis of multi-standard blockchain healthcare implementations	Standardization via control mapping
[19]	China	Cloud governance frameworks	Reviews privacy-aware cloud governance frameworks for medical e-governance data; finds risk analysis and control selection improve while legacy on-premise systems remain the main integration barrier.	primary study count not separately reported	Zero-trust and modern architecture models
[28]	United Kingdom	AI governance / GRC frameworks	Examines how human oversight is balanced against AI automation in GRC practice for high-threat IT delivery environments; finds governance maturity improves when oversight is embedded cross-functionally rather than centralized.	Practice-based conceptual analysis; no fixed empirical sample	Workforce training & cybersecurity culture
[24]	United States	IoT security frameworks	Reviews risk management frameworks for healthcare IoT beyond perimeter-based security; finds security incidents fall and posture improves when	Conceptual framework review of healthcare IoT security literature	Zero-trust and modern architecture models

Ref	Country	Framework	Key Findings	Sample / Scope	Best Practice
			legacy network-segmentation limitations are addressed directly.		
[2]	International	AI governance maturity models	Develops a maturity model for healthcare AI governance based on a systematic review; finds governance maturity gains are most often limited by residual skills gaps in AI risk assessment.	review informing a multi-level maturity model	Workforce training & cybersecurity culture
[25]	United States	Cloud security governance	Systematically reviews security challenges in healthcare cloud APIs; finds incident rates fall with stronger API governance, though third-party vendor risk remains difficult to govern directly.	primary study count not separately reported	Zero-trust and modern architecture models
[31]	Brazil	ISO 27001 / ISMS	Analyzes best-practice data security risk management for healthcare; finds risk analysis and control selection improve where resource constraints are addressed through phased, prioritized investment.	Framework analysis of healthcare data-security best practices (Brazil)	Risk-based continuous improvement
[26]	United States	Threat intelligence frameworks	Proposes threat-intelligence-driven risk management for healthcare cloud systems; finds incident posture improves substantially but third-party vendor risk is the hardest category to mitigate through intelligence alone.	Conceptual framework paper; no fixed empirical sample	Risk-based continuous improvement
[5]	Australia	AI governance frameworks	Scoping review of frameworks for safe and responsible AI in healthcare organizations; finds governance maturity improves where regulatory ambiguity is resolved through internal policy rather than awaiting external standards.	primary study counts not separately reported	Unified policy frameworks
[1]	Malaysia	Ethical AI governance frameworks	Systematic review of ethical and governance frameworks for AI; finds compliance and audit readiness improve when ethical principles are operationalized as concrete controls rather than high-level statements.	primary study counts not separately reported	Workforce training & cybersecurity culture

The overview in Table 4 highlights deviations in the design of the GRC framework, the benefits achieved, implementation challenges, and the governance strategies employed across the 20 included studies. The analysis of Table 4 suggests a clear trend across most papers: implementing GRC frameworks improves governance and risk management. In some cases, GRC frameworks also help improve security operations. However, the implementation process can be quite complicated, as shown in the table below. Problems

such as resource shortages, a lack of knowledge, and integration issues have been noted in several papers. The comparison of results across different countries and organizations suggests that the impact of GRC frameworks cannot be generalized. To sum up, Table 4 shows that the use of GRC frameworks improves cybersecurity governance but only if the frameworks are implemented properly.

Publication trends of included studies

Figure 3 shows how the number of studies in this review has changed over time, covering the period from 2020 to 2026.

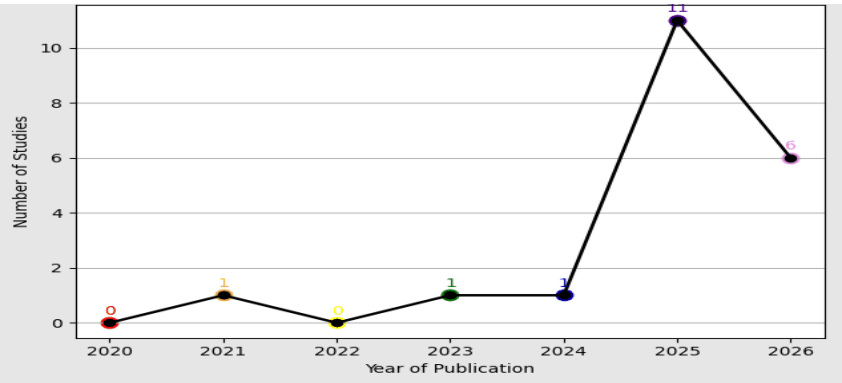

Figure 3. Publication trend of included studies (n = 20)

Figure 3 shows the timeline of research articles related to governance in healthcare cybersecurity. It shows an insignificant number of articles in the initial stages: none in 2020 and 2022 (n = 0), and only one in 2021, 2023, and 2024 (n = 1). The highest number of articles was observed in 2025 (n = 11, 55%), followed by 2026 (n = 6, 30%).

Continental distribution of studies

Figure 4 shows the distribution of the selected studies across different regions.

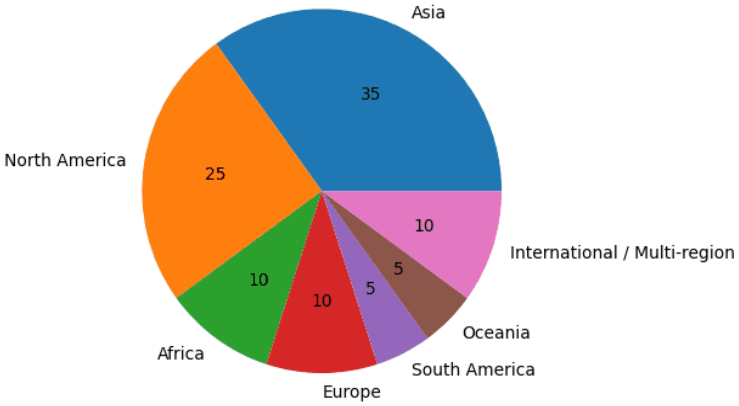

Figure 4. Continental distribution of studies

Figure 4 shows the geographical location of the chosen studies. The largest number comes from Asia (n = 7, 35%) and North America (n = 5, 25%). There are relatively small numbers from Europe and Africa (n = 2, 10%) and small numbers from South America and Oceania (n = 1, 5%). International/multi-regional studies constitute a minority (n = 2, 10%).

Framework distribution

Figure 5 shows the distribution of cybersecurity governance frameworks across the reviewed studies.

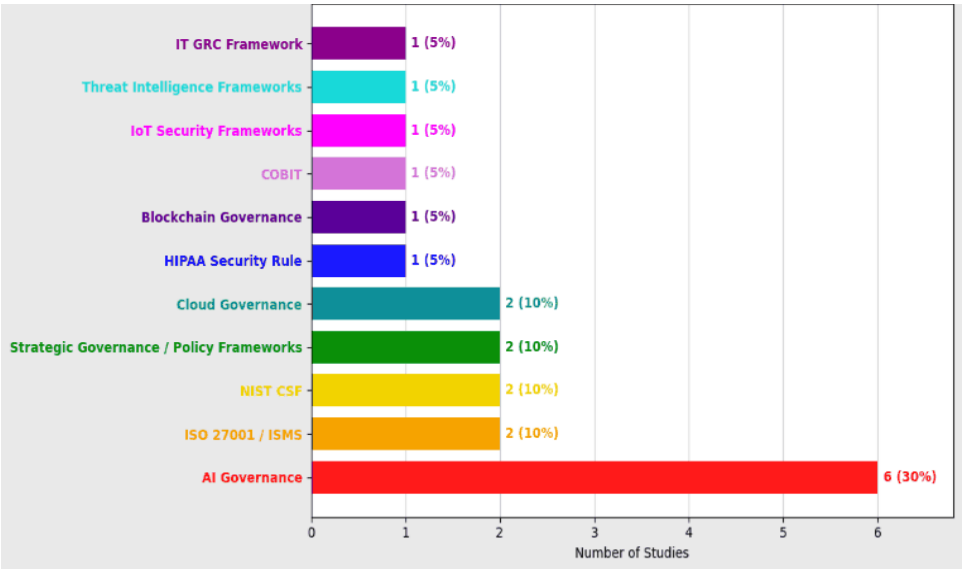

Figure 5. Frequency of referenced frameworks

An analysis of the occurrence of different types of governance frameworks in the examined literature shows a clear trend. AI governance frameworks occur most frequently, with six instances (30%), pointing to their growing importance in healthcare governance. The traditional governance frameworks, such as ISO 27001 and the NIST Cybersecurity Framework, as well as strategic and cloud governance frameworks, each occur twice (10% each). Other types of governance frameworks, such as blockchain, COBIT, IoMT, and threat intelligence, occur once (5% each).

Beyond frequency, the studies in Table 4 suggest that which framework performs best depends heavily on the organizational context in which it is applied. ISO 27001-aligned ISMS and COBIT-based approaches [21], [29], [23], [30], [31] consistently report gains in compliance and audit readiness, but these gains come with a documentation burden that several studies note is difficult for resource-constrained organizations to sustain [21], [23]. These control-catalog frameworks, therefore, appear best suited to larger, more resourced healthcare organizations that already have dedicated compliance staff, rather than smaller providers. By contrast, AI governance frameworks and maturity models [27],[22], [28], [2] are most frequently adopted by organizations facing rapid technology change, but their effectiveness is consistently reported as contingent on resolving regulatory uncertainty first [27], [22].Where that uncertainty is not resolved internally, governance maturity gains stall regardless of the framework's technical design. Cloud and IoT/IoMT-focused frameworks [19],[24],[25] succeed specifically at reducing security incidents in environments with significant legacy infrastructure, but every study in this category also reports that third-party vendor risk remains largely ungoverned by the framework itself [25], [26], suggesting these frameworks are necessary but not sufficient where vendor dependence is high. Among all types of frameworks, organizational issues such as executive sponsorship and cross-functionality show a more consistent link to implementation success than does framework choice. Research papers that highlight governance being present either at the board level or at the cross-functional level [4], [29], [28]usually report better results than studies that present governance as being left solely to IT and security teams, regardless of the framework used. This indicates that the choice of framework plays a smaller role than the organizational context in which it is applied.

Advantages of governance, risk, and compliance (GRC) frameworks

Figure 6 shows the main advantages of GRC frameworks based on the studies included in this review.

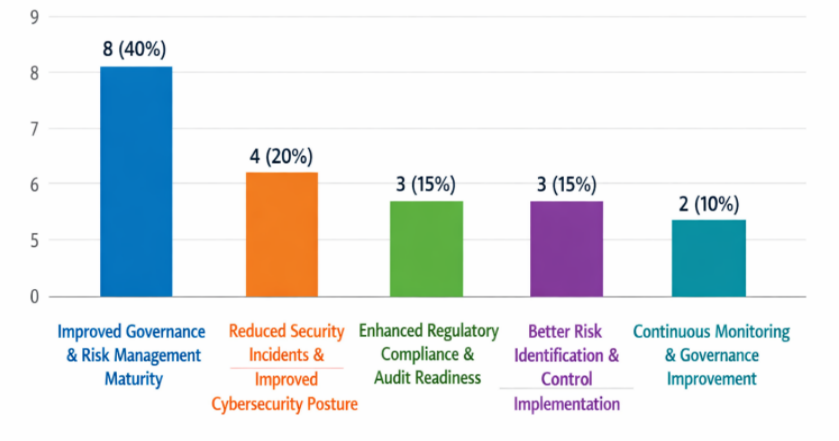

Figure 6. Key advantages of Governance, Risk, and Compliance (GRC) frameworks

The main benefits of GRC approaches, as mentioned in the reviewed literature, are shown in Figure 6. The most common benefit is the development of governance and risk management maturity (n=8, 40%). Another improvement noted in several articles concerns cybersecurity, which involves a decrease in the number of security incidents (n=4, 20%). Three studies highlight the benefits of improved compliance and audits as well as better risk identification and risk control (n=3, 15%). Other improvements, such as continuous monitoring and governance enhancement, are observed in two papers (n=2, 10%).

Implementation challenges in healthcare GRC adoption

Figure 7 shows the common challenges faced when implementing GRC frameworks in healthcare.

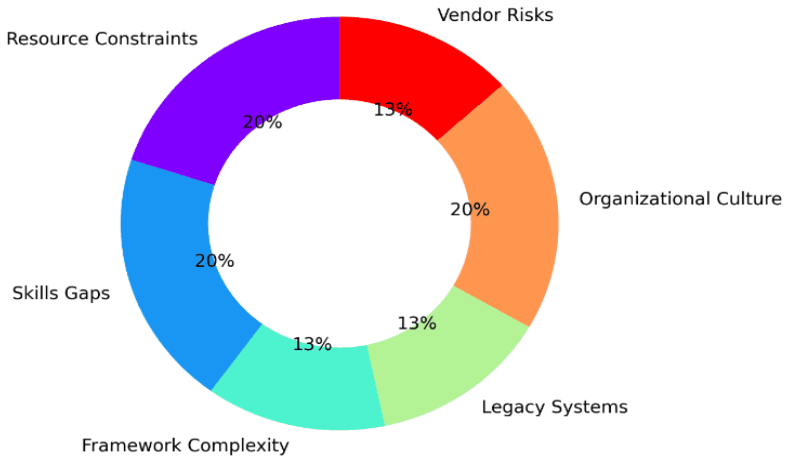

Figure 7. Implementation Challenges categories reported by the studies.

The challenges associated with implementing GRC frameworks are shown in Figure 7 below. The most common challenges mentioned are resource limitations, skill limitations, and cultural barriers, each appearing in three papers (n = 3; 15%). Other challenges, such as complex frameworks, existing systems, and vendor challenges, are also mentioned but less frequently (n = 2; 10%). The complexity of regulations is another challenge mentioned in some studies. It can be concluded that both organizational and technical aspects affect the implementation of GRC frameworks. These challenges are not evenly distributed across organizational contexts, and the reviewed studies suggest why. Resource and skills limitations are reported almost exclusively by studies set in single-site or resource-constrained settings [7], [29], [23], [31], where compliance and monitoring activity competes directly with clinical operating budgets; the same challenges are largely absent from studies of large international or multi-national contexts [30], [2], where dedicated governance staff are more often already in place. Cultural barriers and organizational culture challenges, by contrast, are concentrated in studies describing AI or automation-related governance [4], [28], [1], suggesting that resistance arises less from the technical demands of GRC frameworks themselves than from the organizational change AI introduces to existing roles and decision rights. Legacy-system challenges are

reported specifically in studies involving cloud- or IoT-based infrastructure [18], [23], indicating that this barrier is a property of the technology environment rather than of the chosen GRC framework. This pattern implies that the same framework can succeed in one organizational context and stall in another for reasons that have little to do with the framework's own design, which is consistent with the framework-versus-context distinction noted earlier in relation to Figure 7.

Governance mechanisms for integrating cybersecurity into organizational processes
Figure 8 shows how cybersecurity governance is integrated into organizational processes.

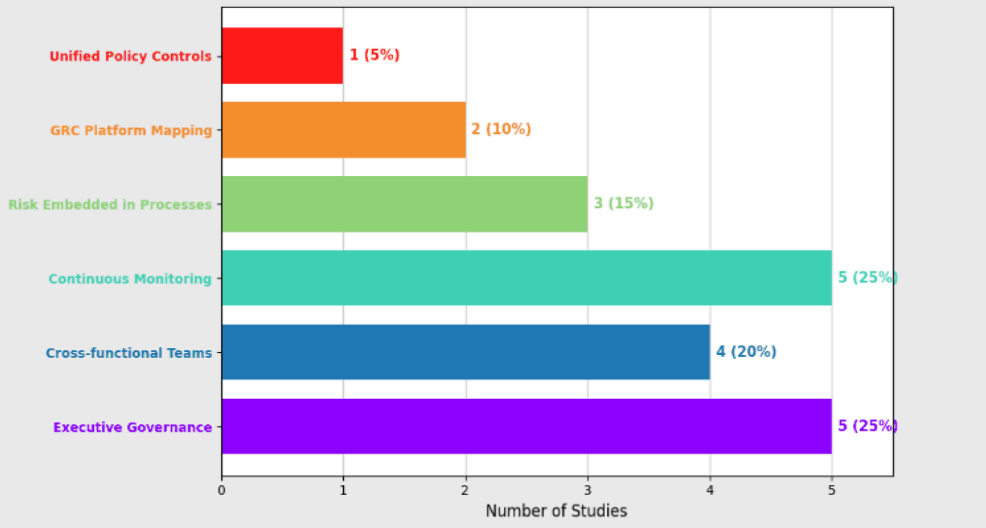

Figure 8. Frequency of integration mechanisms.

Figure 8 highlights the role of cybersecurity governance within organization's process. The most common types of integration include cross-functional cybersecurity governance and risk management processes, both of which are observed in four papers (n = 4; 20%). Other types of integration include continuous monitoring and risk assessment, identified in three papers (n = 3; 15%), as well as integrated GRC and strategic cybersecurity governance approaches, also found in three papers (n = 3; 15%). Less common types of integration include compliance enforcement, incident response integration, and zero trust models, all of which are noted in one paper (n = 1; 5%).

Best Practice Governance Models in Healthcare Cybersecurity
Figure 9 shows the best practice governance approaches identified across the selected studies.

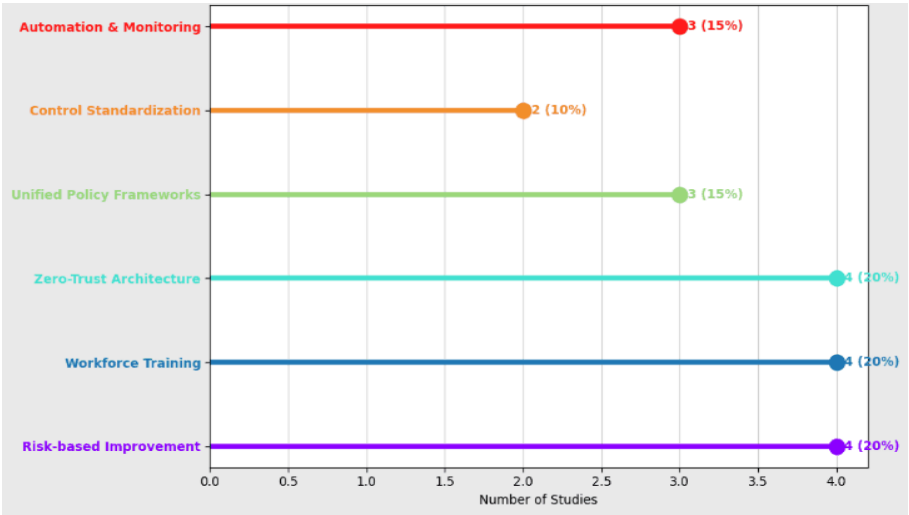

Figure 9. Best-practice recommendations

Figure 9 shows the governance practices found in the reviewed literature. Risk-based continuous improvement, workforce training, and zero-trust practices have been mentioned most often (n = 4; 20%). Unified policies and automation are mentioned three times each (n = 3, 15%), while standardization through framework mapping has been mentioned twice (n = 2, 10%). It can be concluded that efficient governance relies mostly on continuous improvement, readiness, and new security practices.

DISCUSSION

This section interprets the study's findings in relation to the research questions and situates them within the broader context of healthcare cybersecurity governance.

RQ1: GRC Frameworks Applied in Healthcare Cybersecurity

The findings clearly show the trend toward greater integration and adaptability of cyber-governance practices, which are influenced by digital transformation [4], [19]. Even though traditional frameworks like ISO 27001, HIPAA, and the NIST Cybersecurity Framework are still used in healthcare [7], [21], [17], [30]. The focus shifts to methodologies that can address the issues related to the introduction of new technologies. AI, cloud computing, and IoMT technologies change the existing paradigms of governance in healthcare settings [27], [19],[24], [5]. Therefore, AI governance frameworks are becoming more common, which is explained by increasing attention paid to the issue of accountability, transparency, and ethical considerations associated with the implementation of AI solutions [24],[5],[25], [2],[5], [1]. Nevertheless, the findings also demonstrate that the majority of organizations lack the required readiness for implementing AI governance frameworks due to insufficient skills and a lack of clarity regarding regulations [22], [28]. The need for governance frameworks for cloud computing and IoMT becomes apparent because of the necessity to manage distributed and interlinked systems [19], [24], [25]. However, certain barriers to the successful application of such frameworks are also identified, including complexity, interoperability issues, and reliance on third-party suppliers [19], [24], [25]. Despite the fact that traditional frameworks serve as a basis for standardization and ensure compliance with regulations [21], [30], their usefulness appears to be rather limited in the context of digital transformation [21], [30]. The rigidity of ISO 27001 and NIST frameworks is considered one of their drawbacks, which may make them unsuitable for use in rapidly changing healthcare environments [7], [21], [30]. Enterprise-oriented frameworks, such as COBIT and combined IT GRC frameworks, can play an important role in relation to the integration of cybersecurity strategies in terms of an enterprise's risk management policies [29], [23]. However, these models can be too complex and expensive for healthcare organizations with insufficient resources to implement. In conclusion, the findings suggest a trend toward the development of integrated cybersecurity governance models within healthcare organizations.

RQ2: Advantages of GRC Frameworks in Healthcare Cybersecurity

From the above findings, several specific advantages emerge from using GRC frameworks as part of efforts to improve cybersecurity governance in the healthcare industry. While GRC frameworks are not just for compliance, they can be used as part of an organized process of managing cyber risks [4], [27], [29],[1]. The first major advantage is the increased maturity of the governance process, since GRC frameworks define roles and governance processes [27], [29], [23], [1]. The above defines the increased alignment of cybersecurity activities with organizational goals, thereby making cybersecurity a joint effort. At the same time, the scale of these benefits depends on a number of factors, including leadership support and organizational readiness [4], [23]. Another way in which GRC frameworks contribute to enhanced cybersecurity posture concerns risk management and monitoring [14], [30], [24], [26]. The latter is especially critical in the healthcare sector, where it impacts patient safety [14], [24], [26]. Another benefit of GRC frameworks is compliance. Frameworks such as ISO 27001 and HIPAA help maintain necessary documentation and policies and ensure compliance with data protection rules [21], [30], [31]. Even though it promotes accountability, compliance-focused efforts may result in checklists that are not always beneficial from the point of view of cybersecurity [30], [31].

GRC frameworks also allow for better risk identification and prioritization, making it easier for organizations to use their limited resources wisely and address the biggest threats [7], [17],[25]. As a result, cybersecurity becomes more proactive and risk focused. Overall, the analysis of findings suggests that GRC frameworks offer more benefits than compliance alone. Their success mostly depends on proper implementation.

RQ3: Implementation Challenges in Healthcare GRC Adoption

Based on the information above, it could be argued that the use of GRC models in healthcare organizations faces several difficulties. Even though the use of GRC models allows obtaining well-established techniques of cyber governance, the implementation of the mentioned models often poses certain challenges related to organization, technologies, and regulation [4], [21], [23], [31]. Firstly, resource shortages are a major obstacle to implementing GRC models. Quite often, due to various reasons, healthcare organizations lack sufficient resources for successful implementation, including financial, human, and temporal resources [4], [21], [23], [31]. As a result, governance models are sometimes implemented only nominally, without the resources needed to produce real change [4]. Another problem concerns the lack of necessary skills. According to research data, healthcare organizations face a shortage of competencies in AI governance, risk assessment, and cloud technologies. Thus, healthcare organizations find it challenging to manage IT infrastructures [27], [29], [19], [26]. Organizational issues also tend to contribute to the problem. It appears that cybersecurity governance in most cases is handled by technical experts without involving organizational stakeholders [4], [15], [2]. Low levels of leadership involvement and awareness are likely to exacerbate the situation [4],[2]. Moreover, healthcare organizations must address a variety of overlapping standards and regulations, which creates additional barriers [21], [30], [31]. Instead of focusing on risks, organizations may be forced to concentrate on compliance, which can lead to inefficient practices. Various technical issues also represent a challenge for implementing GRC models [19], [24], [25]. For instance, the reliance on legacy IT systems and vendor solutions limits opportunities to introduce innovations. In summary, based on the presented findings, the main challenge associated with GRC implementation is not a lack of tools but a lack of implementation.

RQ4: Integration of Cybersecurity into Enterprise Governance

The findings show that healthcare organizations start regarding cybersecurity as an important component of enterprise governance, as opposed to a purely technical problem [4], [21], [15], [24], [31]. It is driven by the increasing use of digital technologies such as artificial intelligence, cloud computing, and medical devices, which require better coordination across organizational processes. The primary means of integration into enterprise governance is executives' active participation in the process. Including cybersecurity in the strategic planning helps organizations to better align their security needs with the overall goals and risk management processes [4], [21], [15], [31]. At the same time, the effectiveness of this strategy is possible only under the condition that the leadership is familiar enough with cybersecurity issues [24]. Monitoring and reporting are other methods of integrating cybersecurity into enterprise governance. They provide organizations with information about vulnerabilities and threats in real-time, thus allowing for more flexible governance processes [14], [2], [26]. However, implementing these processes requires the necessary technical infrastructure and skills. Another significant factor in integrating cybersecurity into enterprise governance is cross-functional collaboration. In some cases, it can contribute to solving the problem of organizational silos and improve organizational processes [27], [29], [19], [1]. As a result, cybersecurity issues will not be limited to technical departments. The integration of cybersecurity into the processes of procurement and system development can be helpful, as it allows moving away from purely regulatory activities and toward risk management [7], [17], [25]. Using unified GRC platforms can also facilitate this process through increased visibility and reduced redundancy [21], [23].

Thus, based on the above findings, one may conclude that the most efficient way to integrate cybersecurity into enterprise governance includes the various aspects discussed.

RQ5: Best Practice Governance Models in Healthcare Cybersecurity

It becomes clear that, for successful cybersecurity governance, flexible, holistic models are needed rather than compliance-based approaches. The review shows that the best practice always includes the elements of adaptability, organization readiness, and the capability to respond to changes [4], [29], [22], [26].

Continuous, risk-based improvement is a widely discussed practice. It is necessary to be able to change governance activities in view of changes in the technology and cybersecurity landscape [4], [29], [22], [26]. One more significant practice is workforce development. Collaboration of training and awareness programs, along with management involvement, can help to improve governance [17], [28], [2], [1]. At the same time, its implementation needs some effort. Zero-trust architecture is the best practice because of its flexibility and efficiency [32]. Zero-trust models are effective because they incorporate verification and access control policies highly relevant to the healthcare industry. Lastly, the use of a unified governance

framework is another critical practice that helps to overcome fragmentation in cybersecurity governance processes [5]. At the same time, such an approach can require many resources. To conclude, all these practices should be combined to achieve success in governance.

Synthesis Gaps and the Need for an Integrated Governance Framework

Another significant issue identified in the literature review is the fragmentation of the healthcare cybersecurity governance field, as researchers discuss frameworks independently and pay little attention to interoperability. The frameworks reviewed in most papers are ISO 27001, NIST, AI governance, and cybersecurity frameworks for cloud-based security solutions, which rarely work effectively. One of the problems with existing governance frameworks is insufficient integration with operational processes. GRC frameworks help improve governance maturity and compliance, but their implementation may prove ineffective if organizations lack the resources to do so. It should be noted that the analysis of the papers shows that while cybersecurity is a crucial component of modern organizations' infrastructure, it is not necessarily incorporated into corporate governance. There are still healthcare providers who perceive cybersecurity as a purely technical problem, without understanding the potential risks and dangers. Given the emergence of new technologies, healthcare cybersecurity is evolving rapidly, making it increasingly difficult to detect emerging risks and address cybersecurity challenges with traditional tools. For example, frameworks that use emerging technologies such as AI, IoT, and cloud computing may not provide sufficient cybersecurity due to their limited applicability and rigidity. Consequently, all the issues discussed above require the development of an integrated governance model.

Proposed Integrated Healthcare Cybersecurity Governance Ecosystem Framework

Figure 10 shows the proposed integrated governance model for cybersecurity in healthcare based on the results of the current review. According to this framework, cybersecurity governance can be viewed as a system shaped by the interplay among regulatory factors, organizational procedures, GRC frameworks, and digital health technologies. Unlike traditional views of cybersecurity, in which governance, compliance, and security measures are treated separately, this framework integrates them.

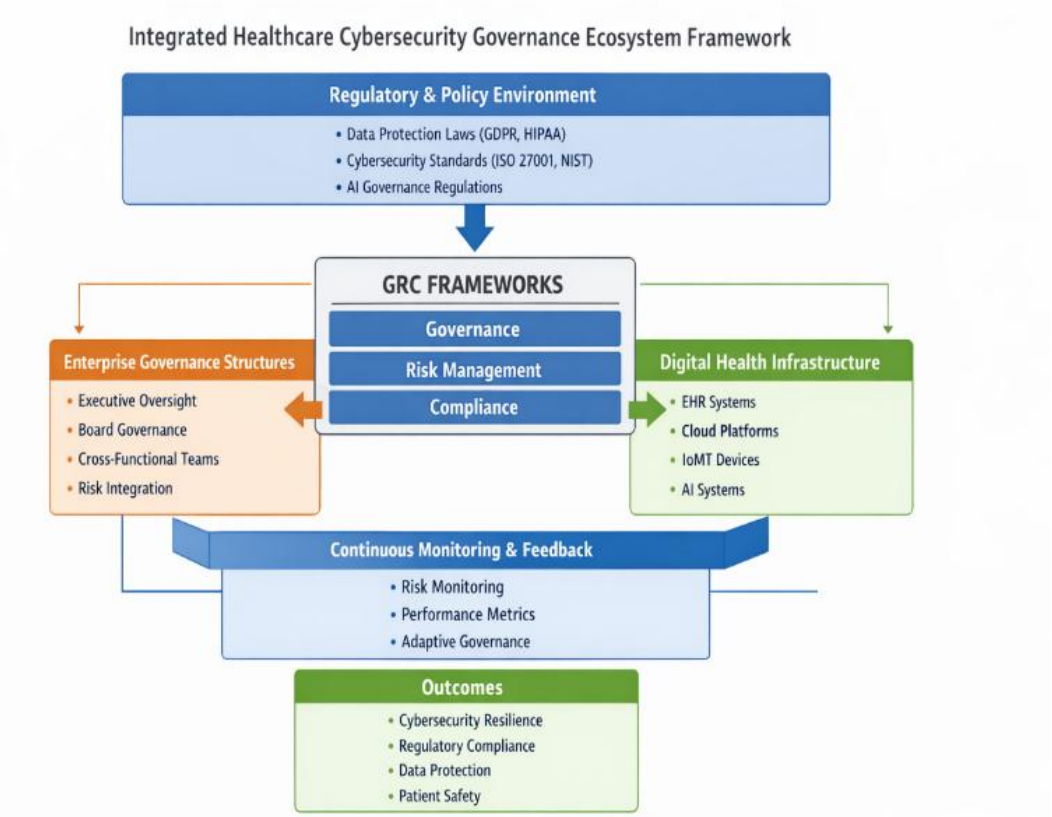

Figure 10. Integrated cybersecurity governance framework for digital healthcare systems

The novelty of this framework relative to existing models lies in what it combines rather than in any single component. ISO 27001 and the NIST Cybersecurity Framework each provide rigorous control catalogs for

information security, but treat regulatory, organizational, and technological governance as implicit background rather than as explicit, interacting layers of the model itself. COBIT offers strong IT governance and management structures but was not designed around the specific regulatory environment of healthcare (e.g., HIPAA, GDPR) or the operational realities of connected medical devices and AI-based clinical systems. HIPAA, in turn, defines compliance obligations but offers no structural guidance on how those obligations should be governed alongside risk management or technology adoption. The frameworks identified in this review's included studies (Table 4) each strengthen one of these layers, for example, blockchain governance for data integrity [14], cloud governance for infrastructure [19], or AI governance maturity models for emerging technologies [2], but none positions all four layers (regulatory and policy environment, enterprise governance structures, digital health infrastructure, and continuous monitoring and feedback) as explicitly interacting components within a single model. The framework proposed here addresses this gap by making those interactions the organizing structure of the model itself, rather than treating any one layer as primary and the others as supporting detail.

At the outer level, the framework recognizes the importance of regulatory and policy considerations, including regulations on cybersecurity, data privacy, and AI. Such regulations influence the organization's priorities and cybersecurity program management. This is why GRC frameworks are created and implemented in the organization as the point of coordination for the proposed model. These frameworks include ISO 27001, NIST, HIPAA, COBIT, and the AI Governance Framework, helping to translate regulatory considerations into governance processes. The other key point of the framework is the difference between organizational and technological governance processes. The organizational ones include structures such as executive oversight, the board of directors' responsibilities, enterprise risk management, and coordination, which support strategic decision-making. The technological ones include cloud computing, EHRs, IoMT, and AI, which are important tools in business operations but also pose potential cybersecurity risks. Another characteristic feature of the proposed framework is the ability to provide continuous monitoring and feedback to identify new risks and process changes. In turn, the consideration of continuous monitoring and feedback represents a transition from static, compliance-based cybersecurity governance to a risk-based process. When combined, these processes affect important outcomes, including cybersecurity resilience, regulatory compliance, continuity, data protection, and patient safety. In addition, the framework accounts for some of the practical barriers discussed in the literature review, including resource constraints, a lack of skilled personnel, regulatory complexity, governance fragmentation, and legacy technology. Each of these obstacles could adversely affect the implementation of governance processes at the organizational level. It should be noted that although the proposed framework is described as a multi-layered structure, it constitutes a holistic system in which each element continually influences the others.

IMPLICATIONS

Practical Implications

The above results imply a shift from cybersecurity-centered governance methods to holistic approaches in healthcare organizations. The holistic approach needs to take into consideration involvement at the highest level through management and the board, along with cooperation between departments, to mainstream cybersecurity in healthcare governance. With the adoption of innovations such as artificial intelligence and cloud computing in modern healthcare organizations, there is a need for governance that ensures data integrity and monitoring.

Theoretical Implications

Based on the above discussion, it is evident that a shift away from purely technical cybersecurity governance toward holistic governance becomes necessary in healthcare organizations. Holistic governance requires the involvement of top management, the board of directors, and other departmental members in cybersecurity within healthcare governance. This requirement arises from the use of new technologies, such as artificial intelligence and cloud computing, in modern healthcare systems, which extend cybersecurity risk beyond the IT department and into clinical and administrative operations.

Policy Implications

The above findings highlight the need for cooperation in cybersecurity governance within the healthcare industry. The policies may be inconsistent at times, which makes it difficult for organizations to maintain a coherent approach while implementing the policies. It is necessary for policymakers to ensure that such policies are consistent and aligned across data protection, cybersecurity, and even AI governance. There

should also be efforts made to foster capacity development within the organizations. This will ensure the successful implementation of policies through proper cybersecurity governance practices.

LIMITATIONS

There are several limitations of this study, which need to be noted. First, only specific English-language databases and articles were used for the analysis. It may lead to the exclusion of relevant studies and negatively impact the representativeness of findings. Second, the study was conducted as a qualitative analysis of existing literature, not as an empirical study. Thus, the conclusions made concern the practice described in the literature but not implemented. Also, one needs to pay attention to the differences in research methodologies and contexts among the chosen papers. It can complicate the analysis and comparison process. Finally, the applicability of suggested frameworks will depend on the specifics of the healthcare system, including its level of digitalization, legislative support, and available resources.

FUTURE WORKS

Several directions for future research follow from this study. One priority is an empirical investigation into the impact of GRC models on the operations of healthcare organizations, demonstrating their impact and scalability across different settings. Another area for further research is the effect of organizational governance maturity on an organization's ability to build cybersecurity resilience under resource constraints. Future research will also need to focus on governing new technologies such as AI.

CONCLUSION

The purpose of this research paper was to analyze the role of GRC framework models in implementing cybersecurity governance in healthcare organizations. The research found a shift from control-based frameworks to cybersecurity governance frameworks that align with risk management strategies, regulatory requirements, and new technological solutions. Though existing frameworks such as ISO 27001 and NIST remain relevant, the growing popularity of AI and cloud computing may bring changes in this area. A further finding of this study is that success factors for cybersecurity governance are related to the integration process at the organizational, technological, and regulatory levels. Among them, executive sponsorship, the maturity level of cybersecurity governance, and continuous monitoring were highlighted, while skill set limitations, lack of budget, and outdated technology were identified as potential obstacles. Therefore, the present paper summarizes the existing literature on GRC frameworks in the context of cybersecurity governance in healthcare organizations.

REFERENCES

[1] O. Ismail and N. Ahmad, "Ethical and Governance Frameworks for Artificial Intelligence: A Systematic Literature Review," *Int. J. Interact. Mob. Technol.*, vol. 19, no. 14, pp. 121–136, Jul. 2025, doi: 10.3991/ijim.v19i14.56981.

[2] R. Hussein *et al.*, "Advancing Healthcare AI Governance: A Comprehensive Maturity Model Based on Systematic Review," *medRxiv*, p. 2024.12.30.24319785, Dec. 2024, doi: 10.1101/2024.12.30.24319785.

[3] C. Mhlanga and B. Ndlovu, "Sentiment Analysis in Electronic Health Records for Patient-Centric Care : A Systematic Literature Review of Methods , Applications , and Challenges," vol. 8, no. 2, pp. 1740–1775, 2026, doi: 10.63158/journalisi.v8i2.1554.

[4] R. Octavia, S. Tinggi Ilmu Ekonomi Widya Praja Tanah Grogot, P. Profesi Bidan, S. Tinggi Ilmu Kesehatan Salsabila Serang, and C. Author, "Strategic Management Approaches to Healthcare System Resilience: A Systematic Review Post-Pandemic Era," *Brill. Int. J. Manag. Tour.* , vol. 6, no. 1, pp. 169–174, Feb. 2026, doi: 10.55606/bijmt.v6i1.6761.

[5] A. Wang, S. Freeman, and F. Magrabi, "Governance for safe and responsible AI in healthcare organisations: A scoping review of frameworks," Aug. 2025, doi: 10.21203/rs.3.rs-7209096/v1.

[6] B. M. Ndlovu, B. Chipangura, and S. Singh, "Factors Influencing Quantified SelfTechnology Adoption in Monitoring Diabetes," in *Lecture Notes in Networks and Systems*, 2024, vol. 1014 LNNS, pp. 469–479, doi: 10.1007/978-981-97-3562-4_37.

[7] E. D. Khoza, A. Ludonga, and M. S. Singo, "Cyber Risk Management: Frameworks, Strategies, and Case Studies in Cybersecurity," doi: 10.5281/ZENODO.17581327.

[8] O. Tomashchuk, "Threat and Risk Management Framework for eHealth IoT Applications," *ACM Int. Conf. Proceeding Ser.*, vol. Part F164402-B, pp. 120–126, Oct. 2020, doi: 10.1145/3382026.3431250.

[9] F. M. Dandure and B. Ndlovu, “Federated Learning for Privacy-Preserving Sentiment Analysis in Distributed Electronic Health Record Environments : A Systematic Literature Review,” vol. 8, no. 2, pp. 1812–1842, 2026, doi: 10.63158/journalisi.v8i2.1546.
[10] A. Maramba and B. Ndlovu, “AI-Driven Threat and Incident Detection in Healthcare Cybersecurity : A Stacked Ensemble Model,” *2025 4th Zimbabwe Conf. Inf. Commun. Technol.*, no. November, pp. 1–9, 2025, doi: 10.1109/ZCICT67553.2025.11602039.
[11] V. A. Muderere, B. Ndlovu, and K. Maguraushe, “Blockchain Adoption in Healthcare : Enhancing Interoperability , Security and Data Exchange,” *J. Inf. Syst. Informatics*, vol. 7, no. 3, pp. 2939–2977, 2025, doi: 10.51519/journalisi.v7i3.1267.
[12] M. Moyo and B. Ndlovu, “Towards Cloud-Based Electronic Health Records in Healthcare Systems : Security , Scalability , and Migration Strategies : A Systematic Literature Review,” vol. 8, no. 1, pp. 739–780, 2026, doi: 10.63158/journalisi.v8i1.1431.
[13] R. Sibanda, B. Ndlovu, S. Dube, and K. Maguraushe, “Towards Health 4 . 0 : Blockchain-Based Electronic Health Record for Care Coordination,” pp. 712–720, 2024, doi: 10.34190/ecie.19.1.2606.
[14] L. Xu, M. N. H. Ibrahim, M. M. Alobaedy, and S. B. Goyal, “Systematic Review of Scalable Blockchain-Based Digital Signature Frameworks for Healthcare Data Security,” *J. Comput. Mech. Manag.*, vol. 4, no. 6, pp. 16–29, Dec. 2025, doi: 10.57159/jcmm.4.6.25221.
[15] B. Ndemo, “Revolutionizing African Healthcare: A Systematic Review of Artificial Intelligence and Data Governance,” May 2025, doi: 10.21203/rs.3.rs-6572611/v1.
[16] K. Malm-Nicolaisen, G. Ellingsen, M. Hertzum, and G.-H. Severinsen, “Evolution of Information Infrastructures in Healthcare as Convergence of Digital Trajectories,” 123AD, doi: 10.1007/s10606-024-09502-0.
[17] S. Alla, S. G. Komaragiri, T. Duvall, S. Karahan, N. Bheesetty, and V. K. Chattu, “A Governance-Centric Framework for Strengthening Healthcare Cybersecurity: A Systems Perspective.”
[18] “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
[19] Q. Guan, M. N. H. Bin Ibrahim, M. M. Alobaedy, and S. B. Goyal, “A Systematic Review of Privacy-Aware Cloud Framework for Medical Secure E-Governance Data Processing,” *Journal of Computers, Mechanical and Management*, vol. 5, no. 1. AAN Publishing, pp. 76–92, Feb. 2026, doi: 10.57159/jcmm.5.1.25222.
[20] V. A. Muderere, B. Ndlovu, and K. Maguraushe, “Framework for Enhancing Interoperability, Data Exchange, and Security in Healthcare through Blockchain Technology,” *Indones. J. Comput. Sci.*, vol. 14, no. 4, 2025, doi: 10.33022/ijcs.v14i4.4950.
[21] F. S. A. Alqahtani, A. A. Belal, and N. I. Zakri, “Impact of Governance, Risk Management and Compliance on Healthcare System: A Systematic Review,” *J. Contemp. Dent. Pract.*, vol. 26, no. 9, pp. 904–911, Jan. 2025, doi: 10.5005/jp-journals-10024-3943.
[22] A. A. Bello and J. Reneau, “Literature Review of Artificial Intelligence Security Governance Frameworks: Risk Management Strategies for Regulated Industries Including Healthcare, Financial Services, and Gaming,” *World J. Adv. Res. Rev.*, vol. 18, no. 2, pp. 1503–1522, May 2023, doi: 10.30574/wjarr.2023.18.2.0833.
[23] S. Putri Samsul and M. Muchran, “IT GRC Maturity on Organizational Performance and Financial Reporting Quality: A Systematic Review,” 2025.
[24] “Risk Management Frameworks for Healthcare IoT: Moving Beyond Traditional Perimeter-Based Security.”
[25] B. Reddy Bhavanam, “Security Challenges In Healthcare Cloud Apis: A Systematic Review.”
[26] S. M. Alvarez and K. A. Boateng, “Threat Intelligence-Driven Risk Management Frameworks for Securing Healthcare Cloud Systems.”
[27] C. Prakash, M. Lind, and A. Sisodia, “Agentic AI Governance and Lifecycle Management in Healthcare,” Jan. 2026.
[28] T. Tosin Adewale *et al.*, “Balancing Human Oversight and AI Automation in Governance, Risk, and Compliance (GRC) Practices for IT Program Delivery in High-Threat Environments,” 2025.
[29] F. Alharbi, M. A. Nour Sabra, N. Alharbe, and A. A. Almajed, “Towards a Strategic IT GRC Framework for Healthcare Organizations Clinical Review Department King Fahad Medical City Riyadh, Saudi Arabia.”
[30] A. Ahmed, A. Shahzad, A. Naseem, S. Ali, and I. Ahmad, “Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative

analysis of ISO standards, GDPR, and HIPAA in blockchain technology," *PLoS One*, vol. 20, no. 5 May, May 2025, doi: 10.1371/journal.pone.0324285.
[31] F. M. Dias, M. L. Martens, S. F. de P. Monken, L. F. da Silva, and E. D. R. Santibanez-Gonzalez, "Risk management focusing on the best practices of data security systems for healthcare," *Int. J. Innov.*, vol. 9, no. 1, pp. 45–78, Apr. 2021, doi: 10.5585/iji.v9i1.18246.
[32] A. Dube, B. Mpande, F. Dzehonye, and T. Chazuza, "Zero Trust Architecture : Redefining Security," pp. 26–39, 2026, doi: 10.1007/978-3-032-20533-9.