Sarcouncil Journal of Multidisciplinary

ISSN(Online): 2945-3445

Volume- 06| Issue- 05| 2026

Review Article **Received:** 01-04-2026 | **Accepted:** 25-04-2026 | **Published:** 10-05-2026

Governance, Risk, and Compliance (GRC) Engineering Approaches for IT and Cybersecurity Control Assurance: A Critical Review

William Asare Yirenkyi

Temple University - Fox School of Business, Philadelphia, PA

Abstract: In the United States (U.S.), where escalating cyber threats such as ransomware and supply chain attacks increasingly imperil national security and economic stability, Governance, Risk, and Compliance (GRC) engineering has emerged as a critical mechanism for Information Technology (IT) and cybersecurity control assurance. This critical literature review examines peer-reviewed academic studies, standards-informed research, and authoritative professional literature from 2020 to 2025, confined to U.S. regulatory contexts. Employing a critical review methodology, it inductively surfaces themes from recurring patterns, contrasts, and tensions across sources, viewed through lenses of functional integration, risk alignment, control effectiveness, auditability, and scalability in regulated environments. This involves thematic coding to derive patterns, evaluative comparison to assess strengths and weaknesses, and contradiction mapping to identify inconsistencies and gaps. The analysis reveals a dominant emphasis on hybridizing frameworks such as National Institute of Standards and Technology (NIST) and Control Objectives for Information and Related Technology (COBIT) to unify governance and risk functions, alongside risk-based control design and automation for monitoring and predictive analytics. While these approaches demonstrably bolster enterprise risk management and sectoral resilience particularly in finance and healthcare, they simultaneously expose persistent weaknesses. This can be in the form of limited adaptability, insufficient cultural integration, scalability constraints for smaller entities, and unresolved contradictions in AI adoption amid fragmented regulations like SOX, HIPAA, and CCPA. Empirical validation remains thin, and behavioral dimensions are largely overlooked. These findings carry significant implications for assurance quality, regulatory accountability, and institutional resilience. The review illuminates how current GRC engineering supports risk-based auditing yet falls short in addressing the full complexity of U.S. regulated environments, thereby clarifying both its contributions and its enduring limitations.

Keywords: GRC Engineering, Cybersecurity Control Assurance, Risk-Based IT Auditing, NIST COBIT Integration, Cybersecurity Governance United States.

INTRODUCTION

In the United States, the escalating complexity of digital ecosystems has amplified the national significance of Governance, Risk, and Compliance (GRC) engineering as a cornerstone for ensuring robust IT and cybersecurity control assurance. As organizations grapple with pervasive cyber threats, such as ransomware and supply chain attacks, GRC engineering emerges as a vital mechanism to integrate governance oversight, risk management strategies, and compliance adherence into cohesive systems that safeguard critical infrastructure and economic stability. According to Quinn *et al*. (2025), the integration of cybersecurity risks into enterprise risk management (ERM) frameworks is essential for addressing uncertainties that could undermine national security and business objectives. This is particularly pertinent in the U.S. Regulatory landscapes there include the Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), and National Institute of Standards and Technology (NIST) guidelines. These demand rigorous control assurance to mitigate financial, reputational, and operational harms.

The rationale for a U.S.-focused review stems from the country's unique regulatory environment, characterized by federal mandates, state-specific laws like the California Consumer Privacy Act (CCPA), and sector-specific requirements that influence GRC engineering practices. For instance, financial institutions must align with Dodd-Frank and Gramm-Leach-Bliley Acts, while healthcare entities adhere to HIPAA, creating a fragmented yet stringent compliance ecosystem (Proudfoot *et al*., 2024). This fragmentation necessitates GRC approaches that are adaptable to U.S. regulatory dynamics, emphasizing risk-based auditing and control effectiveness in high-stakes sectors like finance, healthcare, and critical infrastructure. Recent incidents, such as the 2021 Colonial Pipeline ransomware attack, underscore the national imperatives for enhanced GRC engineering to bolster institutional resilience and prevent cascading economic disruptions.

The purpose of this critical literature review is to synthesize peer-reviewed and authoritative sources from 2020 to the present, evaluating GRC engineering approaches for IT and cybersecurity control assurance within U.S. contexts. By adopting a critical lens, the review moves beyond descriptive summaries to interrogate assumptions, strengths, limitations, and gaps in existing

***Corresponding Author:** William Asare Yirenkyi

DOI- https://doi.org/10.5281/zenodo.20113026

literature. The scope is delimited to U.S.-relevant studies, incorporating standards like NIST Cybersecurity Framework (CSF) and COBIT, while excluding pre-2020 works to capture post-pandemic evolutions in cyber threats and regulations. This focus contributes to scholarship by deriving inductive themes from literature, highlighting inconsistencies in GRC integration and offering insights for improved assurance practices.

GRC engineering, as conceptualized in recent studies, involves the architectural design and functional implementation of systems that unify governance policies, risk assessments, and compliance mechanisms. Maleh *et al*. (2021) emphasize that effective GRC frameworks guide standards adoption to enhance information security governance, aligning with U.S. priorities for auditability and resilience. However, challenges persist, such as siloed functions that hinder holistic risk management (Plant *et al*., 2022). In the U.S., cyber incidents cost billions annually, GRC engineering must prioritize scalability to accommodate diverse organizational sizes, from small enterprises to multinational corporations under federal oversight.

Moreover, the evolution of AI in GRC introduces transformative potential but also new risks. Studies indicate that AI-powered tools enable predictive analytics and automated compliance monitoring, yet they raise concerns over algorithmic bias and integration with legacy systems (Faruq, 2025). This review critically examines these developments, revealing tensions between innovation and regulatory assurance. For example, (Alfaadhel *et al*., 2023) propose risk-based compliance assessments that leverage AI for dynamic evaluations, but limitations in data privacy compliance under U.S. laws like CCPA highlight unresolved gaps.

The contribution of this review lies in its inductive synthesis, identifying literature-derived themes such as framework integration and audit effectiveness, while applying analytical lenses to evaluate practical relevance in U.S. regulated environments. Varying emphases on cultural factors in cybersecurity governance (Alshaikh, 2020), for example, are addressed to advance understanding of how GRC engineering can enhance control assurance without prescribing new models. Ultimately, this work informs stakeholders on navigating U.S. regulatory complexities to foster resilient IT and cybersecurity postures.

METHODOLOGICAL APPROACH TO THE CRITICAL REVIEW

The Methodological Approach outlines the process for conducting the literature review, beginning with a literature identification strategy, followed by inclusion and exclusion criteria, then the analytical approach and justification for the critical review methodology.

Literature Identification Strategy

Targeted searches on academic databases like Google Scholar, IEEE Xplore, and ACM Digital Library using keywords such as "GRC engineering," "IT auditing," "cybersecurity governance," and "control assurance" combined with "United States" and date filters from 2020 onward initially identified 58 sources. Duplicates were removed and title/abstract screening applied for U.S. relevance and critical depth, followed by full-text assessment using the inclusion and exclusion criteria, which highlighted peer-reviewed and standards-informed sources with direct applicability to U.S. regulatory environments; this process yielded exactly 25 retained sources. Authoritative sources, including NIST publications and GSA guidelines, were prioritized via government websites. This strategy was supplemented by snowballing from reference lists in key reviews (e.g., Zwilling, 2022). Emphasis was placed on peer-reviewed journals, conference proceedings, and standards-informed reports to ensure relevance to U.S. contexts, capturing evolutions post-COVID-19 in cyber threats and regulations. The exact temporal cutoff was December 2025, with exactly 25 sources retained after application of inclusion and exclusion criteria.

Inclusion and Exclusion Criteria

Inclusion criteria required sources to be peer-reviewed academic studies, standards-informed research, or authoritative professional literature published from 2020 through to 2025, with conceptual relevance to GRC engineering and analytical contributions to IT/cybersecurity control assurance in U.S. regulatory environments. Sources addressing integration, alignment, or auditability were included if they offered critical insights, such as NIST IR 8286r1 (Quinn *et al*., 2025). Exclusion criteria eliminated pre-2020 works, non-U.S.-focused studies without applicability (e.g., solely European GDPR-centric), vendor-specific promotions, or descriptive summaries lacking critique. This ensured a focused corpus of exactly 25 sources

Publisher: SARC Publisher

emphasizing U.S. regulations like HIPAA and SOX.

Analytical Approach and Justification for the Critical Review Methodology

The analytical approach employed a critical review methodology, organizing sources around inductive themes derived from patterns, contrasts, and perspectives rather than sequential summaries. This involved iterative coding for pattern identification, conceptual clustering to group related ideas, and tension mapping to surface contradictions. Lenses such as functional integration and scalability guided evaluation of assumptions, strengths, and gaps. Justification lies in its suitability for synthesizing conceptual contributions over volume, enabling interrogation of inconsistencies like framework silos (Melaku, 2023). Unlike systematic reviews, this method prioritizes depth and critique, ideal for identifying tensions in U.S. GRC practices amid evolving threats, as supported by Proudfoot *et al*. (2024). The synthesis aim was non-exhaustive, focusing on conceptual relevance rather than exhaustive coverage.

CONCEPTUAL FOUNDATIONS OF GRC ENGINEERING

The Conceptual Foundations of GRC Engineering section establishes the theoretical underpinnings by defining GRC and its evolution, exploring interrelationships between GRC systems, IT controls, cybersecurity governance, and auditing, and synthesizing a textual conceptual framework that interconnects governance, risk, compliance, IT controls, and cybersecurity assurance, grounded in the literature to highlight bidirectional relationships and analytical insights into misalignments.

Definitions and Evolution of GRC and GRC Engineering

GRC engineering has evolved from fragmented risk management to integrated systems engineering for unified governance, risk, and compliance functions. Recent literature reflects a shift toward adaptive platforms incorporating automation and analytics. As an example, Maleh *et al*. (2021) define GRC as a structured methodology encompassing guides, standards, and frameworks for IT governance and information security, evolving to address post-2020 cyber threats like remote work vulnerabilities. This evolution primarily organizational and regulatory with technological elements incorporates NIST standards, emphasizing engineering for scalability amid regulatory changes (Quinn *et al*., 2025); this contrasts with pre-2020 static governance focused on compliance checklists versus post-2020 cloud-native, dynamic approaches (NIST, 2024). The literature highlights a progression to dynamic engineering that embeds risk intelligence. This is driven by increasing cyber incidents and the need for resilient control assurance.

Relationship Between GRC Systems, IT Controls, Cybersecurity Governance, and Auditing

Literature consistently portrays GRC systems as intermediaries linking IT controls with cybersecurity governance and auditing processes, critiquing silos that undermine holistic assurance. Auditing validates control effectiveness through evidence-based assessments. Davis (2021) illustrates this interplay by advocating controls-based auditing for cyber security governance, ensuring alignment with risk objectives. This relationship is evident in HIPAA-compliant healthcare systems, where GRC integrates controls for data integrity and audit trails (Yusif & Hafeez-Baig, 2021). Studies reveal tensions, such as auditing gaps in DevOps environments, where rapid deployments challenge traditional governance (Plant *et al*., 2022). In summary, the synthesis underscores GRC's role in harmonizing these elements for assurance.

Literature-Derived Textual Conceptual Framework

Drawing from reviewed sources, a conceptual framework emerges depicting GRC engineering as an interconnected ecosystem where governance establishes policies and roles, risk management identifies and prioritizes threats, and compliance operationalizes controls for assurance. Relationships are bidirectional: governance informs risk appetite, influencing compliance thresholds, while feedback from auditing refines IT controls. Quinn *et al*. (2025) ground this in ERM integration, where cybersecurity risks feed into enterprise profiles via risk registers. Similarly, (Gordon *et al*., 2020) highlight cost-benefit linkages between controls and assurance objectives. Interconnections manifest through NIST CSF alignment, ensuring auditability (Alfaadhel *et al*., 2023). This framework synthesizes variations, acknowledging operational uncertainties in interconnections that remain partially unresolved (Faruq, 2025). It serves as an analytical tool, revealing how misalignments lead to assurance gaps.

Publisher: SARC Publisher

SYNTHESIS OF GRC ENGINEERING APPROACHES

The Synthesis of GRC Engineering Approaches section presents inductively derived themes from the literature, including integration of standards and frameworks, risk-based assurance, AI and automation, and auditability, while offering a comparative synthesis across analytical dimensions such as governance integration, risk alignment, compliance operationalization, control assurance, and auditability, supported by an analytical table that contrasts these elements across themes.

Integration of Standards and Frameworks in GRC Engineering

Literature reveals a recurring pattern of integrating standards like NIST CSF, COBIT, and ISO 27001 into GRC engineering for unified architectures, critiquing inconsistencies in adaptability across frameworks. Quinn *et al*. (2025) describe risk registers as tools for aggregating cybersecurity risks into ERM, enhancing governance integration. Alignment with compliance objectives appears as seen in GSA's RMF implementation (GSA, 2024). Contrasts emerge in adaptability: while NIST supports scalability, COBIT emphasizes audit controls (Maleh *et al*., 2021). This synthesis highlights converging views on framework hybridization for control assurance, though debates persist on implementation in regulated sectors.

NIST RMF adopts a governance orientation centered on risk-based authorization for federal systems, with a control philosophy emphasizing continuous monitoring and authorization boundaries, locating accountability primarily at the system owner and authorizing official levels. In contrast, COBIT emphasizes enterprise-wide IT governance orientation, with a control philosophy rooted in process maturity and alignment with business objectives, placing accountability at the board and executive management locus. Assurance implications differ markedly: NIST RMF supports rigorous federal audit trails through POA&M tracking and continuous monitoring, while COBIT facilitates broader enterprise auditability through control objectives and maturity assessments. These differences create interoperability tensions in hybrid GRC architectures, where NIST's operational focus may conflict with COBIT's strategic emphasis, limiting seamless integration (Bittencourt, 2024).

Risk-Based Assurance and Control Design

A prominent theme is the emphasis on risk-based approaches for designing IT and cybersecurity controls, prioritizing exposure calculations and residual risk assessments, yet critiquing divergences in methodological rigor. Gordon *et al*. (2020) advocate cost-benefit analyses within NIST frameworks to align controls with assurance goals. Healthcare modeling under HIPAA requirements draws from studies such as Yusif and Hafeez-Baig (2021). Divergences appear in methodological rigor: qualitative vs. quantitative analyses (Alfaadhel *et al*., 2023). Overall, the literature converges on adaptive control design for operating effectiveness, with patterns in vulnerability scanning and POA&M tracking.

AI and Automation in GRC Systems

Emerging from post-2023 sources, integration represents a functional dimension, automating compliance monitoring and predictive risk analytics. Faruq (2025) meta-analyzes framework in GRC platforms for audit efficiency in enterprises. Approaches include NLP for regulatory parsing and ML for anomaly detection (Akinsulire & Ohakawa, 2024). Ethical tensions appear in some studies warning of bias in automated assurance. The analysis underscores converging perspectives on integration enhancing scalability, particularly in critical environments, while acknowledging variations in adoption maturity.

Auditability and Evidence Generation

Auditability emerges as a core theme, with GRC engineering focusing on evidence trails and continuous monitoring for assurance. Davis (2021) outlines controls-based auditing, generating artifacts like SARs and POA&Ms. Internal audit strategies under SOX appear in financial sectors (Vuko *et al*., 2025). Patterns include three lines of defense models (Héroux & Fortin, 2025), contrasting with gaps in cultural integration (Alshaikh, 2020). The synthesis reveals debate on evidence automation, converging on its role in regulatory accountability.

The table below contrasts GRC approaches, illustrating how standards enable governance while AI enhances risk alignment, interpreted as facilitating adaptive assurance in U.S. contexts despite tensions in scalability.

Publisher: SARC Publisher

Table 1: Comparative Analysis of GRC Engineering Approaches Across Analytical Dimensions

Theme	Governance Integration	Risk Alignment	Compliance Operationalization	IT/Cybersecurity Control Assurance	Auditability
Standards and Frameworks	Unified via NIST/COBIT (Quinn *et al*., 2025)	Exposure prioritization (Gordon *et al*., 2020)	Tailored baselines (GSA, 2024)	Resilience mechanisms (Yusif & Hafeez-Baig, 2021)	Common controls catalog (Maleh *et al*., 2021)
Risk-Based Assurance	Policy oversight (Plant *et al*., 2022)	Likelihood-impact matrices (Alfaadhel *et al*., 2023)	Regulatory mapping (Proudfoot *et al*., 2024)	Vulnerability remediation (Backman & Stevens, 2024)	POA&M tracking (Davis, 2021)
AI and Automation	Ethical committees (Faruq, 2025)	Predictive scoring (Akinsulire & Ohakawa, 2024)	Not Evident in Reviewed Literature	Anomaly detection (Zwilling, 2022)	Automated trails (Handri *et al*., 2024)
Auditability	Roles and responsibilities (Héroux & Fortin, 2025)	Residual risk assessment (Vuko *et al*., 2025)	Continuous monitoring (Antunes *et al*., 2022)	Three lines of defense (Hossain *et al*., 2024)	SAR generation (Domínguez-Dorado *et al*., 2023)

CRITICAL EVALUATION OF EXISTING APPROACHES

This section assesses the strengths (conceptual and empirical), limitations, inconsistencies, and gaps in GRC engineering methods, supported by literature citations and an evaluative table that summarizes these aspects across categories like framework integration, risk-based assurance, AI and automation, and auditability, emphasizing practical relevance and unresolved tensions in U.S. contexts.

Strengths Supported by the Literature

Existing GRC engineering approaches demonstrate robust strengths in fostering integrated risk management and compliance alignment, particularly through standardized frameworks. Conceptual strengths lie in their architectural coherence, enabling unified governance integration across disparate functions, as NIST RMF and COBIT provide theoretical contributions by framing risk as an enterprise-wide concern rather than isolated technical issues, creating a robust theoretical foundation for interconnected assurance (Bittencourt, 2024). Empirical strengths are evident in demonstrated performance improvements and measurable audit enhancements, with studies showing automation in GRC platforms improves response times to threats and resilience in high-stakes sectors (Faruq, 2025; Bittencourt, 2024), while continuous monitoring patterns mitigate regulatory penalties through POA&M tracking and three lines of defense models enhance audit efficiency in healthcare under HIPAA (Héroux & Fortin, 2025). These strengths are grounded in post-2020 case studies demonstrating improved institutional resilience, though scalability for SMEs remains a limitation.

Limitations, Inconsistencies, and Contradictions

Among the limitations are ad hoc aggregation methods in risk registers, leading to underestimation of cascading risks (Quinn *et al*., 2025). As Alshaikh (2020) notes, inconsistencies arise in framework application: while NIST emphasizes scalability, COBIT's audit focus may overlook cultural elements. Contradictions appear in AI adoption, where predictive benefits conflict with bias risks, as noted in healthcare contexts (Yusif & Hafeez-Baig, 2021). Tensions involve fragmented regulations, with SOX compliance clashing with agile DevOps (Plant *et al*., 2022). These issues reveal practical irrelevance in resource-constrained environments. Debates on

Publisher: SARC Publisher

qualitative vs. quantitative analyses exacerbate inconsistencies (Gordon *et al*., 2020).

Gaps and Unresolved Tensions

Gaps and unresolved tensions in the literature center on three interconnected challenges that undermine the practical effectiveness of GRC engineering. Interoperability challenges arise when integrating NIST RMF and COBIT in hybrid architectures, creating data exchange barriers and inconsistent control mappings that result in fragmented assurance reporting and increased compliance overhead (Bittencourt, 2024). Data governance maturity constraints further limit effectiveness by hindering consistent data classification and quality assurance across IT controls, with many organizations operating at low levels that undermine cybersecurity control assurance and exacerbate interoperability issues (Sprinto, 2024). Finally, federal vs. state-level compliance fragmentation creates structural tensions where NIST RMF federal mandates clash with state-specific laws like CCPA, leading to duplicated controls, increased compliance costs, and inconsistent assurance practices that constrain scalability and institutional resilience (Winston & Strawn, 2025). These gaps collectively highlight the persistent structural limitations that current GRC engineering approaches have yet to fully resolve.

Table 2. Evaluative Summary of GRC Engineering Approaches

Category	Strengths	Limitations	Gaps
Framework Integration	Holistic ERM alignment (Quinn *et al*., 2025)	Siloed applications (Plant *et al*., 2022)	Limited SME focus (Zwilling, 2022)
Risk-Based Assurance	Predictive mitigation (Gordon *et al*., 2020)	Estimation biases (Alfaadhel *et al*., 2023)	Empirical validation shortages (Yusif & Hafeez-Baig, 2021)
AI and Automation	Efficiency in monitoring (Faruq, 2025)	Algorithmic bias (Akinsulire & Ohakawa, 2024)	Not evident in reviewed literature
Auditability	Evidence Generation (Davis, 2021)	Inconsistencies in methods (Vuko *et al*., 2025)	Cultural integration tensions (Alshaikh, 2020)

IMPLICATIONS FOR IT AUDITING AND CYBERSECURITY GOVERNANCE

This section explores the broader ramifications of GRC engineering on assurance quality, regulatory oversight, and cyber risk governance, discussing how literature-derived insights influence assurance precision, accountability mechanisms, and institutional resilience, while acknowledging persistent challenges.Aside that, this evaluation reveals significant implications for IT auditing and cybersecurity governance for CIOs, internal auditors, regulators, and policy makers.For Chief Information Officers, hybrid NIST RMF and COBIT integration exposes trade-offs in risk reporting and constrains technology investment prioritization amid unresolved interoperability tensions. For internal auditors, the shift toward continuous monitoring creates evidence of reliability challenges and requires recalibration of auditability models in automated environments. For regulators and oversight bodies, regulatory language versus operational assurance capability gaps constrains evaluation frameworks and cross-regulatory harmonization. For policymakers, federal-state compliance fragmentation limits alignment between national cybersecurity objectives and enterprise GRC maturity, exposing systemic risks to institutional resilience. These implications collectively highlight how current GRC engineering practices create structural, governance, and accountability consequences that demand continued scholarly attention.

Implications for Assurance Quality

GRC engineering implications for assurance quality in IT auditing involve enhanced evidence generation through automated tools, improving detection of control deficiencies. Davis (2021) indicates that controls-based approaches elevate audit precision in cyber governance. Yet gaps in cultural integration may compromise quality (Alshaikh, 2020). HIPAA-aligned GRC raises assurance by addressing data integrity, yet unresolved biases pose risks (Yusif & Hafeez-Baig, 2021). In essence, implications suggest bolstered resilience but necessitate refined methodologies for consistent quality.

Publisher: SARC Publisher

Regulatory Oversight and Accountability

Implications for regulatory oversight include streamlined accountability via risk registers, facilitating compliance with mandates like SOX and CCPA. Quinn *et al*. (2025) show ERM integration aids federal reporting, enhancing transparency. Tensions in framework silos may hinder accountability (Plant *et al*., 2022). In financial sectors, GRC supports Dodd-Frank oversight. Inconsistencies in audit effectiveness challenge enforcement (Vuko *et al*., 2025). These implications highlight potential for institutional accountability while underscoring needs for adaptive oversight.

Cyber Risk Governance and Institutional Resilience

Implications for cyber risk governance emphasize proactive resilience in critical environments through predictive analytics. Faruq (2025) notes AI in GRC platforms strengthens institutional defenses against threats. Reflecting on these, limitations in scalability for SMEs reveal vulnerabilities (Zwilling, 2022). Literature implies enhanced resilience via three lines of defense, yet cultural gaps persist (Héroux & Fortin, 2025). Overall, implications point to fortified governance but call for resolving tensions.

DIRECTIONS FOR FUTURE RESEARCH

Empirical gaps include limited longitudinal studies on AI integration in GRC, particularly in U.S. SMEs where scalability issues remain underexplored. Conceptual gaps involve underdeveloped models for cultural influences on control assurance, overlooking behavioral dynamics in risk governance. Methodological opportunities lie in mixed-methods approaches combining quantitative risk metrics with qualitative audits to address inconsistencies in framework applications. Future research could investigate adaptive GRC in emerging threats like quantum computing, emphasizing interdisciplinary collaborations for holistic insights.

CONCLUSION

The critical insights from this review synthesize the evolving landscape of GRC engineering, revealing strengths in framework integration and automation while exposing limitations in scalability and cultural alignment. These findings contribute to IT auditing by highlighting the need for adaptive risk-based approaches that enhance control assurance amid U.S. regulatory complexities. For cybersecurity governance, the review underscores the imperative of holistic ERM to foster resilience against dynamic threats. In sum, the work advances GRC scholarship by surfacing themes that clarify both the promise and the persistent challenges of current approaches, while underscoring the need for continued critical scrutiny in evolving regulatory landscapes.

REFERENCES

1. Akinsulire, A. A., & Ohakawa, T. C. "Enhancing Cybersecurity Governance in Financial Institutions: A Quantitative Study on Control Deficiencies and Regulatory Compliance (2024)." (2024).
2. Alfaadhel, A., Almomani, I., & Ahmed, M. "Risk-based cybersecurity compliance assessment system (RC2AS)." *Applied Sciences* 13.10 (2023): 6145.
3. Alshaikh, M. "Developing cybersecurity culture to influence employee behavior: A practice perspective." *Computers & Security* 98 (2020): 102003.
4. Antunes, M., Maximiano, M., & Gomes, R. "A client-centered information security and cybersecurity auditing framework." *Applied Sciences* 12.9 (2022): 4102.
5. Backman, S., & Stevens, T. "Cyber risk logics and their implications for cybersecurity." *International Affairs* 100.6 (2024): 2441-2460.
6. Bittencourt, D. “Differences between COBIT, ISO 27001 and NIST.” (2024).
7. Davis, R. E. “Auditing information and cyber security governance: A controls-based approach.” CRC Press, (2021).
8. Domínguez-Dorado, M., Cortes-Polo, D., Carmona-Murillo, J., Rodríguez-Pérez, F. J., & Galeano-Brajones, J. "Fast, lightweight, and efficient cybersecurity optimization for tactical–operational management." *Applied Sciences* 13.10 (2023): 6327.
9. Faruq, M. O. "A meta-analysis of cybersecurity framework integration in GRC platforms: Evidence from US enterprise audits." *Journal of Sustainable Development and Policy* 1.01 (2025): 224-249.
10. Gordon, L. A., Loeb, M. P., & Zhou, L. "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model." *Journal of Cybersecurity* 6.1 (2020): tyaa005.
11. GSA. “Managing enterprise cybersecurity risk CIO-IT Security-06-30.” General Services Administration. (2024).
12. Handri, E. Y., Sensuse, D. I., & Tarigan, A. "Developing an agile cybersecurity framework

Publisher: SARC Publisher

with organizational culture approach using Q methodology." *IEEE Access* 12 (2024): 108835-108850.
13. Héroux, S., & Fortin, A. "How the three lines of defense can contribute to public firms' cybersecurity effectiveness." *International Journal of Disclosure and Governance* 22.2 (2025): 377-396.
14. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. "Understanding local government cybersecurity policy: A concept map and framework." *Information* 15.6 (2024): 342.
15. Maleh, Y., Sahid, A., Alazab, M., & Belaissaoui, M. "IT governance and information security: Guides, standards, and frameworks." CRC Press, (2021).
16. Melaku, H. M. "A dynamic and adaptive cybersecurity governance framework." *Journal of Cybersecurity and Privacy* 3.3 (2023): 327-350.
17. NIST. "The NIST Cybersecurit) 2.0." National Institute of Standards and Technology. (2024).
18. NIST.IR.8286r1Sprinto. "8 Data Governance Challenges That Can Derail Your Business Success." (2024).
19. Plant, O. H., van Hillegersberg, J., & Aldea, A. "Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment." *International journal of accounting information systems* 45 (2022): 100560.
20. Proudfoot, J. G., Cram, W. A., & Madnick, S. "Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations." *European Journal of Information Systems* 34.3 (2025): 436-459.
21. Quinn, S. D., Ivy, N., Barrett, M., Witte, G. A., & Gardner, R. K. "Integrating cybersecurity and enterprise risk management (ERM) (NIST IR 8286r1)." National Institute of Standards and Technology. (2025).
22. Vuko, T., Slapničar, S., Čular, M., & Drašček, M. "Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective." *International journal of auditing* 29.1 (2025): 188-206.
23. Winston & Strawn. "Navigating the Maze: A Comparison of Selected Federal Cybersecurity Regulations." (2025).
24. Yusif, S., & Hafeez-Baig, A. "A conceptual model for cybersecurity governance." *Journal of applied security research* 16.4 (2021): 490-513.
25. Zwilling, M. "Trends and challenges regarding cyber risk mitigation by CISOs—A systematic literature and experts' opinion review based on text analytics." *Sustainability* 14.3 (2022): 1311.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Yirenkyi, W. A. "Governance, Risk, and Compliance (GRC) Engineering Approaches for IT and Cybersecurity Control Assurance: A Critical Review" *Sarcouncil Journal of Multidisciplinary* 6.5 (2026): pp 1-8.

Publisher: SARC Publisher