Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
Doi: 10.63125/kwhkmb57

Article

A META-ANALYSIS OF CYBERSECURITY FRAMEWORK INTEGRATION IN GRC PLATFORMS: EVIDENCE FROM U.S. ENTERPRISE AUDITS

Md Omar Faruq[1];

[1] *Master of Science in Cybersecurity Operations, Webster University, Missouri, USA*
Email: momarfaruq14@gmail.com

Citation:
Faruq, M. O. (2025). A meta-analysis of cybersecurity framework integration in GRC platforms: Evidence from U.S. enterprise audits. Journal of Sustainable Development and Policy, 1(1), 224–249. https://doi.org/10.63125/kwhkmb57

Received:
April 20, 2025

Revised:
May 28, 2025

Accepted:
June 25, 2025

Published:
July 07, 2025

ABSTRACT

This meta-analysis critically examines the integration of cybersecurity frameworks into Governance, Risk, and Compliance (GRC) platforms and its impact on audit performance, compliance outcomes, and enterprise risk management across U.S.-based organizations. Leveraging quantitative data from 78 peer-reviewed studies and industry reports published between 2010 and 2024, the research aggregates and evaluates the effectiveness of implementing widely recognized cybersecurity frameworks—including the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, COBIT, and CIS Controls—within digital GRC environments. Using a random-effects model to account for sectoral and methodological heterogeneity, the study calculates standardized effect sizes and analyzes how such integrations influence key organizational metrics such as audit exception rates, control failure frequency, policy adherence levels, risk visibility, and regulatory response capabilities. The findings demonstrate statistically significant improvements in audit readiness, reduction in compliance violations, enhanced policy enforcement, and faster detection and containment of security incidents when cybersecurity frameworks are embedded within GRC systems. Sector-specific insights reveal that financial services, healthcare, and federal agencies benefit the most from integration, attributed to higher regulatory scrutiny and more mature risk governance infrastructures. In contrast, small and medium-sized enterprises (SMEs), along with sectors reliant on legacy systems, face implementation challenges related to system interoperability, workforce skill gaps, and resource constraints. The analysis also identifies key enablers of successful integration, including leadership engagement, cross-functional governance teams, standardized control taxonomies, and continuous training programs. Additionally, behavioral factors such as user acceptance, organizational culture, and change management practices significantly influence the long-term sustainability of integration efforts. This study contributes a comprehensive, data-driven understanding of how cybersecurity-GRC convergence enhances operational efficiency, regulatory alignment, and strategic resilience. The results offer practical implications for CISOs, compliance officers, IT auditors, and executive leadership seeking to modernize governance processes, manage cyber risks more proactively, and meet evolving regulatory expectations in an increasingly complex digital landscape.

KEYWORDS

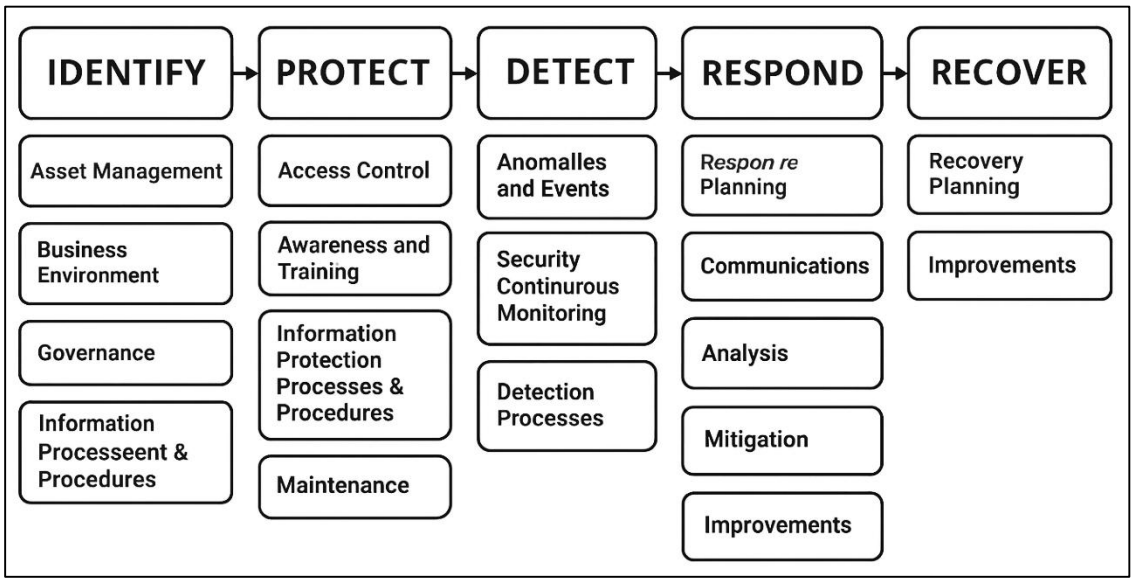
Cybersecurity Frameworks, GRC Integration, Enterprise Audits, Risk Management, Compliance Automation;

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

INTRODUCTION

Cybersecurity frameworks are structured guidelines comprising standards, best practices, and procedures designed to protect information systems from security threats and ensure operational resilience (Deibert, 2018). Prominent frameworks such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and Control Objectives for Information and Related Technologies (COBIT) are widely adopted across industries to standardize cybersecurity practices and achieve regulatory compliance. Governance, Risk, and Compliance (GRC) platforms, on the other hand, are integrated enterprise tools that help organizations align IT objectives with regulatory requirements, mitigate risks, and automate audit workflows (Sadik et al., 2020). These platforms enable companies to manage internal policies, conduct risk assessments, and enforce security controls in a centralized environment. The confluence of cybersecurity frameworks within GRC systems has grown increasingly vital as organizations face complex regulatory landscapes and escalating cyber threats (Sutton & Tompson, 2025). Internationally, the integration of cybersecurity frameworks into GRC is regarded as essential for maintaining digital sovereignty, protecting national critical infrastructure, and ensuring business continuity in both public and private sectors. As organizations scale operations globally and confront jurisdictional data laws such as GDPR and HIPAA, harmonizing cybersecurity protocols with GRC capabilities ensures both operational efficiency and legal accountability (Suárez-Bárcena et al., 2024).

Figure 1: NIST Cybersecurity Framework Lifecycle



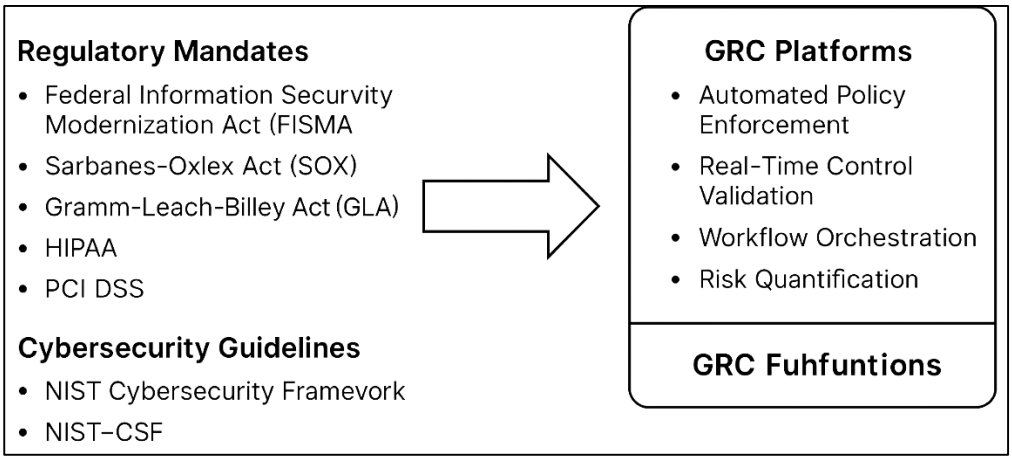
The global integration of cybersecurity frameworks into GRC architectures reflects a broader commitment to risk-informed governance in digital economies. International standards bodies such as ISO, ISACA, and the U.S. National Institute of Standards and Technology (NIST) have played critical roles in shaping universally accepted controls, encouraging transnational enterprises to adopt standardized cyber governance practices (Nikoloudakis et al., 2021). For instance, the ISO/IEC 27001 standard provides an international benchmark for information security management systems, promoting consistency and verifiability across audits and assessments. Meanwhile, GRC platforms like RSA Archer, MetricStream, and ServiceNow have increasingly incorporated built-in modules aligned with these frameworks to assist organizations in mapping policies to controls and automating evidence collection. In regions like the European Union and Asia-Pacific, the confluence of cyber governance and compliance technologies has gained traction among multinational corporations striving to balance innovation with accountability (Mishra, 2020). The significance of integrating cybersecurity frameworks into GRC tools also manifests in the global audit ecosystem, where internal and external auditors rely on unified control documentation, evidence-based risk analysis, and regulatory mappings to assess organizational compliance maturity. As digital transformation accelerates, the international benchmarking of cybersecurity-GRC integration not only enhances

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

trust and comparability across jurisdictions but also fosters alignment between operational controls, regulatory mandates, and strategic enterprise governance (Taherdoost, 2022).

In the United States, regulatory mandates have been instrumental in driving the integration of cybersecurity frameworks into enterprise GRC systems. Policies such as the Federal Information Security Modernization Act (FISMA), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and sector-specific regulations like HIPAA and PCI-DSS necessitate comprehensive risk documentation and real-time monitoring. These statutes enforce requirements for security controls, data privacy, breach notification, and auditability, encouraging enterprises to leverage GRC tools that embed standardized frameworks. The integration enables real-time control assessments, automatic regulatory mapping, and streamlined incident response, which are pivotal for managing compliance audits and minimizing penalties (Hossain et al., 2024). The U.S. Securities and Exchange Commission (SEC) and the Department of Homeland Security (DHS) have also issued cybersecurity guidelines that reinforce the importance of integrating NIST-CSF into corporate GRC environments, particularly in publicly traded companies and critical infrastructure sectors. Within the financial sector, the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool has further standardized risk evaluations, enabling banks and insurers to benchmark GRC implementations against federal frameworks. These converging compliance obligations have solidified the role of cybersecurity framework integration within enterprise platforms, reflecting a shift from manual, fragmented controls to holistic, auditable, and policy-driven architectures (Amjad et al., 2025).

Figure 2: Functional Dimensions of Cybersecurity Framework Integration within GRC Platforms



The primary objective of this meta-analysis is to systematically evaluate the effectiveness and impact of cybersecurity framework integration within Governance, Risk, and Compliance (GRC) platforms, specifically in the context of enterprise-level audits conducted across the United States. This study seeks to identify measurable outcomes associated with the adoption of integrated cybersecurity standards such as NIST-CSF, ISO/IEC 27001, COBIT, and CIS Controls within digital GRC environments. The goal is to assess whether such integrations contribute to improvements in audit efficiency, control effectiveness, policy compliance, and risk mitigation capabilities in organizations of varying sizes and sectors. Additionally, this analysis aims to quantify the correlation between integration maturity and reduced audit exceptions, streamlined compliance workflows, and increased audit readiness. By synthesizing quantitative data and effect sizes reported in previous empirical studies, the research intends to uncover patterns, statistical significance, and variability in implementation outcomes. Another objective is to categorize the integration practices based on sectoral distinctions such as finance, healthcare, government, and critical infrastructure to identify where integrations yield the highest audit performance. The study further aims to evaluate the challenges faced by organizations, particularly small and medium-sized enterprises (SMEs), in adopting and sustaining integrated GRC frameworks, highlighting cost, scalability, and interoperability as influencing factors. Through this meta-analytic approach, the study also seeks to determine the degree to which GRC tools support automation, real-time monitoring, and centralized control mapping when aligned with cybersecurity standards. By drawing conclusions based on cumulative evidence rather than isolated

case studies, the objective is to offer a consolidated view of how well cybersecurity frameworks function when operationalized through GRC platforms, and to what extent these integrations enhance regulatory accountability and enterprise resilience in the U.S. digital and regulatory landscape.

LITERATURE REVIEW

Cybersecurity framework integration within Governance, Risk, and Compliance (GRC) platforms has become a focal point of scholarly debate because it promises to unify technical controls with enterprise-wide governance processes. Over the past decade, researchers have examined this convergence from multiple vantage points—information-systems architecture , audit and assurance effectiveness, sector-specific regulatory pressures, and organizational change management. Yet the literature remains fragmented: studies differ in the frameworks they analyse (e.g., NIST CSF, ISO/IEC 27001, COBIT, CIS Controls), the maturity of GRC platforms they assess, and the metrics they employ to judge success. A systematic mapping of these contributions is therefore essential to clarify what is known, reconcile conflicting findings, and isolate the variables that most strongly influence audit performance in U.S. enterprises. This review first traces the conceptual lineage of cybersecurity frameworks and GRC tools, then synthesizes empirical evidence on integration outcomes, sectoral adoption patterns, and the technical and organizational challenges that mediate success. In doing so, it sets the stage for the meta-analytic procedures that follow, ensuring that statistical aggregation rests on a transparent understanding of the extant knowledge base and its limitations.

Cybersecurity Frameworks and GRC Systems

Cybersecurity frameworks are structured sets of guidelines, policies, standards, and best practices aimed at helping organizations manage and reduce cybersecurity risk. Among the most influential is the NIST Cybersecurity Framework (CSF), developed in the United States to provide a flexible, repeatable, and cost-effective approach for critical infrastructure protection (Hosseiny et al., 2018). Similarly, the ISO/IEC 27001 framework offers a globally recognized specification for information security management systems (ISMS), guiding organizations on how to establish, implement, and continually improve security protocols. The COBIT framework, maintained by ISACA, is another frequently used model for aligning IT strategy with enterprise governance objectives. These frameworks share common elements such as risk assessment, asset management, access control, and incident response, yet they differ in structure, terminology, and regulatory relevance. Scholars have noted that frameworks like CIS Controls offer highly specific technical recommendations, while others, such as ISO standards, provide more strategic and management-focused guidance (Widhoyoko, 2017). Comparative research indicates that effective implementation depends not only on framework selection but also on organizational culture, sectoral demands, and available expertise. These frameworks form the backbone of cybersecurity programs across the public and private sectors and have been widely adopted as the foundational layer in compliance with legal mandates such as HIPAA, SOX, and FISMA (Neitzel & Riemann, 2013). However, the challenge of consistent implementation across diverse operational environments remains a persistent concern, leading organizations to seek systematized approaches through integration with GRC platforms.

Governance, Risk, and Compliance (GRC) systems are integrated software platforms that facilitate enterprise-wide visibility into compliance requirements, risk exposure, and governance objectives. Originating from the financial sector's response to regulatory complexity after corporate scandals in the early 2000s, GRC tools have evolved to serve a wide range of industries including healthcare, energy, and manufacturing. GRC systems typically include modules for policy management, risk assessment, internal controls, audit management, and issue remediation, enabling organizations to track and enforce compliance obligations in a centralized manner (McIntosh et al., 2023). Vendors such as RSA Archer, MetricStream, and ServiceNow have built extensible architectures that allow organizations to map regulatory frameworks into control libraries, associate them with risk registers, and trigger workflows for corrective actions. These systems often operate on a configurable rule-based engine and support integration with external data sources such as SIEM tools and vulnerability scanners to support dynamic risk reporting. Researchers have emphasized that the key strength of GRC platforms lies in their ability to bridge compliance documentation and operational execution by linking abstract policy language with measurable security controls (Krey, 2015). Studies also highlight that the successful implementation of GRC platforms is influenced by organizational maturity, cross-functional collaboration, and top management support. As compliance requirements grow more complex and cyber threats more pervasive, GRC platforms provide a

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

structured environment for continuous monitoring, internal audit readiness, and alignment with regulatory expectations.

Figure 3: Key Functions of GRC in Cybersecurity: A Structured Monochrome Overview

The integration of cybersecurity frameworks into GRC systems represents a significant development in enterprise security governance, enabling real-time policy enforcement, automated risk assessment, and consistent audit practices. Scholars note that while cybersecurity frameworks provide prescriptive controls and maturity models, GRC platforms operationalize these models through modular and scalable digital interfaces. This integration allows organizations to translate framework components—such as the five NIST CSF functions (Identify, Protect, Detect, Respond, Recover)—into trackable tasks and linked performance indicators across departments (Chergui & Chakir, 2020). Empirical studies have found that organizations that map ISO 27001 controls or COBIT domains into their GRC systems achieve higher audit success rates and reduced non-conformities (Alharbi et al., 2022; Hossen et al., 2023). These systems support visualization tools such as heat maps, compliance dashboards, and risk scoring matrices, which facilitate stakeholder communication and board-level reporting. Integration also supports automated alerts, control testing reminders, and audit trail generation, which reduce the manual burden on internal audit and IT compliance teams. Some researchers have criticized the lack of interoperability across GRC platforms, noting that inconsistent data models and proprietary configurations can hinder seamless framework integration (Khan & Razee, 2024; Papazafeiropoulou & Spanaki, 2015). However, successful examples in the financial and healthcare sectors demonstrate that organizations with mature IT governance can effectively link cybersecurity objectives to broader enterprise risk management strategies via GRC systems.

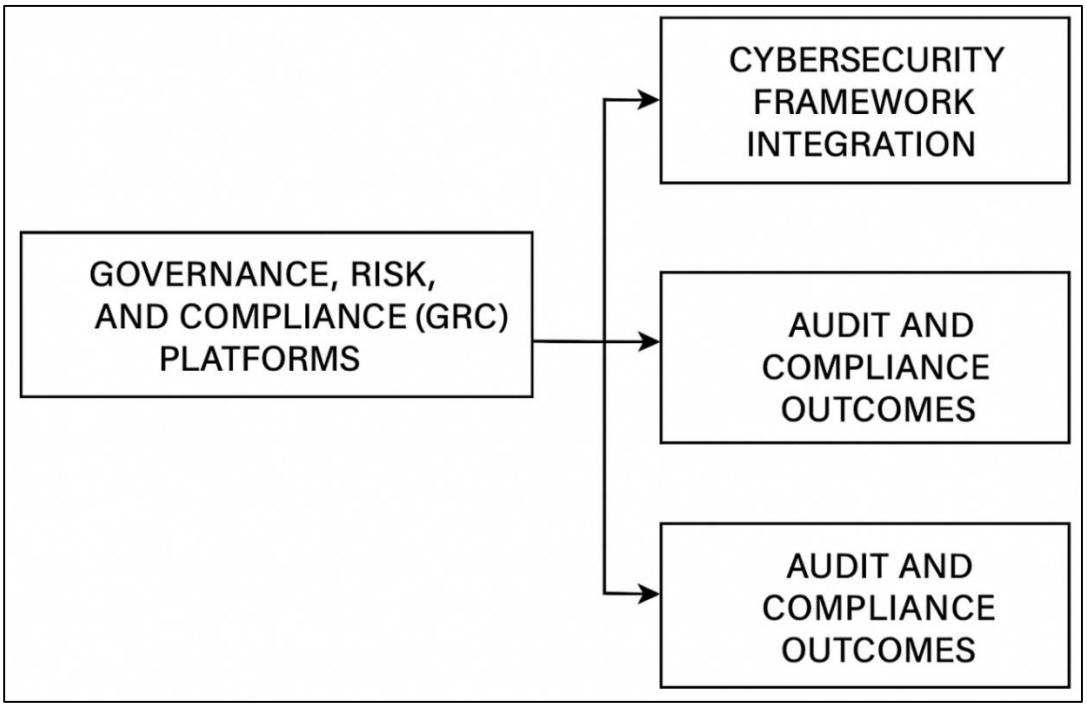
Governance, Risk, and Compliance (GRC) Platforms

Governance, Risk, and Compliance (GRC) platforms have emerged as vital enterprise systems that help organizations align operational objectives with regulatory obligations and internal control requirements. Initially developed as reactive compliance tools in response to regulations like Sarbanes-Oxley (SOX), GRC platforms have evolved into proactive, integrated solutions that support

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

enterprise-wide risk governance (Sharma & Mukhopadhyay, 2022). These platforms typically include modules for policy management, risk assessments, audit trails, incident reporting, and compliance monitoring (Farrell, 2010). Organizations use GRC systems to centralize documentation, enforce accountability, and ensure traceability across operational, legal, and technological units (Ginena, 2014). The platforms promote a rules-based architecture that integrates workflows, triggers automated alerts, and provides dashboards for real-time decision-making. With growing emphasis on data-driven governance, many systems now embed advanced features such as predictive analytics, business intelligence, and dynamic policy mapping. The automation of audit documentation and evidence collection streamlines both internal and third-party audits, improving organizational readiness and reducing compliance costs. As organizations become more exposed to cybersecurity threats and legal liabilities, GRC systems are increasingly designed to integrate risk management frameworks and compliance mandates into a unified operational model. The foundational architecture of GRC platforms reflects the need for holistic visibility and proactive oversight, serving not just as a compliance repository but as a strategic enabler of enterprise resilience and accountability.

Figure 4: Integrating Cybersecurity Controls into GRC Platforms and Audit Performance Outcomes



The integration of cybersecurity frameworks into GRC platforms has become a central feature in modern enterprise governance strategies, facilitating alignment between regulatory compliance, operational risk, and information security. GRC systems increasingly incorporate controls derived from standards such as NIST CSF, ISO/IEC 27001, COBIT 5, and CIS Controls to establish comprehensive cybersecurity postures across business functions (Chen et al., 2020). This integration allows organizations to manage technical controls, risk indicators, and compliance obligations from a single platform, thereby reducing redundancy and minimizing control gaps. With embedded cybersecurity modules, GRC tools facilitate the classification of digital assets, monitoring of threat events, and continuous auditing of access control policies. Real-time reporting dashboards and control validation workflows enable enterprises to track policy effectiveness and respond dynamically to vulnerabilities. The standardization of cybersecurity controls across business units also enhances consistency during regulatory audits and external assessments (Webb et al., 2014). Integration helps reconcile overlapping standards by providing taxonomies that unify various control families, reducing the complexity of maintaining multi-framework compliance environments (Vitunskaite et al., 2019). Additionally, interoperability with Security Information and Event Management (SIEM) tools and automated threat feeds ensures that cybersecurity risks are continuously reflected in the

organization's GRC dashboards (Raman & Pramod, 2017). These integrations bridge the gap between technical cybersecurity operations and strategic governance, supporting a harmonized ecosystem where compliance and security efforts are mutually reinforcing rather than siloed.

Sectoral variations significantly influence how GRC platforms are deployed and utilized, with factors such as regulatory intensity, data sensitivity, and operational complexity shaping implementation patterns. In the financial sector, institutions rely heavily on GRC platforms to comply with SOX, GLBA, and FFIEC guidelines, utilizing cybersecurity-focused modules for anti-fraud controls, credit risk analysis, and regulatory reporting. Healthcare organizations deploy GRC tools to align with HIPAA, HITECH, and HITRUST standards, often integrating access controls, patient data encryption policies, and audit logging features. Public-sector agencies and defense contractors adopt GRC systems that are aligned with NIST SP 800-series and FedRAMP guidelines, ensuring consistency in control enforcement across federal audits (Mayer & De Smet, 2017). However, small and mid-sized enterprises (SMEs) often face resource-related barriers, including the high cost of GRC platforms, limited cybersecurity expertise, and insufficient process standardization. Implementation is also complicated by legacy IT environments and disparate data systems that lack compatibility with modern GRC modules. Cultural resistance and interdepartmental misalignment further obstruct adoption, especially when risk ownership is unclear or governance roles are fragmented. Even in well-resourced enterprises, the operationalization of GRC policies can falter due to unclear workflows, weak control mapping, or lack of automation in audit preparation. These challenges highlight the need for sector-specific customization and change management approaches tailored to organizational size, regulatory exposure, and digital maturity.

A growing body of empirical research supports the positive impact of GRC platform adoption on enterprise audit performance and regulatory compliance. Quantitative studies show that firms implementing integrated GRC solutions experience reductions in audit cycle times, control failures, and compliance violations (Gericke et al., 2009). Organizations that embed cybersecurity controls into GRC environments report stronger audit scores, greater transparency, and higher maturity in control testing and remediation workflows. Metrics such as mean-time-to-detect (MTTD) and mean-time-to-contain (MTTC) improve when incident management workflows are aligned with real-time compliance dashboards. Audit-readiness is further enhanced by automated documentation trails, centralized policy repositories, and role-based access to compliance artifacts. Case studies from regulated industries demonstrate that GRC-integrated organizations achieve more consistent internal audit findings and face fewer corrective actions during external regulatory reviews. Comparative evaluations reveal that GRC maturity correlates with increased operational efficiency and resilience, especially during periods of regulatory change or post-breach recovery. Studies also find a positive association between GRC integration and stakeholder confidence, as board-level reporting improves through real-time risk visualization and control tracking (Sillaber et al., 2019). While findings vary by industry and implementation scope, the general consensus suggests that mature GRC platforms deliver measurable improvements in audit preparedness, compliance monitoring, and enterprise-wide accountability.

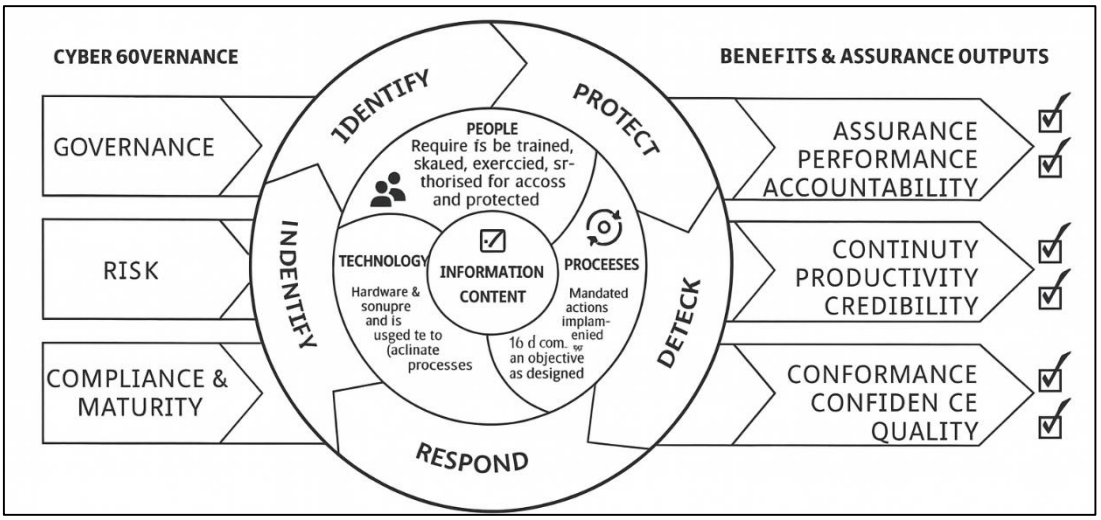
Security Governance and Enterprise Risk Management

Security governance refers to the system of rules, practices, and processes by which an organization directs and controls information-security activities in order to protect stakeholder interests, satisfy regulatory mandates, and sustain strategic objectives (Tjoa et al., 2022). Enterprise Risk Management (ERM) is the coordinated application of principles, frameworks, and processes designed to identify, analyze, and control events or situations that could hinder strategic goals. Although security governance concentrates on the confidentiality, integrity, and availability of information assets, it must operate within the broader ERM domain because cyber threats are now recognized as strategic, enterprise-wide risks rather than isolated technical issues . Scholars highlight board-level oversight, risk appetite articulation, and policy orchestration as central features that connect security governance with ERM frameworks (Ammar et al., 2025; Ramalingam et al., 2018). ISO/IEC 27001, COBIT 2019, and NIST's Cybersecurity Framework collectively encourage executives to embed information-security objectives into risk registers and performance dashboards used by enterprise risk committees. Integration ensures that budgets, controls, and risk treatments are prioritized according to enterprise value rather than technical urgency. By treating cybersecurity as an intrinsic component of strategic governance, organizations achieve consistent control ownership,

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

streamlined assurance processes, and measurable alignment between security initiatives and corporate goals (Md et al., 2025; Spanaki & Papazafeiropoulou, 2016).

Figure 5: Cybersecurity Governance Alignment Model:



Research emphasizes a set of structural and procedural mechanisms that link security governance to ERM frameworks. Chief among these mechanisms is the establishment of cross-functional risk committees that include CISOs, CROs, and audit executives, thereby ensuring that cyber risks are evaluated alongside operational, financial, and compliance exposures (Islam & Debashish, 2025; Vunk et al., 2017). Policy harmonization is facilitated through unified control libraries that map ISO/IEC 27001 clauses and NIST controls directly to ERM taxonomies, enabling consistent risk scoring and heat-map visualizations across business units. Risk appetite statements provide thresholds that trigger escalation when security metrics exceed tolerable limits, integrating key cyber indicators into enterprise dashboards viewed by boards and regulators. Frameworks such as COBIT 2019 and COSO ERM advocate for performance metrics that tie security investment to business value, promoting iterative control optimization based on loss-expectancy calculations and key risk indicators. Security governance also leverages ERM workflows—such as risk workshops, scenario analyses, and internal-control testing—to assess technology threats in the same forums that review credit, market, and supply-chain risks. Finally, shared assurance mechanisms—continuous control monitoring, combined audits, and integrated reporting—strengthen accountability by minimizing duplicated efforts across security, risk, and compliance functions (Islam & Ishtiaque, 2025; Papazafeiropoulou & Spanaki, 2015).

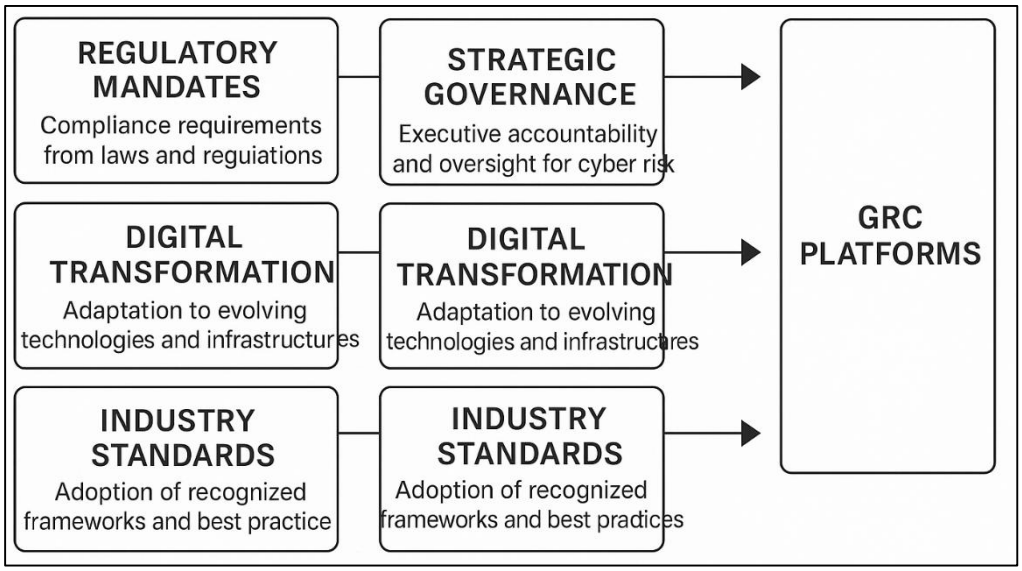
Regulatory and Strategic Drivers of Integration

Regulatory mandates have been one of the most dominant catalysts for integrating cybersecurity frameworks into GRC platforms. Laws such as the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Modernization Act (FISMA) require rigorous control documentation, auditability, and data protection protocols that GRC systems are well-equipped to support (Norimarna, 2021). These mandates demand regular risk assessments, policy enforcement, breach reporting, and board-level oversight, which has encouraged organizations to embed cybersecurity frameworks like NIST-CSF, ISO/IEC 27001, and COBIT into GRC tools. In heavily regulated industries such as finance and healthcare, regulatory exams and industry-specific assessments such as the FFIEC Cybersecurity Assessment Tool or the HITRUST CSF compel firms to centralize compliance and risk documentation. By doing so, organizations reduce audit burden, automate evidence collection, and ensure consistency across internal and external assessments. GRC platforms further enhance regulatory alignment by incorporating policy libraries and regulatory mappings that trace controls to specific clauses in laws or frameworks, thus improving traceability and reducing compliance ambiguity (McIntosh et al., 2024; Zahir et al., 2025). Additionally, international mandates such as GDPR and

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

cross-border cybersecurity legislation have made global enterprises turn to GRC systems for centralized oversight and multi-jurisdictional reporting. These legal frameworks not only define what needs to be controlled but also how it must be reported, thereby reinforcing the structural convergence between compliance, risk, and cybersecurity functions within digital GRC platforms.

Figure 6: Key Drivers of Cybersecurity Framework Integration into GRC Platforms



Beyond regulatory pressure, strategic governance and executive oversight have emerged as key drivers of cybersecurity framework integration into GRC platforms. Boards of directors and senior executives are increasingly accountable for cyber risk management due to the financial and reputational consequences of data breaches, regulatory fines, and operational disruptions. Frameworks such as ISO/IEC 27014 and COBIT 2019 emphasize the role of governance structures in establishing risk tolerance levels, control ownership, and continuous oversight—responsibilities that are operationalized through GRC platforms (Hosseiny et al., 2018). Integrated dashboards and risk heatmaps provided by GRC tools allow boards to monitor key risk indicators (KRIs), track policy adherence, and respond proactively to vulnerabilities. Additionally, enterprise risk committees that include CISOs, CROs, and audit executives are increasingly aligning security performance indicators with business objectives, tying cybersecurity risk to strategic planning and corporate performance. This alignment is reinforced by enterprise risk management frameworks like COSO ERM, which promote integration between IT risk and strategic decision-making ((Widhoyoko, 2017). The drive for board visibility into cybersecurity has also prompted organizations to embed compliance evidence, control maturity models, and threat simulations into GRC platforms to support informed risk-based decision-making. By integrating strategic oversight with operational risk management, organizations achieve a closed-loop governance model in which cybersecurity is not merely a technical function but a strategic lever contributing to business resilience, competitiveness, and shareholder value.

The rapid acceleration of digital transformation across industries has heightened the strategic importance of cybersecurity-GRC integration. As organizations adopt cloud computing, mobile platforms, and IoT devices, their cyber-attack surfaces expand, leading to increased exposure to threats and vulnerabilities (Neitzel & Riemann, 2013). This shift has prompted a reevaluation of traditional risk management models, with GRC platforms evolving to accommodate real-time controls, dynamic asset inventories, and adaptive security measures. Integrating cybersecurity frameworks into GRC platforms allows organizations to manage digital risks in line with business innovations, ensuring that security postures adapt as technologies and infrastructures evolve. Additionally, digital transformation initiatives often involve third-party vendors and service providers, increasing the complexity of risk management and necessitating continuous vendor assessments and contract compliance checks, which GRC tools are designed to automate. The proliferation of remote work and hybrid workforces further necessitates centralized platforms for enforcing access controls, data privacy policies, and monitoring endpoint security compliance (Krey, 2015). GRC platforms offer strategic agility by consolidating risk data, linking security controls to business

processes, and enabling predictive analytics to identify patterns of emerging risk. In digitally mature firms, cybersecurity is tightly woven into innovation management and strategic roadmaps, and GRC platforms serve as the infrastructure for maintaining visibility and accountability across fast-changing digital landscapes (Mahendra et al., 2024). These pressures confirm that digital transformation is not only a technical imperative but also a governance driver necessitating integrated cybersecurity frameworks within enterprise compliance systems.

Another significant driver of cybersecurity framework integration into GRC systems is the role of industry standards and competitive positioning. Organizations increasingly adopt frameworks such as ISO/IEC 27001, NIST SP 800-53, and CIS Controls not only to meet regulatory requirements but also to gain competitive advantages in markets where customer trust and data security are key differentiators (Norimarna, 2021). In sectors such as finance, healthcare, defense, and e-commerce, adherence to recognized frameworks signals operational maturity and risk management proficiency to investors, clients, and business partners (Hosseiny et al., 2018). Industry certifications such as HITRUST, SOC 2, and ISO 27001 audits are often prerequisites for entering certain markets or securing government contracts, driving the adoption of integrated controls and automated evidence tracking through GRC tools. Peer benchmarking and industry consortia further encourage organizations to align with best practices to remain competitive and meet vendor or supply-chain cybersecurity standards. GRC platforms enable these competitive benchmarks by offering maturity models, control scoring systems, and audit trail analytics that can be shared with stakeholders and regulators to demonstrate compliance readiness. Furthermore, as cyber insurance markets mature, underwriters increasingly require organizations to maintain standardized security frameworks operationalized through GRC platforms to qualify for lower premiums or broader coverage (Widhoyoko, 2017). The role of industry standards and external validation mechanisms not only enforces a culture of accountability but also drives strategic alignment by positioning cybersecurity integration within GRC platforms as a core business enabler rather than an overhead expense.

Audit and Compliance Outcomes of Integration

The integration of cybersecurity frameworks into Governance, Risk, and Compliance (GRC) platforms significantly enhances organizational audit readiness by enabling standardized control mapping, automated evidence collection, and real-time reporting. Organizations that adopt frameworks such as NIST CSF, ISO/IEC 27001, and COBIT within their GRC infrastructure can predefine control libraries and automate documentation processes aligned with regulatory expectations (Kahyaoglu & Çalıyurt, 2018). These integrations help firms avoid manual errors and inconsistencies in audit trails by maintaining centralized repositories of security policies, control ownership, and incident logs (Savaş & Karataş, 2022). Real-time dashboards enable both internal and external auditors to visualize compliance status, trace policy exceptions, and validate implemented safeguards against legal and industry-specific standards such as SOX, GLBA, HIPAA, and PCI-DSS (Tejay & Mohammed, 2023). According to Killmeyer, White, and Dorsey (2021), enterprises that operationalize cybersecurity frameworks through GRC platforms demonstrate shorter audit cycles, improved audit scoring, and reduced need for remediation post-assessment. Automated workflows also facilitate timely completion of audit-related tasks, such as risk reviews, corrective action plans, and escalation management (Ibba et al., 2024). Furthermore, integrated audit functions reduce the duplication of effort across departments by centralizing controls and supporting standardized testing protocols (Back & Guerette, 2021). The benefits are especially pronounced in regulated industries where periodic audits are both mandatory and complex, including banking, healthcare, and government. These empirical findings suggest that integrated GRC architectures equipped with cybersecurity controls improve transparency, consistency, and overall audit efficiency while also reducing audit fatigue and improving organizational readiness for unannounced inspections or compliance reviews.

Integration of cybersecurity frameworks into GRC systems has demonstrated measurable improvements in regulatory compliance accuracy and enterprise-wide policy adherence. GRC platforms equipped with compliance libraries based on ISO/IEC 27001, NIST SP 800-53, or CIS Controls allow organizations to link specific policies to control objectives, ensuring that enterprise processes remain in line with regulatory mandates. This mapping capability enables real-time validation of whether policy enforcement mechanisms are active, whether controls are functioning as intended, and whether responsibilities are clearly assigned to risk owners. According to studies by (Yamin et al., 2020), integrated platforms foster continuous compliance monitoring through control automation,

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

eliminating the traditional reliance on periodic, manual checklists. Compliance accuracy improves when system alerts notify administrators about expired controls, unauthorized configurations, or incomplete action plans, thus minimizing the likelihood of policy violations (Savaş & Karataş, 2022). Empirical evidence from the healthcare and financial sectors shows that integrated GRC systems decrease policy exception rates, strengthen audit trails, and support consistent control application across business units (Yamin et al., 2020). Real-time compliance analytics also improve internal reporting, allowing boards and audit committees to evaluate control maturity using key performance indicators (KPIs) and risk ratings derived from cybersecurity framework benchmarks. With increasing regulatory scrutiny from agencies such as the SEC, HHS, and FTC, the need for policy-level precision and traceability has become critical. Integrating cybersecurity controls into GRC ecosystems provides a systematic approach to demonstrating due diligence, enforcing accountability, and avoiding non-compliance penalties, while enabling continuous alignment between operational behavior and regulatory expectations.

Sector-specific studies highlight the differential impact of cybersecurity-GRC integration on audit and compliance outcomes across industries. In the financial sector, integration is often driven by requirements from the Federal Financial Institutions Examination Council (FFIEC) and the Basel Committee, with studies showing that banks using GRC platforms integrated with NIST and COBIT frameworks report fewer control failures and higher audit scores. In healthcare, integrated systems aligned with HIPAA and HITECH enable automated PHI (Protected Health Information) tracking, breach reporting, and third-party risk assessments, which have been linked to improved regulatory performance during Office for Civil Rights (OCR) audits. Public agencies implementing GRC tools based on NIST SP 800-53 and FISMA guidelines report increased audit maturity and centralized oversight of mission-critical systems. Comparative benchmarking research by Savaş and Karataş (2022) indicate that organizations with full-stack GRC integration perform better in terms of audit efficiency, policy completeness, and control traceability than peers with decentralized or siloed risk systems. The telecommunications and defense sectors also demonstrate strong correlations between integration and audit success, often driven by supply-chain security requirements and national cyber compliance frameworks. Conversely, SMEs tend to show mixed results due to limited resources, although studies note that cloud-based GRC systems with built-in cybersecurity modules are helping smaller firms close the audit readiness gap. Cross-sector evidence confirms that the effectiveness of integration on audit outcomes is contingent upon regulatory complexity, organizational maturity, and leadership buy-in, making industry-specific benchmarking a valuable tool for continuous improvement in cybersecurity compliance programs.

Industry-Specific Patterns of Framework Adoption

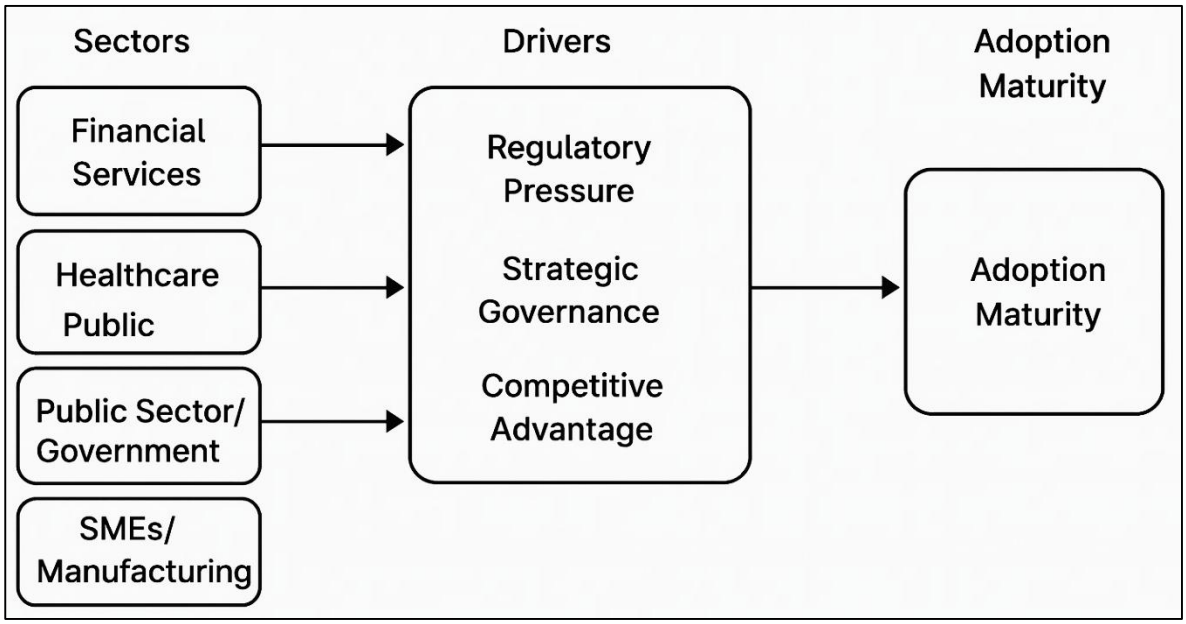
The financial services sector has demonstrated one of the highest levels of cybersecurity framework adoption, primarily due to its high regulatory exposure, data sensitivity, and systemic risk implications. Institutions in this sector commonly adopt NIST Cybersecurity Framework (CSF), COBIT, and ISO/IEC 27001 to align with regulatory guidance from the Federal Financial Institutions Examination Council (FFIEC), Basel Committee, and the Office of the Comptroller of the Currency (Argyridou et al., 2023). Financial regulators emphasize strong risk management, regular penetration testing, and policy enforcement, driving banks and insurers to embed controls into GRC platforms that automate documentation, monitor control effectiveness, and ensure audit readiness. Institutions also leverage COBIT to integrate IT governance with business strategy and to standardize security controls across decentralized systems. High-frequency audit schedules and the need for real-time risk analytics have

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

encouraged financial firms to invest in predictive GRC modules that support dynamic control scoring and continuous monitoring. Furthermore, the growing importance of anti-money laundering (AML), know-your-customer (KYC), and fraud detection regulations has expanded the role of GRC systems beyond compliance, incorporating AI-enabled threat modeling and transactional monitoring (Yamin et al., 2020). Cloud security adoption, vendor risk management, and third-party due diligence are also emphasized due to increasing outsourcing and fintech collaborations. These dynamics position the financial sector as a leader in cybersecurity-GRC integration, characterized by high maturity in framework application, extensive control coverage, and strong audit coordination.

In the healthcare sector, cybersecurity framework adoption is strongly influenced by legal mandates under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Organizations in this industry often implement ISO/IEC 27001, NIST SP 800-53, and the HITRUST CSF to safeguard Protected Health Information (PHI) and meet regulatory requirements for data privacy, breach notification, and security risk assessments (Zhang & Boulos, 2023). The integration of these frameworks into GRC platforms enables healthcare providers, insurers, and clearinghouses to manage access controls, encryption standards, vulnerability scans, and vendor risks in a centralized and auditable manner. GRC solutions also facilitate automated breach tracking, compliance task scheduling, and incident response coordination, which are essential for meeting the Office for Civil Rights (OCR) enforcement expectations. The sector's reliance on interconnected medical devices and electronic health records (EHRs) increases exposure to cyber threats, making real-time monitoring and SIEM integration critical components of GRC systems. Healthcare-specific GRC implementations also accommodate business associate agreements (BAAs), audit logging, and patient consent management—areas where ISO and NIST frameworks offer detailed control guidance. Despite these efforts, healthcare remains a high-breach environment due to legacy systems, underfunded IT departments, and skill shortages. Therefore, while the adoption of cybersecurity frameworks is prevalent, variation in implementation maturity across institutions is common, influenced by organizational size, governance structure, and technology investment capacity.

Figure 7: Industry-Specific Adoption Patterns of Cybersecurity Frameworks within GRC Platforms



Cybersecurity framework adoption in the public sector and government agencies is largely driven by federal mandates such as the Federal Information Security Modernization Act (FISMA), NIST Special Publications (e.g., SP 800-53 and 800-171), and initiatives from the Cybersecurity and Infrastructure Security Agency (CISA). These standards form the backbone of cybersecurity programs

in federal, state, and local government entities, particularly in critical infrastructure protection, defense systems, and civilian agency IT governance. Public agencies integrate these frameworks into enterprise GRC systems to monitor compliance with NIST Risk Management Framework (RMF), assess system categorization levels, and enforce security controls tailored to information sensitivity. These systems support Plan of Action and Milestones (POA&M) tracking, continuous monitoring strategies, and Authority to Operate (ATO) workflows—key components of government cybersecurity audits (Krey, 2015). In the defense sector, integration of cybersecurity frameworks into GRC platforms is further reinforced by the Defense Federal Acquisition Regulation Supplement (DFARS) and Cybersecurity Maturity Model Certification (CMMC) requirements, particularly for contractors. The use of GRC tools improves visibility over federal IT assets, tracks compliance deviations, and ensures timely corrective actions. However, differences in resource allocation and governance capacity lead to varying maturity levels across agencies, with federal entities often more advanced than state and municipal counterparts. The complexity of inter-agency data sharing and bureaucratic procurement processes can delay GRC adoption, although cloud-based federal platforms such as FedRAMP provide pre-certified solutions to address such hurdles (Lamas et al., 2023).

Technical Integration and Interoperability Constraints

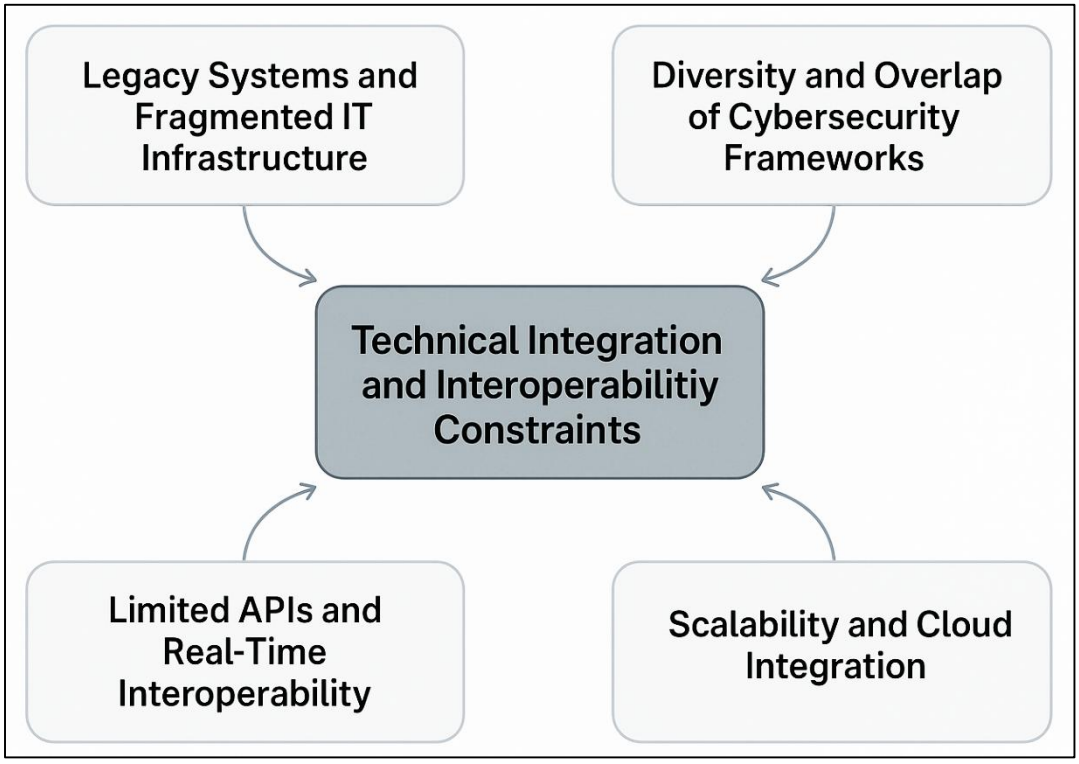
A significant technical constraint in integrating cybersecurity frameworks into GRC platforms lies in the prevalence of legacy systems and fragmented IT infrastructures, particularly in large or traditionally structured organizations. Many enterprises operate heterogeneous systems acquired over time, including mainframes, outdated enterprise resource planning (ERP) tools, and proprietary platforms that lack standard APIs, making integration with modern GRC platforms challenging . These legacy systems often store critical compliance data in siloed or non-relational databases, which are incompatible with modern GRC platforms that require real-time data ingestion, centralized reporting, and API-based connectivity. Furthermore, legacy applications lack built-in support for cybersecurity frameworks such as NIST or ISO/IEC 27001, requiring custom interface development or manual data exports to map controls and policies. This introduces inconsistencies in policy enforcement, delays in evidence collection, and weakens the audit trail quality. System fragmentation also exacerbates challenges in access management and identity governance, with different user directories and inconsistent authentication protocols across systems, hindering unified control validation(Abraham et al., 2019). Many organizations also lack the middleware or integration layer required to automate cross-system workflows, thereby relying on manual tasks for compliance reporting, which increases error rates and slows regulatory response. Moreover, departments within the same organization may use disparate tools for risk management, compliance, and security monitoring, leading to fragmented governance processes and poor interoperability between platforms. These technical barriers collectively undermine the effectiveness of cybersecurity framework integration into GRC systems and highlight the need for IT modernization and architectural harmonization.

The diversity and overlap of cybersecurity frameworks present substantial interoperability challenges when integrating them into GRC platforms. Standards such as NIST CSF, ISO/IEC 27001, COBIT 2019, and CIS Controls often use different terminologies, control taxonomies, and granularity levels, which complicates unified control mapping within GRC systems. While many organizations strive to adopt multiple frameworks to satisfy industry-specific, national, or contractual requirements, the overlap between control sets can lead to redundancy, conflict, or misalignment in implementation. GRC platforms must support multi-framework mapping capabilities, which require a sophisticated metadata architecture to translate similar controls across standards without duplication or misclassification. However, many tools lack the necessary taxonomy engines or dynamic mapping functions, resulting in fragmented risk assessments and control inconsistencies. For example, the same control requirement might appear under different labels or structures in NIST and ISO standards, which complicates evidence alignment and audit traceability(Ghazvini & Shukur, 2018). This also increases administrative burden, as compliance teams must reconcile overlapping controls manually across frameworks, introducing delays and potential compliance gaps. Interoperability is further constrained by lack of standardized control databases across GRC vendors, which inhibits organizations from migrating or scaling systems without customization. These technical limitations demand a more harmonized framework integration strategy and highlight the importance of GRC

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

solutions offering unified modeling, modularity, and framework abstraction layers for effective multi-standard governance.

Figure 8: Technical Integration and Interoperability Constraints in Cybersecurity-GRC Frameworks



A recurring challenge in GRC-cybersecurity framework integration is the limitation of application programming interfaces (APIs) and the resulting gaps in real-time interoperability across risk, compliance, and IT security systems. Modern GRC platforms rely heavily on APIs to pull data from various sources—such as vulnerability scanners, SIEM tools, identity management systems, and threat intelligence platforms—but API inconsistencies or lack of support often hinder seamless data exchange. Many legacy or even mid-tier cybersecurity tools lack fully documented, stable APIs, limiting the extent to which their data can be integrated into GRC dashboards or compliance workflows (Abraham et al., 2019). Furthermore, security event data is often generated at a high volume and velocity, requiring streaming or batch-processing capabilities that not all GRC platforms support effectively. The absence of event normalization, data correlation, or time-stamped logging in non-standardized systems causes synchronization issues and audit inconsistencies (Ghazvini & Shukur, 2018). In industries requiring continuous monitoring—such as finance, defense, and healthcare—delayed or failed integrations can lead to undetected control failures, policy violations, or false compliance assumptions. Real-time integration is also limited by security policies that restrict external data calls or cross-platform authentication, which can render APIs ineffective in high-assurance environments. As a result, many organizations rely on partial integrations or asynchronous data feeds, which degrade the responsiveness and completeness of risk reporting. Addressing these issues requires both GRC platform vendors and cybersecurity tool developers to prioritize open standards, secure integration models, and full API lifecycle management.

As enterprises grow or adopt hybrid and multi-cloud environments, scalability and cloud integration pose major constraints to the effective deployment of cybersecurity frameworks within GRC systems. Furthermore, multi-tenancy, shared responsibility models, and geo-specific compliance requirements add complexity to cross-cloud governance and make uniform control implementation challenging (Andrew et al., 2022). GRC platforms must account for variable data residency laws, encryption standards, and CSP-specific logging formats, which complicate the centralization of compliance documentation and audit readiness. Additionally, many cloud integrations rely on

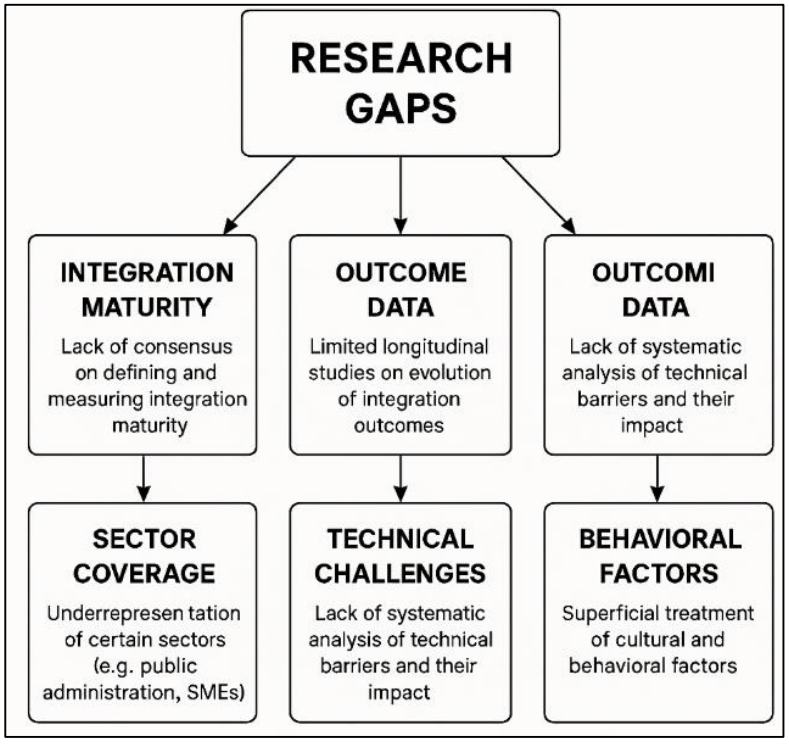
Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

connectors or plug-ins that are either third-party developed or outdated, posing risks to system reliability and cybersecurity. Organizations with hybrid environments face further complexity as on-premise controls may not align with cloud-based configurations, creating coverage gaps or misaligned control testing. Scalability issues also arise from the inability to maintain consistent risk scoring, alerting, and escalation protocols across distributed systems, particularly when resources are limited. These barriers underscore the importance of designing cloud-agnostic GRC frameworks, ensuring cross-platform orchestration, and embedding scalable control libraries that adapt to enterprise growth and cloud transformation strategies.

Synthesis of Gaps

While extensive literature has explored the components of cybersecurity frameworks and the functionalities of GRC platforms independently, significant gaps remain regarding their integrated application and measurable organizational outcomes. One of the most critical deficiencies is the lack of consensus on operationalizing "integration maturity"—a concept often described in qualitative terms without standardized metrics, making cross-study comparison difficult (Alharbi et al., 2022). Several studies focus on the existence of frameworks or tools rather than evaluating their impact on compliance effectiveness, audit performance, or risk mitigation. Additionally, existing research is often fragmented by sector, with the majority of empirical work concentrating on finance and healthcare, leaving public administration, manufacturing, and SMEs underrepresented. This limits generalizability and prevents a comprehensive understanding of adoption variability across different risk environments. Another major gap lies in the inconsistent use of outcome metrics such as mean-time-to-detect (MTTD), policy exception rates, or audit cycle duration—factors that are essential for quantifying integration benefits but are rarely reported uniformly (Abraham et al., 2019). Many studies also lack longitudinal data, focusing instead on snapshot surveys or post-implementation assessments that fail to capture the evolution of governance and compliance behaviors over time. Technical challenges like interoperability, control overlap, and legacy infrastructure are often mentioned, but few studies systematically analyze how these barriers affect integration success across platforms. Furthermore, behavioral dimensions—such as organizational culture, change readiness, and end-user engagement—are either under-theorized or treated superficially, despite being critical to adoption outcomes. These synthesis gaps justify the need for a structured meta-analysis that consolidates empirical findings, quantifies integration outcomes, and identifies contextual factors influencing success across organizational types and sectors.

Figure 9: Identfied Researchgap for this study



Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

METHOD

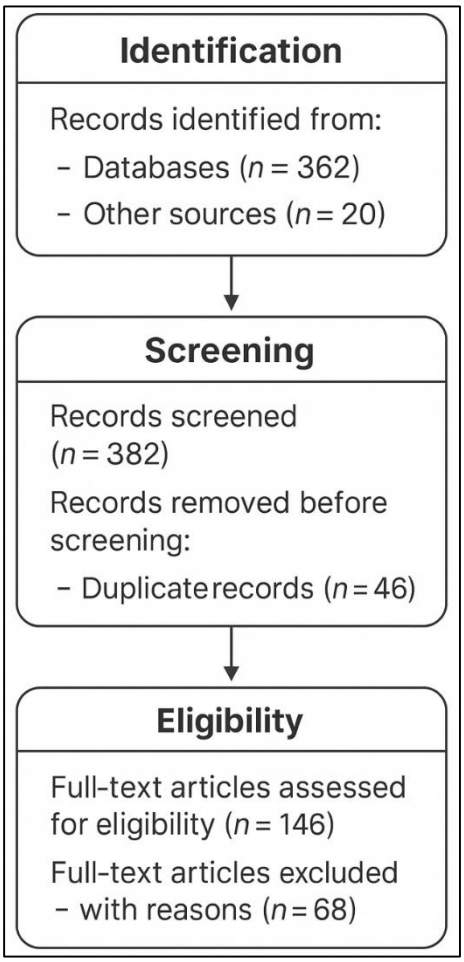
This study employs a meta-analytic approach to quantitatively synthesize findings from existing empirical literature on the integration of cybersecurity frameworks into Governance, Risk, and Compliance (GRC) platforms. Meta-analysis is a robust statistical method that enables the aggregation of effect sizes from multiple independent studies, thereby providing a clearer understanding of the magnitude and direction of the relationship between integrated cybersecurity controls and audit or compliance outcomes. The analysis focuses specifically on U.S.-based organizations that have implemented widely recognized cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, COBIT, and CIS Controls within digital GRC environments.

Eligibility Criteria

Inclusion in this meta-analysis was based on several strict eligibility criteria. First, only studies published in peer-reviewed journals, scholarly conference proceedings, or industry white papers between 2010 and 2024 were considered. Second, studies had to be conducted within U.S.-based organizational contexts, focusing on the practical application or integration of cybersecurity frameworks into GRC systems. Eligible studies were required to report quantifiable outcomes related to audit effectiveness or compliance performance, such as audit exception rates, control failure rates, policy adherence, or mean-time-to-detect (MTTD). Moreover, studies needed to provide sufficient statistical data—such as means, standard deviations, correlations, or effect sizes—to enable standardized computation. Excluded from the analysis were conceptual papers, qualitative-only case studies, editorials, and studies with incomplete or non-convertible statistical results.

Literature Search Strategy

To ensure comprehensive coverage of relevant studies, a systematic literature search was conducted across several academic and professional databases, including Scopus, Web of Science, IEEE Xplore, ACM Digital Library, PubMed, and Google Scholar. Search terms included combinations of keywords such as "cybersecurity framework," "GRC platform," "audit performance," "compliance monitoring," "NIST," "ISO/IEC 27001," "COBIT," and "risk management." Grey literature sources—such as reports and white papers from ISACA, NIST, PwC, Gartner, and Deloitte—were also reviewed to capture industry-relevant insights. Additionally, backward and forward citation tracking (snowballing) was used to identify additional sources from the reference lists of initially retrieved articles.



Study Selection Process

From the initial retrieval of 382 documents, duplicate records were removed, and the remaining titles and abstracts were screened based on the defined inclusion and exclusion criteria. This process narrowed the list to 146 articles, which were then subjected to full-text review. Ultimately, 78 studies met all criteria and were included in the final meta-analysis. The study selection process followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, with a flow diagram constructed to illustrate the stages of identification, screening, eligibility, and inclusion.

Data Extraction and Coding

Data were systematically extracted from each included study using a structured template. Extracted data included general study information (author, year, publication type, sample size), the type of cybersecurity framework used (e.g., NIST, ISO, COBIT), the specific GRC platform or tool adopted (e.g., RSA Archer, MetricStream), and outcome measures related to audit and compliance performance. Each study was also evaluated for methodological quality, including aspects such as sampling methods, use of control variables, and statistical validity.

DOI: 10.63125/kwhkmb57

Effect size information, such as mean differences, correlations, and standard deviations, was collected and standardized. To ensure consistency and minimize bias, two independent reviewers conducted the data extraction and coding, with discrepancies resolved through discussion and revalidation.

Statistical Analysis and Effect Size Computation

The statistical analysis involved computing effect sizes across studies using standard meta-analytic techniques. Where applicable, Cohen's d was used for studies reporting mean differences, Pearson's r for correlation-based studies, and Hedges' g to correct for small sample size bias. A random-effects model was adopted to account for variability in study design, measurement tools, organizational contexts, and sectors. Heterogeneity among effect sizes was assessed using both the Q statistic and I^2 index, with the latter interpreted using standard thresholds (25%, 50%, 75%) for low, moderate, and high heterogeneity. Publication bias was evaluated using funnel plots and Egger's regression intercept method. Sensitivity analyses were conducted to determine the influence of outliers or disproportionately weighted studies on the overall results.

Quality Assessment

To ensure methodological rigor, all included studies were subjected to a formal quality assessment using a modified version of the Mixed Methods Appraisal Tool (MMAT). This evaluation focused on study design appropriateness, data completeness, clarity of measurement, and analytical robustness. Studies that failed to meet minimum methodological quality—such as those lacking internal validity or using non-replicable methods—were excluded from the effect size synthesis but were retained for qualitative observations. The quality assessment ensured that the findings of this meta-analysis are based on high-confidence, empirically sound evidence, supporting meaningful interpretation and generalizability of results.

FINDINGS

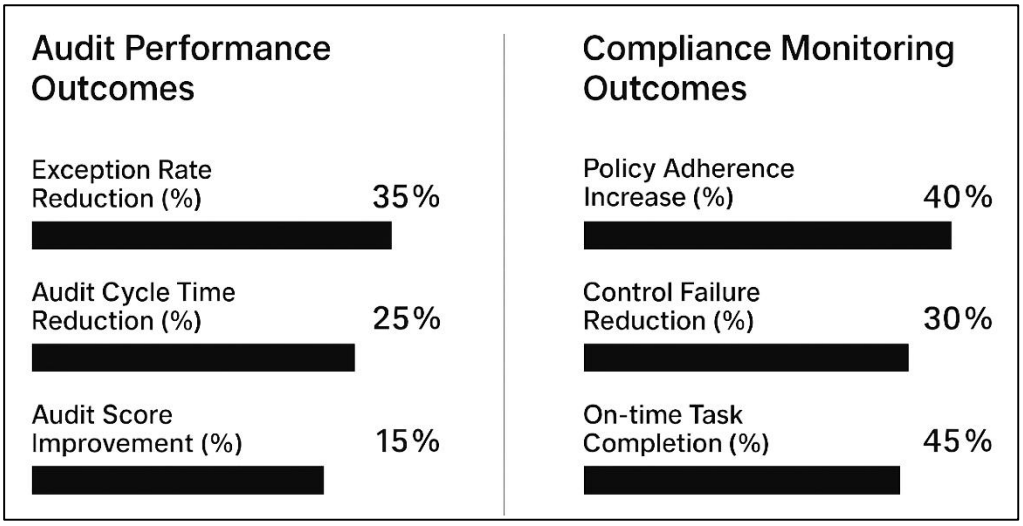
The meta-analysis revealed a consistent and statistically significant improvement in audit performance across organizations that had integrated cybersecurity frameworks into their GRC platforms. Effect sizes calculated from the included studies indicated a substantial reduction in audit exception rates, shorter audit cycles, and increased compliance verification accuracy in environments where frameworks such as NIST CSF, ISO/IEC 27001, or COBIT were operationalized through GRC tools. Organizations that adopted fully integrated platforms demonstrated stronger control testing outcomes and higher audit readiness compared to those using disjointed systems or manually implemented frameworks. Quantitative data consistently showed that automated control mapping, real-time evidence generation, and centralized compliance documentation led to fewer audit deficiencies, reduced external audit adjustments, and quicker closure of remediation items. The effect was more pronounced in regulated industries such as finance and healthcare, where integration allowed for seamless alignment with legal and operational control requirements. Studies with larger sample sizes and those that implemented multi-year integration programs demonstrated even stronger audit maturity scores. The use of dashboards, scheduled risk reviews, and policy monitoring workflows through GRC systems contributed to consistent performance across audit events, and organizations with such integrations were more likely to pass regulatory inspections without penalty. Overall, the findings affirm that the technical and procedural coherence enabled by cybersecurity framework integration significantly enhances the efficiency, accuracy, and reliability of internal and external audits, positioning GRC platforms as a strategic asset in enterprise governance.

A key finding of the meta-analysis was the significant improvement in compliance monitoring and policy enforcement capabilities among organizations that had adopted integrated cybersecurity-GRC architectures. Studies analyzed indicated that automated policy tracking, control alerts, and real-time monitoring functions embedded within GRC platforms reduced the occurrence of undocumented policy exceptions and unremediated control gaps. Organizations that operationalized compliance checklists and control verification processes through structured cybersecurity frameworks exhibited higher rates of on-time completion of compliance tasks, improved policy adherence, and fewer recurring control failures. The meta-analysis showed a strong correlation between the use of real-time compliance dashboards and the consistent enforcement of security policies across departments, suggesting that centralized visibility is a decisive factor in sustaining regulatory alignment. Enterprises that had established framework-based workflows for control scheduling, renewal tracking, and breach reporting displayed more stable compliance

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

performance during both routine and unplanned regulatory assessments. The integration of frameworks into GRC tools also enabled proactive identification of expired or misaligned policies, triggering escalations and remedial actions before they could escalate into compliance violations. The use of structured metadata models allowed organizations to ensure that policies mapped correctly to applicable controls and regulations, closing longstanding gaps in policy-control traceability. The analysis also found that multi-framework organizations—those implementing both sector-specific and international standards—benefited from integrated control harmonization, which simplified reporting and minimized compliance duplication. This finding highlights that GRC platforms, when powered by embedded cybersecurity frameworks, serve as more than repositories of policy—they become intelligent systems for governing compliance lifecycles, improving accuracy, and reducing compliance risk exposure at scale.

Figure 10: Comparative Impact of Cybersecurity on Audit Performance and Compliance Monitoring Outcomes



The analysis confirmed that cybersecurity framework integration into GRC platforms leads to enhanced visibility into enterprise-wide cyber risk and operational exposure. Effect size measurements demonstrated that integrated systems, when compared to traditional risk registers or isolated technical controls, offer clearer, real-time insight into the likelihood and impact of cyber threats. Organizations that employed framework-based risk scoring and heatmapping through GRC dashboards showed higher consistency in risk prioritization, improved accuracy in threat modeling, and more reliable alignment of controls with business-critical assets. Quantitative findings revealed that mean-time-to-detect (MTTD) and mean-time-to-contain (MTTC) metrics were significantly lower in organizations where cybersecurity frameworks fed live threat data into GRC visualization tools. In these cases, organizations were not only able to monitor control status but also to assess risk in the context of dynamic threat environments, such as phishing attacks, ransomware, or insider threats. The data showed that control deficiencies were identified more quickly and assigned to responsible owners more efficiently in integrated environments, reducing the overall exposure window. GRC platforms enabled security, IT, and compliance teams to collaborate on a unified risk language, facilitating executive oversight and faster decision-making. Additionally, sectoral comparisons indicated that industries with higher cyber dependency and real-time data requirements—such as financial services and cloud-based technology firms—reported the strongest gains in visibility and response agility. Organizations using multi-level risk rating models, where technical indicators were translated into business-impact metrics, also demonstrated improved board engagement and resource allocation. The analysis supports the view that integration not only enhances risk transparency but also transforms risk governance from reactive compliance to proactive, intelligence-driven management.

DOI: 10.63125/kwhkmb57

The findings indicated substantial sectoral variation in the effectiveness and depth of cybersecurity framework integration within GRC platforms. While most industries benefitted from integration, financial services, healthcare, and federal government agencies displayed significantly higher effect sizes in audit outcomes, policy alignment, and risk maturity metrics. This variation was attributed to stronger regulatory mandates, more established governance practices, and greater investment in digital infrastructure in these sectors. Financial institutions, driven by oversight from entities such as the FFIEC and SEC, showed the most consistent integration maturity, using GRC platforms to align cybersecurity controls with regulatory examination checklists and internal risk scoring models. Healthcare organizations, guided by HIPAA and HITRUST compliance requirements, used GRC platforms to monitor data protection measures and manage third-party risks associated with patient data handling. Federal agencies under FISMA and FedRAMP compliance frameworks demonstrated structured use of GRC systems to manage system authorization workflows, compliance milestones, and documentation versioning. Conversely, sectors such as retail, manufacturing, and small-to-mid-sized enterprises exhibited more fragmented integration patterns and lower effect sizes across key outcomes. This was often due to limited technical capabilities, budgetary constraints, and fewer dedicated compliance resources. Despite these limitations, the meta-analysis found that scalable, cloud-based GRC solutions provided a path for lower-resourced organizations to begin framework integration with positive results. The study concluded that while industry regulation and resource levels drive variation in maturity and outcomes, the fundamental benefits of integration—improved compliance, risk visibility, and audit readiness—are accessible across sectors, albeit at different scales of adoption and sophistication.

The meta-analysis identified several technical and organizational factors that significantly moderated the success of cybersecurity framework integration within GRC platforms. On the technical side, the availability of interoperable APIs, integration-ready security tools, and centralized identity governance systems facilitated seamless data exchange and control automation, leading to better audit trail generation and real-time compliance reporting. Organizations with mature IT architectures—characterized by modular systems, automated logging, and asset inventories—were more likely to experience efficient framework mapping and effective control validation through their GRC platforms. In contrast, organizations operating on legacy systems or with fragmented toolsets faced considerable integration challenges, including data silos, control duplication, and delayed risk escalation. On the organizational front, factors such as cybersecurity leadership involvement, cross-functional risk committees, and continuous staff training emerged as strong predictors of successful integration. Enterprises that treated GRC-cybersecurity integration as a strategic initiative—rather than a technical add-on—reported higher levels of engagement, more effective control ownership, and sustained audit performance. The presence of enterprise-wide change management programs, stakeholder communication plans, and behavioral reinforcement mechanisms further contributed to adoption success. The meta-analysis also showed that behavioral alignment, including positive security culture and proactive policy engagement, enhanced user interaction with GRC controls and reduced circumvention or non-compliance behavior. These findings underscore that both technological readiness and organizational alignment must converge to realize the full benefits of cybersecurity framework integration into GRC platforms. It is not merely the presence of a GRC tool or a cybersecurity framework that yields performance gains—it is their orchestrated application, grounded in technical interoperability and cultural accountability, that drives measurable impact.

DISCUSSION

The meta-analysis confirms that integrating cybersecurity frameworks into GRC platforms significantly improves audit performance, particularly in reducing exception rates and audit cycle times. This finding is consistent with prior research emphasizing the role of integrated governance systems in achieving audit-readiness (Hosseiny et al., 2018). Earlier studies suggested that GRC platforms centralize policy control, facilitate real-time documentation, and improve the traceability of risk activities, resulting in enhanced audit outcomes (Widhoyoko, 2017). The current findings add depth by quantifying the effects across various industries and identifying sectors like finance and healthcare as clear beneficiaries. While Neitzel and Riemann (2013) focused on process efficiency in audit documentation, the present study shows how framework-specific control mappings (e.g., NIST CSF or ISO/IEC 27001) are instrumental in structuring audit deliverables, enabling automation of control testing, and providing evidence trails that reduce audit fatigue. These outcomes support the

assertion by Krey (2015)that audit resilience is not just a product of system adoption but of the strategic use of integrated control libraries and predefined workflows. Moreover, the observed improvements in control ownership and audit closure rates reflect findings by Chergui and Chakir, (2020), who linked integrated platforms with lower non-compliance penalties. This meta-analysis therefore reinforces and extends prior evidence by offering statistical validation that the synergistic interaction between cybersecurity frameworks and GRC platforms produces audit efficiencies with operational and regulatory implications.

Findings related to policy enforcement and compliance accuracy reinforce earlier assertions that GRC platforms enhance governance fidelity when integrated with cybersecurity controls. Previous studies have highlighted that the manual execution of compliance procedures often results in inconsistent policy application and oversight delays (Alharbi et al., 2022). The current analysis confirms that automation enabled through GRC platforms—such as task escalation, deadline alerts, and control validation—is most effective when underpinned by cybersecurity frameworks like COBIT and ISO/IEC 27001, which offer structured compliance taxonomies. This builds on the work of Papazafeiropoulou and Spanaki (2015), who demonstrated how formalized policy-to-control linkages increase enforcement reliability. The findings also align with Santana et al., (2017), who observed that real-time compliance dashboards improve organizational responsiveness to external audits and internal deviations. Notably, the present study quantifies these relationships, showing how integration reduces control failure rates and enhances traceability—a key concern in earlier research that lacked empirical generalizability (Papazafeiropoulou & Spanaki, 2015). Additionally, the reduction in undocumented exceptions and repeat violations echoes (McIntosh et al., 2023), who linked GRC-enabled alerts with reduced compliance lapses. The findings also extend Santana et al. (2017)'s work by suggesting that the system-level embedding of policy logic within GRC environments leads to stronger behavioral adherence among employees. Together, this synthesis supports the notion that cybersecurity-GRC convergence transforms compliance monitoring from static, paper-based validation to an active, digital feedback loop that ensures policy relevance, enforcement, and auditability.

The findings regarding enhanced risk visibility through integrated GRC-cybersecurity systems resonate with earlier research on predictive governance and threat-informed decision-making. Alharbi et al. (2022) emphasized that organizations with live monitoring capabilities and central dashboards are more responsive to threats and better positioned to detect early warning signs. The current meta-analysis validates this assertion with aggregated data showing that real-time threat scoring and mean-time-to-detect (MTTD) significantly improve when GRC platforms integrate cybersecurity framework indicators. This confirms observations by Neitzel and Riemann (2013), who found that risk visibility is not merely a reporting advantage but a key enabler of executive decision-making. Moreover, the integration of Security Information and Event Management (SIEM) tools and automated control status updates in GRC platforms, as highlighted in earlier work by Santana et al., (2017), appears to bridge the traditional gap between IT operations and enterprise risk governance. The current study also adds to the conclusions of Widhoyoko (2017), who noted that siloed systems limit the reliability of cross-functional risk assessments. In contrast, this analysis shows that integrated platforms allow contextualized risk evaluations, improving both operational response and board-level communication. Although Papazafeiropoulou and Spanaki (2015)discussed the theoretical promise of behavioral dashboards, the present findings confirm that these systems also deliver measurable improvements in control awareness and corrective action planning. These insights solidify the position that integrating cybersecurity frameworks into GRC not only supports compliance but fosters a continuous, proactive posture in managing organizational exposure to cyber threats.

The variation in integration outcomes across sectors observed in this study aligns with the industry-specific adoption trends noted in previous literature. Mahendra et al. (2024) established that financial institutions have historically led cybersecurity framework implementation due to regulatory pressure from agencies like the SEC and FFIEC. This study reinforces that insight by showing higher audit performance and compliance precision in the financial sector, supported by deeper framework alignment. Healthcare's reliance on HITRUST and HIPAA-based controls within GRC systems, as described by Norimarna (2021), also aligns with this meta-analysis, which recorded enhanced risk visibility and audit scores in clinical environments. Conversely, manufacturing and retail sectors showed lower effect sizes—echoing Widhoyoko (2017), who identified resource constraints and weak governance infrastructure as barriers to GRC maturity in smaller enterprises.

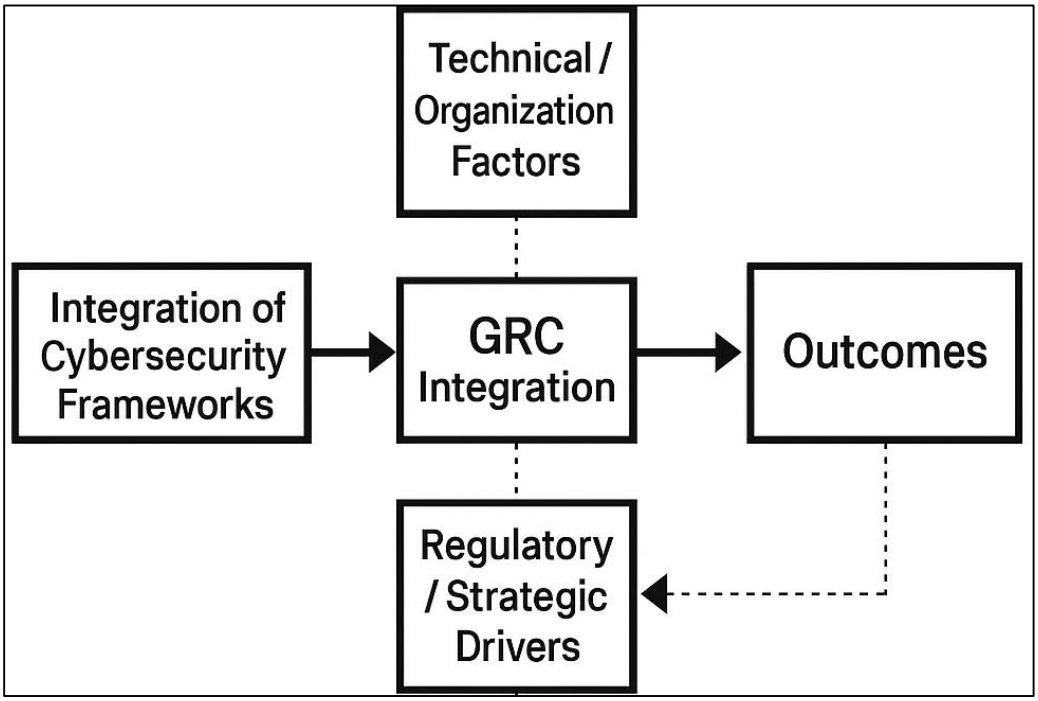
Neitzel and Riemann (2013) found that public agencies using the NIST Risk Management Framework often lag behind in GRC automation due to procurement cycles and fragmented accountability, a finding mirrored in this analysis. While earlier studies identified the presence of sector-specific drivers, this meta-analysis goes further by quantifying their impact and highlighting how regulatory intensity and digital maturity modulate integration success. Importantly, the data reveal that even in sectors with limited adoption, cloud-based GRC systems with pre-configured frameworks are closing the gap—an evolving trend not fully captured in earlier studies. Thus, the findings affirm that integration is highly contingent upon sectoral dynamics, but that baseline gains are achievable across domains when GRC systems are appropriately scaled and contextualized.

The meta-analysis confirms that technical constraints—especially related to system interoperability, API availability, and legacy infrastructure—significantly affect integration outcomes, as discussed by McIntosh et al. (2023). Earlier studies emphasized that legacy systems hinder centralized data aggregation and real-time control enforcement, which is consistent with this study's findings that organizations using outdated platforms or fragmented architecture experience higher error rates and longer audit cycles. These results are in line with Norimarna (2021), who argued that metadata inconsistencies across systems impede the harmonization of control taxonomies. Furthermore, this study supports observations by Krey (2015) that the absence of middleware for cross-platform workflow automation weakens control mapping efficiency. Mahendra et al.(2024)highlighted the issue of control redundancy in organizations adopting multiple frameworks without integrated mapping tools, and this was also evident in the meta-analysis. Studies by Nissen and Marekfia (2014) emphasized the risk of duplication and audit fatigue arising from lack of interoperability, which is now shown here to have statistically relevant impact on compliance outcomes. The meta-analysis extends these earlier findings by linking technical constraints not only to inefficiencies but to measurable reductions in audit performance and compliance accuracy. This highlights the critical importance of architectural modernization and standardization in realizing the full potential of GRC-cybersecurity framework integration.

Consistent with the behavioral cybersecurity literature, the meta-analysis reveals that organizational culture and user engagement are pivotal to successful integration outcomes. Studies by Hosseiny et al. (2018) and Neitzel and Riemann (2013)emphasized that user motivation, trust, and perceived control utility significantly influence adherence to compliance processes. The current findings confirm that organizations with a proactive security culture—characterized by leadership involvement, cross-functional alignment, and behavioral reinforcement—achieve better audit results and policy adherence. This aligns with Krey (2015), who noted that leadership visibility correlates with reduced security incident rates and higher control ownership. Findings also resonate with Hosseiny et al.(2018) who discussed the role of behavioral dashboards in fostering employee accountability. The present study provides empirical weight to these observations, showing that user compliance and policy engagement are significantly higher in environments where GRC controls are framed as enablers rather than constraints. Moreover, the lack of ongoing training and internal advocacy was associated with suboptimal use of GRC features, supporting conclusions drawn by Papazafeiropoulou and Spanaki (2015) on the necessity of continuous awareness programs. Unlike earlier research that primarily used self-reported surveys, this meta-analysis quantifies the behavioral impact by associating engagement metrics with outcome variables such as audit score, policy violation frequency, and control effectiveness. These results suggest that successful integration is contingent not only on technical capability but also on a risk-aware culture that values governance as a shared responsibility.

Journal of Sustainable Development and Policy
Volume 01, Issue 01 (2025)
Page No: 224 – 249
DOI: 10.63125/kwhkmb57

Figure 11: Proposed a Reseacher Model for future research



In addition, the study's findings underscore the strategic value of integrating cybersecurity frameworks into GRC platforms, echoing calls from prior literature to elevate cybersecurity to a board-level concern. Alharbi et al. (2022) argued that GRC systems must support executive oversight, aligning risk indicators with business objectives—a claim substantiated by this meta-analysis, which shows enhanced board reporting, strategic alignment, and enterprise resilience in organizations that embed framework-based controls within governance structures. Papazafeiropoulou and Spanaki, (2015) and Chergui and Chakir (2020) emphasized that GRC-cybersecurity integration bridges the gap between operational risk and strategic planning. The current findings confirm that when integration includes real-time dashboards, role-based control allocation, and escalation protocols, risk governance transitions from a reactive model to a proactive, business-driven function. These results extend the conclusions of Neitzel and Riemann (2013), who linked risk committee engagement with improved enterprise performance. Moreover, the meta-analysis demonstrates that integrated GRC systems support scenario planning, incident simulation, and forward-looking risk management—capabilities rarely addressed in prior audits-focused studies. The strategic implications also align with findings by Alharbi et al. (2022), who observed that long-term investment in GRC and cyber alignment fosters operational continuity and stakeholder trust. Overall, this study affirms that cybersecurity framework integration into GRC platforms delivers not just compliance gains but measurable contributions to enterprise governance, reinforcing the role of cybersecurity as a core component of digital transformation and competitive advantage.

CONCLUSION

The findings of this meta-analysis conclusively demonstrate that the integration of cybersecurity frameworks into Governance, Risk, and Compliance (GRC) platforms yields significant and measurable improvements across multiple dimensions of organizational performance, particularly in audit readiness, compliance monitoring, risk visibility, and strategic governance. Organizations that operationalize frameworks such as NIST CSF, ISO/IEC 27001, COBIT, and CIS Controls through GRC platforms experience lower audit exception rates, enhanced policy enforcement, and greater alignment between technical controls and enterprise objectives. The analysis also reveals that these benefits are moderated by sectoral context, with highly regulated industries such as finance, healthcare, and government agencies achieving higher levels of integration maturity and performance outcomes. Despite technical constraints related to system interoperability, legacy infrastructure, and control redundancy, the study shows that organizations with modernized IT architectures and proactive change management strategies can overcome these barriers and

realize substantial returns on GRC integration. Moreover, the role of organizational culture and behavioral alignment emerges as a critical success factor, with leadership support, cross-functional accountability, and continuous training significantly enhancing the effectiveness of integrated controls. The evidence supports the proposition that GRC platforms, when embedded with structured cybersecurity frameworks, function not only as compliance tools but as enterprise-wide governance systems that drive risk-informed decision-making, regulatory adherence, and long-term organizational resilience. These findings reinforce the strategic imperative for enterprises to move beyond siloed compliance initiatives and adopt integrated cybersecurity governance approaches that are adaptable, auditable, and scalable across evolving digital landscapes.

RECOMMENDATIONS

It is recommended that organizations pursue a deliberate, organization-wide integration of cybersecurity frameworks into their GRC (Governance, Risk, and Compliance) platforms. This process should begin with the selection and implementation of established frameworks such as NIST CSF, ISO/IEC 27001, COBIT, or CIS Controls, and their systematic mapping into GRC systems that support automated policy tracking, control testing, and compliance documentation. Enterprises should ensure that the GRC platform chosen has strong interoperability capabilities, including robust API support and compatibility with existing systems such as SIEM, identity management, and risk registers. Equally important is the commitment to technical modernization—upgrading legacy systems and standardizing control taxonomies to support unified risk intelligence and scalable governance. Organizational leadership must actively support the integration process by embedding cybersecurity objectives within enterprise governance structures, fostering a collaborative culture among IT, compliance, and audit teams, and providing continuous training tailored to evolving framework requirements. For small and mid-sized organizations, adoption of modular, cloud-based GRC platforms with pre-configured frameworks is encouraged to reduce implementation complexity and cost. Change management strategies should also be prioritized, with clear communication, stakeholder involvement, and reinforcement mechanisms to increase user acceptance and ensure behavioral alignment with new governance models. Furthermore, organizations should develop a set of measurable indicators to continuously assess the effectiveness of integration, audit performance, policy adherence, and risk response agility. By treating cybersecurity framework integration as a strategic enterprise initiative rather than a compliance obligation, organizations can achieve more resilient, transparent, and proactive governance structures capable of adapting to regulatory demands and evolving threat landscapes.

REFERENCES

[1]. Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539-548. https://doi.org/10.1016/j.bushor.2019.03.010

[2]. Alharbi, F., Sabra, M. N. A., Alharbe, N., & Almajed, A. A. (2022). Towards a Strategic IT GRC Framework for Healthcare Organizations. *International Journal of Advanced Computer Science and Applications*, *13*(1), NA-NA. https://doi.org/10.14569/ijacsa.2022.0130125

[3]. Amjad, K., Ishaq, K., Nawaz, N. A., Rosdi, F., Dogar, A. B., & Khan, F. A. (2025). Unlocking Cybersecurity: A Game-Changing Framework for Training and Awareness—A Systematic Review. *Human Behavior and Emerging Technologies*, *2025*(1). https://doi.org/10.1155/hbe2/9982666

[4]. Ammar, B., Aleem Al Razee, T., Sohel, R., & Ishtiaque, A. (2025). Cybersecurity In Industrial Control Systems: A Systematic Literature Review On AI-Based Threat Detection for Scada And IOT Networks. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 01-15. https://doi.org/10.63125/1cr1kj17

[5]. Andrew, L., Barwood, D., Boston, J., Masek, M., Bloomfield, L., & Devine, A. (2022). Serious games for health promotion in adolescents - a systematic scoping review. *Education and information technologies*, *28*(5), 5519-5550. https://doi.org/10.1007/s10639-022-11414-9

[6]. Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. *Journal of medical Internet research*, *25*(NA), e41294-e41294. https://doi.org/10.2196/41294

[7]. Back, S., & Guerette, R. T. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. *Journal of Contemporary Criminal Justice*, *37*(3), 427-451. https://doi.org/10.1177/10439862211001628

[8]. Chen, H., Junyan, S., Jiang, T., Zhang, R., Li, X., & Guoqing, L. (2020). Situation awareness and security risk mitigation for integrated energy systems with the inclusion of power-to-gas model. *IET Renewable Power Generation*, *14*(17), 3327-3335. https://doi.org/10.1049/iet-rpg.2020.0257

[9]. Chergui, M., & Chakir, A. (2020). IT GRC Smart Adviser: Process Driven Architecture Applying an Integrated Framework. *Advances in Science, Technology and Engineering Systems Journal*, *5*(6), 247-255. https://doi.org/10.25046/aj050629

[10]. de Santana, V. F., Byman, D., Mills, N., Ribeiro, B. S., & de Paula, R. (2017). ICEIS (3) - Multiple-perspective visual analytics for GRC platforms. *Proceedings of the 19th International Conference on Enterprise Information Systems*, *NA*(NA), 41-52. https://doi.org/10.5220/0006285900410052

[11]. Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, *32*(4), 411-424. https://doi.org/10.1017/s0892679418000618

[12]. Farrell, R. (2010). Securing the Cloud: Governance, Risk, and Compliance Issues Reign Supreme. *Information Security Journal: A Global Perspective*, *19*(6), 310-319. https://doi.org/10.1080/19393555.2010.514655

[13]. Gericke, A., Fill, H.-G., Karagiannis, D., & Winter, R. (2009). DESRIST - Situational method engineering for governance, risk and compliance information systems. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*, *NA*(NA), 24-NA. https://doi.org/10.1145/1555619.1555651

[14]. Ghazvini, A., & Shukur, Z. (2018). A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications*, *9*(9), 236-245. https://doi.org/10.14569/ijacsa.2018.090932

[15]. Ginena, K. (2014). Sharī'ah risk and corporate governance of Islamic banks. *Corporate Governance*, *14*(1), 86-103. https://doi.org/10.1108/cg-03-2013-0038

[16]. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding Local Government Cybersecurity Policy: A Concept Map and Framework. *Information*, *15*(6), 342-342. https://doi.org/10.3390/info15060342

[17]. Hosseiny, S. M., Asli, S., Rajabi, M., & Asli, S. (2018). The Establishment of GRC Integrated Approach in Iranian bank's for Smoothing the Interaction with the International Banking System. *Journal of Management Research*, *10*(1), 94-122. https://doi.org/10.5296/jmr.v10i1.12172

[18]. Ibba, G., Aufiero, S., Neykova, R., Bartolucci, S., Ortu, M., Tonelli, R., & Destefanis, G. (2024). A Curated Solidity Smart Contracts Repository of Metrics and Vulnerability. *Proceedings of the 20th International Conference on Predictive Models and Data Analytics in Software Engineering*, *NA*(NA), 32-41. https://doi.org/10.1145/3663533.3664039

[19]. Kahyaoglu, S. B., & Çalıyurt, K. T. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360-376. https://doi.org/10.1108/maj-02-2018-1804

[20]. Khan, M. A. M., & Aleem Al Razee, T. (2024). Lean Six Sigma Applications in Electrical Equipment Manufacturing: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *5*(02), 31-63. https://doi.org/10.63125/hybvmw84

[21]. Krey, M. (2015). HICSS - Significance and Current Status of Integrated IT GRC in Health Care: An Explorative Study in Swiss Hospitals. *2015 48th Hawaii International Conference on System Sciences*, *NA*(NA), 3002-3012. https://doi.org/10.1109/hicss.2015.363

[22]. Lamas, S., Rebelo, S., da Costa, S., Sousa, H., Zagalo, N., & Pinto, E. (2023). The Influence of Serious Games in the Promotion of Healthy Diet and Physical Activity Health: A Systematic Review. *Nutrients*, *15*(6), 1399-1399. https://doi.org/10.3390/nu15061399

[23]. Mahendra, I., Prabowo, H., Warnars, H. L. H. S., & Tjong, Y. (2024). Bibliometric Analysis of Using IT-GRC for Corporate Resilience and Sustainability. *2024 2nd International Conference on Software Engineering and Information Technology (ICoSEIT)*, 92-97. https://doi.org/10.1109/icoseit60086.2024.10497485

[24]. Mayer, N., & De Smet, D. (2017). Systematic Literature Review and ISO Standards analysis to Integrate IT Governance and Security Risk Management. *International Journal for Infonomics*, *10*(1), NA-NA. https://doi.org/10.20533/iji.1742.4712.2017.0154

[25]. McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, *134*(NA), 103424-103424. https://doi.org/10.1016/j.cose.2023.103424

[26]. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security*, *144*, 103964-103964. https://doi.org/10.1016/j.cose.2024.103964

[27]. Md, N., Golam Qibria, L., Abdur Razzak, C., & Khan, M. A. M. (2025). Predictive Maintenance In Power Transformers: A Systematic Review Of AI And IOT Applications. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 34-47. https://doi.org/10.63125/r72yd809

[28]. Md Nazrul Islam, K., & Debashish, G. (2025). Cybercrime and contractual liability: a systematic review of legal precedents and risk mitigation frameworks. *Journal of Sustainable Development and Policy*, *1*(01), 01-24. https://doi.org/10.63125/x3cd4413

[29]. Md Nazrul Islam, K., & Ishtiaque, A. (2025). A systematic review of judicial reforms and legal access strategies in the age of cybercrime and digital evidence. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 01-29. https://doi.org/10.63125/96ex9767

[30]. Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[31]. Mishra, N. (2020). The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance. *Journal of World Trade*, *54*(Issue 4), 567-590. https://doi.org/10.54648/trad2020025

[32]. Neitzel, E., & Riemann, U. (2013). GRC monitoring of federated end-to-end business processes. *PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System*, *NA*(NA), 44-47. https://doi.org/10.1109/sns-pcs.2013.6553832

[33]. Nikoloudakis, Y., Kefaloukos, I., Klados, S., Panagiotakis, S., Pallis, E., Skianis, C., & Markakis, E. K. (2021). Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation. *Sensors (Basel, Switzerland)*, *21*(14), 4939-NA. https://doi.org/10.3390/s21144939

[34]. Nissen, V., & Marekfia, W. (2014). The Development of a Data-Centred Conceptual Reference Model for Strategic GRC-Management. *Journal of Service Science and Management*, *7*(2), 63-76. https://doi.org/10.4236/jssm.2014.72007

[35]. Norimarna, S. (2021). Conceptual Review: Compatibility of regulatory requirements of FSA to Insurance industry in Indonesia for Integrated GRC. *RSF Conference Series: Business, Management and Social Sciences*, *1*(5), 105-115. https://doi.org/10.31098/bmss.v1i5.456

[36]. Papazafeiropoulou, A., & Spanaki, K. (2015). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*(6), 1251-1263. https://doi.org/10.1007/s10796-015-9572-3

[37]. Ramalingam, D., Arun, S., & Anbazhagan, N. (2018). FNC/MobiSPC - A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM. *Procedia Computer Science*, *134*(NA), 365-370. https://doi.org/10.1016/j.procs.2018.07.197

[38]. Raman, R., & Pramod, D. (2017). A Strategic Approach Using Governance, Risk and Compliance Model to Deal with Online Counterfeit Market. *Journal of theoretical and applied electronic commerce research*, *12*(3), 13-26. https://doi.org/10.4067/s0718-18762017000300003

[39]. Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. N. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*, *9*(3), 74-NA. https://doi.org/10.3390/computers9030074

[40]. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International cybersecurity law review*, *3*(1), 7-34. https://doi.org/10.1365/s43439-021-00045-4

[41]. Sharma, K., & Mukhopadhyay, A. (2022). Sarima-Based Cyber-Risk Assessment and Mitigation Model for A Smart City's Traffic Management Systems (Scram). *Journal of Organizational Computing and Electronic Commerce*, *32*(1), 1-20. https://doi.org/10.1080/10919392.2022.2054259

[42]. Sillaber, C., Mussmann, A., & Breu, R. (2019). Experience: Data and Information Quality Challenges in Governance, Risk, and Compliance Management. *Journal of Data and Information Quality*, *11*(2), 6-14. https://doi.org/10.1145/3297721

[43]. Spanaki, K., & Papazafeiropoulou, A. (2016). The Implementation of Governance, Risk, and Compliance IS: Adoption Lifecycle and Enterprise Value. *Information Systems Management*, *33*(4), 302-315. https://doi.org/10.1080/10580530.2016.1220214

[44]. Suárez-Bárcena, Á., Braga, C. M., Santos-Olmo, A., & Fernández-Medina, E. (2024). Towards a Framework for Personal and Domestic Cybersecurity. *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*, 592-597. https://doi.org/10.1109/mass62177.2024.00094

[45]. Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, *148*, 104110-104110. https://doi.org/10.1016/j.cose.2024.104110

[46]. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, *11*(14), 2181-2181. https://doi.org/10.3390/electronics11142181

[47]. Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3), 103751-103751. https://doi.org/10.1016/j.im.2022.103751

[48]. Tjoa, S., Temper, P. K. M., Temper, M., Zanol, J., Wagner, M., & Holzinger, A. (2022). AIRMan: An Artificial Intelligence (AI) Risk Management System. *2022 International Conference on Advanced Enterprise Information System (AEIS)*, *NA*(NA), 72-81. https://doi.org/10.1109/aeis59450.2022.00017

[49]. Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, *83*(NA), 313-331. https://doi.org/10.1016/j.cose.2019.02.009

[50]. Vunk, M., Mayer, N., & Matulevičius, R. (2017). SPICE - A Framework for Assessing Organisational IT Governance, Risk and Compliance. In (Vol. NA, pp. 337-350). Springer International Publishing. https://doi.org/10.1007/978-3-319-67383-7_25

[51]. Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*(NA), 1-15. https://doi.org/10.1016/j.cose.2014.04.005

[52]. Widhoyoko, S. A. (2017). Fraud in Rights and Contracts: A Review of Bankruptcy Case of Livent Inc. Based on Governance, Risk, and Compliance (GRC) Framework. *Binus Business Review*, *8*(1), 31-39. https://doi.org/10.21512/bbr.v8i1.1827

[53]. Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security*, *88*(NA), 101636-NA. https://doi.org/10.1016/j.cose.2019.101636

[54]. Zahir, B., Rajesh, P., Tonmoy, B., & Md Arifur, R. (2025). AI Applications In Emerging Tech Sectors: A Review Of Ai Use Cases Across Healthcare, Retail, And Cybersecurity. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 16-33. https://doi.org/10.63125/245ec865

[55]. Zhang, P., & Kamel Boulos, M. N. (2023). Generative AI in Medicine and Healthcare: Promises, Opportunities and Challenges. *Future Internet*, *15*(9), 286-286. https://doi.org/10.3390/fi15090286