INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

The Role of IT Governance Risk and Compliance (IT GRC) in Modern Organizations

Adebayo Adeyinka Victor[1], Mubarak A Moronkunbi[2], Oyetunde Christian Oyedeji[3], Popoola Olusegun Victor[4], Shodunke Ajani Samuel[5]

[1]Electrical Department, University of Johannesburg, South Africa

[2]MuVio Solutions Ltd, Old Lagos Road Ibadan Oyo state Nigeria.

[3]BlueSky Citadel 193 Crayford Rd. London

[4]National Institute for Policy and Strategic Studies

[5]Baker Ripley, USA

DOI : https://doi.org/10.51583/IJLTEMAS.2024.130607

Received: 09 June 2024; Accepted: 15 June 2024; Published: 13 July 2024

Abstract: The study delves into the intricacies of IT Governance, Risk, and Compliance (IT GRC) in modern organisations, emphasising its significance amidst evolving regulatory landscapes and increased reliance on IT systems. IT GRC is an integrated framework combining IT governance, risk management, and compliance, ensuring alignment with business goals, mitigating risks, and adhering to regulations. The paper outlines the theoretical foundation of IT GRC and highlights the challenges and gaps in the current literature, underscoring the need for further research and understanding. It discusses the components and importance of IT GRC, illustrating how effective implementation enhances operational efficiency and reduces vulnerability to threats. Key frameworks such as COBIT and ISO 27001 are examined for their roles in establishing IT GRC standards. The study also explores the challenges in implementing IT GRC systems, recommending best practices for successful integration. Emerging technologies and future trends in IT GRC are analysed, projecting the domain's evolution in response to dynamic business environments. The research underscores modern organisations' need to adopt a holistic and integrated approach to IT GRC, aligning it with broader corporate governance to achieve sustainable performance and compliance.

I. Introduction to IT Governance Risk and Compliance (IT GRC)

The IT GRC constructs have attracted the attention of various stakeholders and have emerged differently in different societies despite social concerns regarding their importance (Sikdar, 2021; Zammit et al., 2021; Chergui & Chakir, 2020). Despite its emergence, the theoretical foundation of IT GRC is still immature. There are limited studies in the literature around IT GRC, with little debate from researchers and minimal argumentation on the relationship between its underlying constructs (Alharbi et al., 2022). Therefore, organisations might be concerned about implementing such a novel integrated concept without profound knowledge. Consequently, a research gap exists in understanding IT GRC as an integrated concept, with its theoretical foundation still needing to progress. The role of IT GRC in modern organisations and its management should be redefined. IT governance risk and compliance (IT GRC) is a novel integrated concept in modern organisations. It provides automated tools to deliver various frameworks to address associated risks, ensure security in IT systems, and efficiently implement and develop IT governance programs. IT GRC generally has three main interconnected disciplines (components): IT governance (alignment of IT with business, value delivery of IT, risk management in IT associated with business, resource management in IT, performance measurement of IT using a balanced scorecard); IT compliance (adheres to external laws, regulations, standards, internal company rules, policies, guidelines); and IT risk (assesses risk probability, risk impact, risk inherent, and develops risk response with control self-assessment)

Definition and Components

In their pursuit of meeting legal requirements, many organisations embrace implementing IT GRC. This approach ensures the accommodation of all regulatory requirements, which are increasingly complex and changing rapidly. The dynamism in these regulations stems from legislative bodies and international organisations continuously regulating corporate behaviour and information in more detail. The underlying reason for such legislative efforts is to promote organisational transparency and trust. It is widely recognised that the lack of an adequate approach towards GRC, or the lack of integration of GRC methods, insights, and technologies, may lead to operational inefficiency and increased threat, vulnerability, and compliance exposure. Therefore, the IT GRC approach, with its potential to enhance operational efficiency and mitigate risks, is becoming embedded in corporate thinking and operations.

IT governance risk and compliance (IT GRC) is a compound term consisting of three vital elements: governance, risk management, and compliance. In modern organisations, implementing these three elements concerning information technology is of utmost importance, and consultants, vendors, and scholars have provided extensive advice and guidelines for achieving an integrated view of those elements (Sikdar, 2021; Zammit et al., 2021). Governance is about the decision rights and accountability for decisions and actions associated with information technology. It constitutes the structure of rules and practices that guide and control IT capabilities and services. From an IT perspective, risk concerns the variability of IT outcomes and the possibility that conditions, events, or threats will materialise and affect

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

IT and IT-related business processes. Risk management can be utilised to balance company objectives with safeguards against loss or damage related to the use of IT. Compliance relates to the adherence to rules that originate from external entities. Those rules may come from legislation, industry standards, contracts, or internal organisational rules.

II. Importance of IT GRC in Organizations

At a corporate level, some boards or their delegated committees are currently responsible for overseeing the management of both the business and the IT. Their concern is reassurance that significant risks are being managed and that the organisation is operating effectively—to deliver reliable financial reporting, sustainable financial and business performance, and compliance with laws and regulations (Massicotte & Henri, 2021; Aspan, 2022). In modern organisations, where a considerable part of corporate compliance depends on IT controls, implementing frameworks such as ITIL and COBIT to govern IT processes becomes a board issue. The board must ensure that appropriate structures are in place and that delegations and authorisations are being observed. The board prefers to see a single 'control' organisation without overlapping controls, ensuring corporate and business compliance are addressed and coordinated by the design and operation of business processes. Furthermore, they would like to see 'risk management' as an integrating factor (as a link to making the governance risk connection at the enterprise governance level), encompassing business risk, compliance risk, and IT risk (Aboud & Yang, 2022; Hartmann & Carmenate, 2021). IT GRC has emerged from aligning three key organisational governance areas—IT governance, risk management, and compliance. The increasing requirements of laws, regulations, and industry standards that require strong supporting IT internal controls have cast the concept of IT GRC into the mainstream of corporate management. Today's business environment has transformed from the classical commercial world based on transactions to a world based on relationships, especially in a service context. Internally, the modern business has more of an identity through its corporate governance, encompassing a core of values and objectives that all the stakeholders understand and recognise. In this new business environment, IT GRC, to be beneficial, should be aligned and integrated with other relevant governance areas like corporate governance, enterprise governance, business process governance, and supply chain governance. IT GRC sits at the intersection of three organisational areas with particular governance functions (Kalsum, 2021).

Risk Management

Without apparent risk evaluation mechanisms, the company might be unable to detect external or internal threats to its development. For instance, compliance failures can negatively affect the corporation, reducing customer trust and resulting in substantial financial penalties (Chhetri, 2022). Therefore, the concept of compliance is related more to the internal rules established by the organisation, covering from the bylaws to the rules and procedures of each level of the company's structure, as well as the external laws and regulations identified within the same environment (Kuchma & Kotukh, 2023). Risk, compliance, and governance are complex areas that require a unique approach when connecting people, processes, and systems with rules and regulations. The strength of compliance controls is that they act as barriers preventing employees from carrying out inappropriate actions. Enforcing compliance through internal controls is a means of safeguarding corporate assets and ensuring accurate financial reporting. Risk is inherent in all activities of an organisation and should be managed in a planned and systematic manner. Therefore, risk management is identifying, assessing, and prioritising organisational risk as part of its governance function to manage and control any danger that could hinder the organisation in achieving its business goals (Makaš, 2023). In this context, risk management at a strategic level is enterprise risk management, but when related to the implementation and operation of information technology, it is IT risk management (Zammit et al., 2021). IT GRC encompasses IT governance, which helps make sure that the organisation's IT supports and realises its strategies and objectives and, in turn, enterprise governance; corporate governance, which focuses on fulfilling stakeholder expectations for broad organisational accountability and making sure of compliance with law and other requirements; and risk management, ensuring that IT risks are analysed and included in the organisation's enterprise risk context (Alharbi et al., 2022).

Regulatory Compliance

In conclusion, IT GRC is a framework that helps modern organisations achieve objectives while reporting operational rules to stakeholders and adapting to ever-changing regulations (Fischer et al., 2020). It benefits from established corporate governance proprietary frameworks like COSO and CoBIT. Government and industry bodies have established specific compliance requirements which regulate corporate governance, risk management, and control setting (Atmaja et al., 2022). Compliance with regulations involves meeting specific requirements sets and objectives. Compliance with different legislative environments is typically based on meeting control objectives and executing a set of specific controls. The question then becomes, "How can IT GRC be utilised in a practical manner to ensure rule-setting and control activities are properly designed into the corporate IT governance structure?" The upcoming section starts with a discussion of IT governance in general, followed by specific details of IT governance frameworks in section 3 and compliance in section 4. The paper then uses the details discussed to answer the above-posed question in section 5 and concludes in section 6. Regulatory compliance involves adhering to many laws, regulations, and industry standards that prescribe corporate governance, risk management, and control-setting rules. To enlist a few, regulators could include the Securities Exchange Commission (SEC), the Sarbanes-Oxley Act (SOX), Japan's Financial Instruments and Exchange Law (J-Sox), the European Union's 8th directive, and Novell Inc. (COSO and Co BIT). Industries have standards; the payment card industry (PCI) has a data security standard, health care has the Health Insurance Portability and Accountability Act (HIPAA), and the government has the Federal Information Security Management Act (FISMA). The essence of regulation is to establish specific control objectives and controls necessary to ensure organisations operate within established rule sets (Hu et al., 2021). The controlling bodies are specifically interested in designing,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

operating, and assessing control activities associated with IT and business-related processes. IT GRC combines several activities to operate within rules and objectives (Pererva et al., 2021).

III. Key Frameworks and Standards in IT GRC

Utilising the control objectives for information and related technology (Cob IT) framework, which is a different approach to IT governance, the IT GRC breakdown structure articulates the three IT disciplines, and the information flows between them, specific to managing performance and conformance in IT. The IT GRC breakdown structure addresses GRC integration along the GRC information flows between the three IT GRC disciplines. A limitation of the approach in the literature is the heavy focus on the internal information flows for internal IT GRC considerations and little attention to or information about the external information flows dealing with external service providers, who participate in the execution of IT processes, pose IT risks, and deliver IT GRC solutions. Solms proposes to link the Cob IT, ITIL, and CMMI frameworks with the IT GRC breakdown structure and incorporate GRC approaches to service level management and security in service provider-customer ecosystems. While IT GRC is a relatively new research topic, several key frameworks and standards already exist and provide guidelines to organisations concerning the three individual disciplines of IT GRC. Focusing on GRC in general, the GRC Capability Model (GRC-CM) provides a more integrated approach for GRC and was constructed based on the five attributes of any capability model: the scope of the enterprise, the goals, the competencies, the processes, and the performance dimensions. The GRC-CM identifies six high-level GRC process and capability domains that collectively match the enterprise's governance system, structured and matching governance mechanisms and related information that executive boards and executive management require and use to ensure that their collective GRC-related objectives are being achieved.

COBIT

COBIT provides a foundation for implementing IT-related standards, frameworks, and best practices. By using COBIT, an organisation can assess and measure performance using ISACA's performance measurement platform, linking people, skills, and IT resources in a systems environment using the Balanced Scorecard and in a highly automated environment using CMMI for Services (Thabit, 2021). Processes can be improved with COBIT and the assistance of the Val IT framework, and organisations can seek conformance or compliance with COBIT using Control Objectives for Sarbanes-Oxley (Almusawi, 2021). This aspect of COBIT integrates guidance available in other sources, setting a high level for control and governance activities. It provides more detailed guidance in the form of control objectives, management guidelines, and key indicators in the form of metrics to assess the success of both management and control activities.

Initially, COBIT was created as an IT control framework for the audit profession. It evolved with the joint stewardship of ISACA and the IT Governance Institute (ITGI) into a comprehensive framework addressing IT governance and enterprise governance from an IT perspective (Al-Fatlawi et al., 2021). As a governance framework, COBIT is described in "Governance of the IT-related Enterprise," providing a roadmap linking business goals/service requirements to IT goals, enablers (such as processes, policies, and IT resources), and the means to measure and balance IT performance. COBIT identifies business enablers necessary to provide business goal traceability for governing and managing enterprise IT (Alsaleem & Husin, 2023). COBIT business enablers are provided by domains executed by IT and supported by IT processes, influenced by enterprise goals and enabling enterprise stakeholder value objectives (De et al., 2020).

ISO 27001

The 27001 standard is not unique in the security field. Others exist, like COBIT and the IT Information Library (ITIL). Whereas COBIT is a control framework and does not provide comprehensive guidance on managing security, ITIL only addresses operational security (Fonseca-Herrera et al., 2021). ISO 27001 differs from COBIT in that it is less of a control framework and more of an ISMS standard, though the two could be used together. ISO 27001 has a broader security management scope than ITIL, which addresses only operational issues. ISO 27001 is also more process-oriented, whereas ITIL is more standards-oriented. ISO 27001, COBIT, and ITIL are not incompatible and can be implemented together, with each standard or framework addressing its specific coverage area at the appropriate level of detail (Al et al., 2020).

ISO 27001 is an Information Security Management System (ISMS) standard that addresses critical areas of information security: key security management responsibilities, security policy, organisation of information security, asset management, access control, cryptography, physical and environmental security, security of information systems, security operations, security for suppliers, customers, and third-party services, incident management, business continuity, and compliance (Fathurohman & Witjaksono, 2020). Specific controls are identified in Annex A of the standard. An ISMS like ISO 27001 ensures that control security is integrated with other security dimensions such as security architectures, security processes, and security culture. ISO 27001 uses the Plan-Do-Check-Act (PDCA) model, which is expected for many management systems. Based on an organisation's objectives, it provides a systematic approach for integrating, implementing, operating, monitoring, reviewing, maintaining, and improving information security (Alexei, 2021). Organisations use the standard to demonstrate their commitment to information security (Aquino et al., 2020).

IV. IT GRC Technologies and Tools

There are many IT GRC tools that organisations can consider from both speciality vendors and broader business application vendors. These tools include configuration assessment tools, content management software tools (about IT standards and regulations), data protection tools (DLP), encrypted communications, endpoint security applications, identity and access management applications, IT risk management and analysis tools, IT service management tools, and security information and event management (SIEM) applications. The

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

use of specific IT GRC frameworks that combine tools from multiple vendors can also be incorporated, which can include common IT control objectives for the enterprise involved (Kjærvik, 2023) (Sanz & Zhu, 2021) (Antunes et al., 2022). Such control objectives are often built for enterprise and mid-market customers based on recognised GRC standards, which include COBIT, ITIL, COSO, ISO 17799, HIPAA/HITECH, and others used in the marketplace (Katuu, 2021). IT governance, risk, and compliance (IT GRC) require a set of prescriptive practices or policies to align IT with the enterprise's business objectives. IT GRC has three components: IT governance, risk, and compliance. IT governance ensures that investments in IT generate business value and that IT risks are managed. It is based on tools and technologies that provide decision-makers and policymakers with enterprise insight into IT health, performance, and risk, enabling more effective business. IT risk comes from the potential loss of information integrity, confidentiality, availability and services, and IT not performing. IT risk management relies on tools and technologies that help ensure that business executives have insight into the risk exposure associated with business and IT, allowing informed risk decisions across the enterprise. IT compliance is about using tools to automate the enforcement and implementation of IT GRC policy (Kwong & Pearlson, 2024).

GRC Software Solutions

Given the potential complexity of GRC environments and the range of specialist G, R, and C tools available, it is suggested that organisations take a phased approach to GRC systems implementation. Organisations can benefit from selecting a specialised GRC system that facilitates integration in the longer term and investing in a vendor's ecosystem. It is possible to start with a basic system that can be rapidly implemented low-costly and expanded as experience is gained and requirements grow (Norimarna, 2021). The increasing importance of GRC disciplines has led to considerable investment in GRC software solutions. These solutions support particular aspects, such as industry requirements or the different methodologies within the G, R, and C components. The design of software supporting GRC can be considered from two perspectives. First, tools can be developed to support and apply the frameworks and methodologies within G, R, and C separately, recognising that each area has different established management processes and organisational structures. Second, there is the challenge of achieving integration between the separate G, R, and C tools concerning data, workflows, and reporting, given consistent feedback as to the governance of the actual state of risk and compliance within an organisation (Abdurrahman et al., 2024) (Cu et al., 2023) (PUDJIANTO, 2021).

V. Challenges and Best Practices in Implementing IT GRC

Implementing IT GRC (Information et al., and Compliance) systems presents significant challenges, often leading to redundancy and inefficiency at high costs. A major challenge in GRC information systems is correctly allocating resources to ensure critical real-time GRC activities are not overwhelmed by irrelevant data from ineffective controls. This challenge is central to the risk management pillar of GRC. Recognising that not all risk events are equal—some have catastrophic consequences while others are negligible, and existing contingency plans cover many—is crucial. Sufficient governance resourcing is essential to make these judgments and escalate risk events as necessary (Adisuria & Jayadi, 2023; Mahendra et al., 2022).

Common Challenges and Pitfalls

One of the primary issues is the inconsistent reporting of information. Different departments or business units often have unique ways of understanding concepts driven by their specific business goals, knowledge, and risk appetite. This inconsistency can manipulate risk information to suit specific needs, hampering the risk assessment. Ensuring a consistent definition of risk and a standardised reporting structure can significantly enhance risk assessment (Madkhali & Sithole, 2023; McIntosh et al., 2023). Common challenges and pitfalls in implementing IT GRC include hidden costs, inconsistent reporting, adopting the wrong framework, overlooking organisational culture, treating a GRC tool as a silver bullet, and not clearly defining roles and responsibilities. Hidden costs, such as customisation of IT systems, professional consulting services, additional staffing needs, and the time required from employees and management, often make the reality of GRC implementation differ significantly from initial perceptions (Butler et al., 2023; Manhart et al., 2020).

At the governance level, achieving stakeholder buy-in and business alignment is critical. IT secondary governing bodies often lack input into business objectives, limiting their decision-making capability. The challenge is customising IT governance frameworks like COBIT and ITIL to provide a coherent enterprise view of crucial IT risk and performance indicators relative to business processes. Customising such frameworks is crucial and complex, underscoring the importance of IT governance (Keith et al., 2022; Faulkner et al., 2020). Addressing these challenges requires recognising the intricate relationship between governance, risk management, and compliance and ensuring stakeholder alignment and efficient resource allocation. Best practices include standardising risk definitions, adopting appropriate frameworks, understanding organisational culture, clearly defining roles, and planning for hidden costs to ensure successful IT GRC implementation (Eling et al., 2021; Boiral et al., 2020).

Best Practices for Successful Implementation

Custom viable solutions—To ensure that GRC—related objectives are achieved, a range of organised capabilities that together provide tailored governing structure, managing processes, and enabling entity behaviour must be employed. GRC should specify decision rights and promote desired behaviours.

Appropriate oversight—GRC activities require appropriate monitoring and reporting at different levels within the organisational structure to ensure effective compliance and proper risk management.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

Competent personnel—People at all organisational levels must be competent in assessing and addressing GRC-related activities. Roles and responsibilities should be clearly defined and understood, and sufficient training and awareness should be provided.

Effective communication—Timely, accurate, relevant, and consistent upward and downward communication that addresses governance, risk, and compliance activities between senior management and other organisational levels must be established and effectively maintained.

Policies and standards—Well-defined, documented, and widely disseminated policies and standards that address governance, risk, and compliance requirements must be developed, and related guidance norms, rules or other criteria informed by relevant authorities adopted to drive desirable behaviour throughout the organisation.

Clear direction from senior leadership—A clearly defined and effectively communicated mission and vision regarding governance, risk, and compliance requirements is essential to ensure alignment and support an appropriate and consistent organisational culture.

An integrated view—Organizations must recognise the interrelationships of governance, risk, and compliance activities and adopt a holistic, integrated approach to address them properly and effectively.

Based on its extensive and successful experience, ISACA provides clear and valuable guidelines for an effective IT GRC implementation, including:

VI. Future Trends in IT GRC

Over the short term, the increased diversity of solution delivery will stress vendors relying on a single solution model. Business leaders continuously make choices and take actions regarding risk, compliance, and security, integrating these decisions into daily operations. Large organisations are adopting IT GRC platforms, often starting with a single component, such as Compliance, and gradually expanding to other components. The average time to expand platform utilisation is around six years, while the selection process takes about five months. SaaS (Software as a Service) is emerging as a preferred model, with vendors and implementation partners demonstrating SaaS maturity benefiting the most (Apeh et al., 2023; Chakir et al., 2020). The IT GRC domain is evolving, encompassing Enterprise and Operation Risk Management (ORM), Compliance Management, and Security Management. Over the next five years, significant trends include broader and deeper GRC platform penetration, the convergence of ORM, Compliance, and Security components, increased sophistication of GRC platform components, and a shift towards diverse business models, particularly SaaS (Kjærvik, 2023; Sikdar, 2021).

Emerging Technologies and Their Impact

Enterprise IT is crucial for business and societal progress and deeply integrates into our behaviours and operations. Managing IT effectively is vital for business and public sector success. Emerging technologies enhance service and product delivery but also increase associated risks. IT governance must support corporate objectives while safeguarding assets, making sound investment decisions, and optimising risk management. Coherent IT governance, part of overall corporate governance, requires shared goals, sound structures, and collaborative decision-making processes (Chhetri, 2022). Emerging technologies can substantially impact enterprise activities, posing both risks and opportunities. Effective management of these technologies depends on insight, foresight, and mature decision-making before and after transformative initiatives. Modern organisations recognise the importance of integrating IT with business goals, facilitated by sound IT governance principles. Managing business and IT aspects is central to IT GRC practices (Kravariti & Johnston, 2020; Lapuente & Van de Walle, 2020; Neumann et al., 2024; Di et al., 2022).

VII. Conclusion

Modern organisations find themselves operating in a generally frantic and fast-moving corporate environment. They benefit from various factors that help them succeed and improve their performance. The enablement and support provided by information technology (IT) are crucial and widely accepted factors. Modern organisations are subject to many regulations, standards, and laws that aim to ensure that organisations act responsibly concerning their stakeholders. Compliance with these rules is mandatory, and many consequences result from non-compliance. Failure to achieve compliance may result in organisations being prevented from activity, significant financial losses, or loss of reputation. However, as individual management disciplines, governance, risk, and compliance (GRC) do not provide a sufficiently holistic view and guidance concerning aligning and supporting IT-related matters to accomplish corporate objectives. IT GRC enables the alignment of corporate governance with IT governance, allowing modern organisations to operate in a coherent and coordinated way across different functions and levels, addressing the key issues, constraints, and risks that affect the achievement of corporate objectives. This contribution is increasingly acknowledged and recognised in academic and professional arenas from various fields with different focuses. As a result, the body of knowledge related to IT GRC, although fragmented at present, is becoming more consolidated and increasingly extensive.

References

1. Sikdar, P. (2021). Strong Security Governance Through Integration and Automation: A Practical Guide to Building an Integrated GRC Framework for Your Organization. [HTML]

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

2. Zammit, C., Grima, S., & Kizilkaya, Y. M. (2021). A Maturity Evaluation of Governance, Risk Management and Compliance (GRC) within the Maltese Public Sector. In Contemporary Issues in Public Sector Accounting and Auditing (pp. 219-255). Emerald Publishing Limited. [HTML]
3. Chergui, M., & Chakir, A. (2020). IT GRC smart adviser: Process driven architecture applying an integrated framework. Advances in Science, Technology and Engineering Systems, 5(6), 247-255. researchgate.net
4. 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). academia.edu
5. Chhetri, I. T. (2022). Cybersecurity and governance, risk and compliance (grc). Australian Journal of Wireless Technologies, Mobility and Security, 1. researchgate.net
6. Kjærvik, S. B. (2023). Utilization of ServiceNow's Risk Management Functionality Within the GRC Module: A Case Study. ntnu.no
7. Michelberger, P., & Kemendi, Á. (2020). Data, information and it security-software support for security activities. Problems of Management in the 21st Century, 15(2), 108-124. semanticscholar.org
8. Massicotte, S. & Henri, J. F. (2021). The use of management accounting information by boards of directors to oversee strategy implementation. The British Accounting Review. [HTML]
9. Aspan, H. (2022). Ocdy Amelia, William Lam (2022). Re-Appointment of Directors and Commissioners in the Same Position in a Limited Liability Company. Sch Int J Law Crime Justice. saudijournals.com
10. Aboud, A., & Yang, X. (2022). Corporate governance and corporate social responsibility: new evidence from China. International Journal of Accounting & Information Management, 30(2), 211-229. port.ac.uk
11. Hartmann, C. C. & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. Current issues in auditing. [HTML]
12. Kalsum, U. (2021). Factors affecting the disclosure of corporate social responsibility. International Journal of Business Economics (IJBE). umsu.ac.id
13. Kuchma, O. & Kotukh, Y. (2023). INSTITUTING A ROBUST RISK MANAGEMENT FRAMEWORK FOR THE STATE-OWNED IT GOVERNANCE. Матеріали конференцій МЦНД. mcnd.org.ua
14. Makaš, A. (2023). Governance, risk and compliance frameworks applicability in the organizations. International Journal of Science and Research Archive. ijsra.net
15. Fischer, M., Imgrund, F., Janiesch, C., & Winkelmann, A. (2020). Strategy archetypes for digital transformation: Defining meta objectives using business process management. Information & Management, 57(5), 103262. sciencedirect.com
16. Atmaja, D. S., Fachrurazi, F., Abdullah, A., Fauziah, F., Zaroni, A. N., & Yusuf, M. (2022). Actualization Of Performance Management Models For The Development Of Human Resources Quality, Economic Potential, And Financial Governance Policy In Indonesia Ministry Of Education. iainptk.ac.id
17. Hu, X., Yan, H., Casey, T., & Wu, C. H. (2021). Creating a safe haven during the crisis: How organizations can achieve deep compliance with COVID-19 safety measures in the hospitality industry. International Journal of Hospitality Management, 92, 102662. nih.gov
18. Pererva, P., Kobielieva, T., Kuchinskyi, V., Garmash, S., & Danko, T. (2021). Ensuring the Sustainable Development of an Industrial Enterprise on the Principle of Compliance-Safety. Studies of Applied Economics, 39(5). ual.es
19. Thabit, T. H. (2021). The Impact of Implementing COBIT 2019 Framework on Reducing the Risks of e-Audit. Buhuth Mustaqbaliya. researchgate.net
20. Almusawi, I. G. (2021). Using COBIT Framework for Reducing the Audit Risks of Accounting Information Systems. Akkad Journal of Contemporary Accounting Studies. acefs.org
21. Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. Webology. webology.org
22. Alsaleem, E. A., & Husin, N. M. (2023). The Impact of Information Technology Governance Under Cobit-5 Framework on Reducing the Audit Risk in Jordanian Companies. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(2), 4. unirioja.es
23. De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, 125-162. [HTML]
24. Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. IAENG Int. J. Comput. Sci, 48(2), 213-222. researchgate.net
25. Al Faruq, B., Herlianto, H. R., Simbolon, S. H., Utama, D. N., & Wibowo, A. (2020). Integration of ITIL V3, ISO 20000 & iso 27001: 2013forit services and security management system. International Journal, 9(3). academia.edu
26. Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and design of information security management system based on ISO 27001: 2013 using Annex Control (Case Study: District of Government of Bandung City). Bulletin of Computer Science and Electrical Engineering, 1(1), 1-11. bcsee.org
27. Alexei, A. (2021). Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. Journal of Social Sciences. idsi.md
28. Aquino Cruz, M., Huallpa Laguna, J. N., Huillcen Baca, H. A., Carpio Vargas, E. E., & Palomino Valdivia, F. D. L. (2020, October). Implementation of an Information Security Management System based on the ISO/IEC 27001: 2013 standard for the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

information technology division. In The International Conference on Advances in Emerging Trends and Technologies (pp. 264-272). Cham: Springer International Publishing. [HTML]

29. Sanz, J. L., & Zhu, Y. (2021, September). Toward scalable artificial intelligence in finance. In 2021 IEEE International Conference on Services Computing (SCC) (pp. 460-469). IEEE. [HTML]
30. Antunes, M., Maximiano, M., & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. Applied Sciences. mdpi.com
31. Katuu, S. (2021). Trends in the enterprise resource planning market landscape. Journal of Information and Organizational Sciences. srce.hr
32. Kwong, J. & Pearlson, K. (2024). Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs. hawaii.edu
33. Norimarna, S. (2021, November). Conceptual Review: Compatibility of regulatory requirements of FSA to Insurance industry in Indonesia for Integrated GRC. In RSF Conference Series: Business, Management and Social Sciences (Vol. 1, No. 5, pp. 105-115). researchsynergypress.com
34. Abdurrahman, A., Gustomo, A., & Prasetio, E. A. (2024). Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. The Electronic Journal of Information Systems in Developing Countries, 90(2), e12299. [HTML]
35. Cu, M., Peko, G., Chan, J., & Sundaram, D. (2023). … -based Governance, Risk Management, and Compliance for Fractional Ownership: Design and Implementation of A Decentralized Autonomous Agent System. hawaii.edu
36. PUDJIANTO, W. (2021). Process mining in governance, risk management, compliance (grc), and auditing: A systematic literature review. Journal of Theoretical and Applied Information Technology, 99(18). researchgate.net
37. Adisuria, K. F., & Jayadi, R. (2023). Analysis Of The Implementation GRC Information System in Supporting Performance Optimization. Journal of Information System Management (JOISM), 4(2), 97-106. amikom.ac.id
38. Mahendra, I., Prabowo, H., & Hidayanto, A. N. (2022, August). Information technology challenges for integrated governance, risk and compliance (grc). In 2022 1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS) (pp. 79-84). IEEE. [HTML]
39. Madkhali, A. & Sithole, S. T. M. (2023). Exploring the role of information technology in supporting sustainability efforts in Saudi Arabia. Sustainability. mdpi.com
40. 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, 103424. sciencedirect.com
41. Butler, T., Gozman, D., & Lyytinen, K. (2023). The regulation of and through information technology: Towards a conceptual ontology for IS research. Journal of Information Technology, 38(2), 86-107. [HTML]
42. Manhart, P., Summers, J. K., & Blackhurst, J. (2020). A meta-analytic review of supply chain risk management: assessing buffering and bridging strategies and firm performance. Journal of Supply Chain Management, 56(3), 66-87. [HTML]
43. Keith, D. A., Ferrer-Paris, J. R., Nicholson, E., Bishop, M. J., Polidoro, B. A., Ramirez-Llodra, E., ... & Kingsford, R. T. (2022). A function-based typology for Earth's ecosystems. Nature, 610(7932), 513-518. nature.com
44. Faulkner, E., Holtorf, A. P., Liu, C. Y., Lin, H., Biltaj, E., Brixner, D., ... & Payne, K. (2020). Being precise about precision medicine: what should value frameworks incorporate to address precision medicine? A report of the personalized precision medicine special interest group. Value in Health, 23(5), 529-539. sciencedirect.com
45. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125. [HTML]
46. Boiral, O., Talbot, D., & Brotherton, M. C. (2020). Measuring sustainability risks: A rational myth?. Business Strategy and the Environment, 29(6), 2557-2571. researchgate.net
47. Apeh, A. J., Hassan, A. O., Oyewole, O. O., Fakeyede, O. G., Okeleke, P. A., & Adaramodu, O. R. (2023). GRC strategies in modern cloud infrastructures: a review of compliance challenges. Computer Science & IT Research Journal, 4(2), 111-125. fepbl.com
48. Chakir, A., Chergui, M., & Andry, J. F. (2020). A smart updater it governance platform based on artificial intelligence. risk. researchgate.net
49. Kravariti, F. & Johnston, K. (2020). Talent management: a critical literature review and research agenda for public sector human resource management. Public Management Review. researchgate.net
50. Lapuente, V. & Van de Walle, S. (2020). The effects of new public management on the quality of public services. Governance. wiley.com
51. Neumann, O., Guirguis, K., & Steiner, R. (2024). Exploring artificial intelligence adoption in public organizations: a comparative case study. Public Management Review. tandfonline.com
52. Di Vaio, A., Hassan, R., & Alavoine, C. (2022). Data intelligence and analytics: A bibliometric analysis of human–Artificial intelligence in public sector decision-making effectiveness. Technological Forecasting and Social Change, 174, 121201. e-tarjome.com