International Journal of Information Security (IJIS)
Volume 4, Issue 1, January-June 2025, pp. 69-97, Article ID: IJIS_04_01_004
Available online at https://iaeme.com/Home/issue/IJIS?Volume=4&Issue=1
ISSN Online: 2273-1307; Journal ID: 1230-2805
Impact Factor (2025): 8.50 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJIS_04_01_004

DATA SECURITY AND COMPLIANCE THROUGH EFFECTIVE DATA GOVERNANCE

Jude Osakwe, Iyaoo Haitula-Waiganjo
Department of Informatics
Namibia University of Science and Technology, Namibia.

ABSTRACT

This systematic literature review explores the critical intersection of data governance, security, and compliance within organizations amidst evolving regulatory landscapes and increasing data breaches. The research aims to identify effective data governance frameworks that ensure data security while adhering to compliance requirements. Utilizing a structured methodology, the review synthesizes findings from 53 relevant studies published between 2017 and 2024, highlighting key themes such as the importance of data stewardship, the role of data quality, and the integration of security measures into governance practices. The results indicate that inadequate data governance strategies can lead to significant risks, including data breaches and loss of stakeholder trust. Furthermore, the study reveals a lack of comprehensive understanding regarding the implementation of best practices in data governance and their impact on compliance outcomes. The findings underscore the necessity for organizations to adopt holistic data governance approaches that align security and compliance efforts, thereby mitigating risks associated with data management. This research contributes to the existing body of knowledge by providing a roadmap for practitioners and future researchers, emphasizing the need for ongoing collaboration between data scientists and ethicists to develop robust governance tools. Ultimately,

the study calls for further investigation into innovative data governance solutions that can effectively leverage data for business growth while ensuring security and compliance.

Keywords: Data Security, Compliance, Data Governance, Technology.

Cite this Article: Jude Osakwe, Iyaoo Haitula-Waiganjo. (2025). Data Security and Compliance Through Effective Data Governance. *International Journal of Information Security (IJIS)*, 4(1), 69-97.

https://iaeme.com/MasterAdmin/Journal_uploads/IJIS/VOLUME_4_ISSUE_1/IJIS_04_01_004.pdf

1. Introduction

Organisations have accumulated and continue to amass huge amounts of data, which often include sensitive and private information. At the same time, the regulatory environment has been overhauled, thus necessitating compliance with established rules (Pansara, 2022; Shahid et al., 2022; Pansara, 2022; Abbas et al., 2024). Security breaches have also brought data governance to the forefront, and it is now recognised as a critical factor contributing to the data protection lifecycle (Shahid et al., 2022; Pansara, 2022; Abbas et al., 2024). Setting up data governance is a continuous and iterative process where data quality, security, privacy, and access policy components come together (Abbas et al., 2024; Ahmad et al., 2022; Díaz-Rodríguez et al., 2023). Therefore, authorisations "by design" data governance, including "policies and practices and creating a systematic approach to data governance in an organisation," besides ensuring that data governance operations are authorisable, thus offering transparency and traceability (Pansara2022; Shahid et al., 2022; Pansara, 2022; Abbas et al., 2024; Ahmad et al., 2022; Díaz-Rodríguez et al., 2023).

A significant amount of literature has been written on the critical questions: "How can compliance and security be part of operations, and why is governance seen as an effective approach?" (Hamid et al., 2021; Fathi et al., 2022; Tandon et al., 2021; Kumar et al., 2021). It is also raised if a perception exists among the companies that consider governance frameworks and models, and further, what are the existing approaches, models, and solutions that offer a way of doing business closer to the standards? To present a structured view, this systematic literature review has been performed to analyse existing literature on data governance as a measure to ensure that data security can be managed in a way compliant with the rules (Hamid et al., 2021; Fathi et al., 2022; Tandon et al., 2021; Kumar et al., 2021; Di Vaio et al., 2021; Viljoen, 2021; Rathore et al., 2021).

1.1. Rationale

As the practice of maintaining the privacy and security of organisational data becomes increasingly data-driven and digitised, organisations are expected to develop and deploy rigorous data governance frameworks for ensuring compliance with emerging data security regulations. An inadequate governance strategy may result in data breaches, financial failure, damage to the company's reputation, and loss of customer and stakeholder trust (Abrahams et al., 2024; Nzeako et al., 2024). Continuous developments in digitisation and emerging data privacy regulations that specify strict punitive measures in case of non-compliance further draw attention to securing data and regulatory compliance (Abrahams et al., 2024; Nzeako et al., 2024; Yeung & Bygrave, 2022; Zhang et al., 2022; Adeniran et al., 2024).

Insufficiencies in most organisations' data governance practices to ensure compliance and to secure their data, prevent comparisons of typical practices available in the public domain. Researchers have a limited understanding of how data governance practices improve regulatory compliance outcomes or avert data breaches (Pansara, 2023; Balasubramanian et al., 2024; Yallop et al., 2023). Despite the publication of data governance best practices, researchers have not yet found how widely these best practices are implemented in organisations, and if adherence to compliance practices reduces the likelihood of breaches (Yallop et al., 2023; Arabsorkhi & Khazaei, 2024; Duggineni, 2023; Tariq2024; Pansara, 2022; Pansara, 2021). Ensuring data security and compliance are the main activities of the robust data governance model. Emphasis on them is crucial as the volume and complexity of data processing operations are sharply increasing and organisations require an approach to target resources managing privacy and security risks associated with data processing.

2. Understanding Data Governance

Data governance is a critical process for ensuring the reliability of data moving through an organisation (Viljoen, 2021; McGilvray, 2021; Hamid et al.; 2021; Halchenko et al., 2021). It is designed to manage and maintain the trustworthiness and security of the data, and it is designed, in part, to ensure the organisation's compliance with laws and regulations (McGilvray, 2021; Hamid et al.; 2021; Halchenko et al., 2021). Data governance is a framework that combines strategies, guidelines, and rules that have been developed collectively with all the stakeholders so that they reflect a common vision and strategy promoting data integrity, security, and privacy (Viljoen, 2021; McGilvray, 2021; Hamid et al.; 2021).

Data governance addresses the way data and information are stored, managed, and maintained. It promotes simple and clear organisational processes and an effective organisational framework. It is about ensuring compliance with the existing policies and frameworks while maintaining data privacy, confidentiality, and protection to minimise data breaches, as well as ensuring complete accessibility to authorised individuals (Halchenko et al., 2021; Spanaki et al., 2021). It focuses on the information assets, guiding in terms of information business purposes, policies, standards, and the latest technologies. It is central in maintaining good corporate governance and providing responsiveness to the stakeholders, particularly customers, shareholders, and regulatory institutions (Deepa et al., 2022; Miyachi & Mackey, 2021).

Data security and compliance are essential practices to affect data governance, to reduce the service processing risk and achieve service optimisation (Viljoen, 2021; McGilvray, 2021; Hamid et al.; 2021). A holistic approach in data management is necessary to guarantee the identified roles and framework for efficient operation, governance, regulation, and monitoring (Halchenko et al., 2021; Spanaki et al., 2021; Deepa et al., 2022; Miyachi & Mackey, 2021)

2.1 Conceptual Framework

Data governance, security, and compliance are ways to protect data, mitigate risk, and meet regulatory and organisational expectations, which are visually presented in a conceptual framework (Pansara, 2023; Sun et al., 2021; Bandari, 2023; Pansara2022; Yallop et al.2023). This framework serves as the hypothetical basis of the literature review. It links the concepts of data governance, security, and compliance, reflecting the close relationships between these elements. This framework identifies that organisational factors and governance objectives should be used to inform data security and compliance practices and guide the implementation of any tools used to facilitate security and compliance. It serves as the starting point for discussions of data governance practice and research around data governance.

Data security includes protecting against unauthorised access, changes to, or destruction of data. Compliance refers to ensuring that relevant laws, regulations, or organisational policies and procedures are met (Akhtar et al., 2021; Duggineni, 2023; Dastres & Soori, 2021). It is becoming apparent from investigations that it is inappropriate to discuss each of these concepts in silos; indeed, successful practice requires that they are discussed in the same sentence. This is because, in practice, the relationship between security and compliance is deeply rooted; many of the security controls applied to data are employed in an attempt to satisfy regulatory and legal requirements, and many compliance efforts focus on the efficacy of security measures as implemented (Duggineni, 2023; Dastres & Soori, 2021; Al-Harrasi et al., 2023; Vegesna,

2021). This implies that organisations must understand the issues associated with security and compliance and be able to tackle them by focusing on the creation and/or enforcement of relevant policies to guide employee behaviour. The theoretical links between data governance, security, and compliance are needed to ensure that the definitions of these concepts provide a context for the discussion of practice (Bandari, 2023; Akhtar et al., 2021; Duggineni, 2023; Dastres & Soori, 2021; Al-Harrasi et al., 2023; Vegesna, 2021)

2.2.1. Data Security

Data security is seen as an essential protection policy to ensure that organisation's goals can be met with the best business data (Brown & Marsden, 2023;m Fernandez, 2022; Ahmad et al., 2021; Uchendu et al., 2021). Data security starts with assessments and decisions based on potential risks. As a result, appropriate protective actions can then be implemented. Data security is generally dominated by internal and external threats that exist both temporarily and intentionally (Brown & Marsden, 2023; Fernandez, 2022; Ahmad et al., 2021; Uchendu et al., 2021; González-Granadillo et al., 2021)

The risk of data security is also serious because the loss of sensitive information can have severe negative consequences with international laws and regulations for an organisation. It is estimated that the cost of a data security violation was significant in recent years (Ismagilova et al., 2022; Li & Liu, 2021; Thapa & Camtepe, 2021; Dutta & Fischer, 2021; Aslan et al., 2023). Data security is significantly improved by training employees to be proactive in ensuring data privacy protection. In an organisation, data security is largely regulated by the data security policy, which is integrated into authorised standards and guidelines (Li & Liu, 2021; Duggineni, 2023; Butler et al., 2023). Moreso, the latest technology patterns that shape current data security practices are now more detailed. Ensuring data privacy is a necessary part of safe data governance. Data security policies must be continuously developed and sustained at numerous levels in any organisation. Organisations can sometimes adhere to certain regulations or laws, or respect business requirements. There are a number of international norms and directives identifying the need for various areas of world government participation in applying security restrictions to prevent data security failures (Karale, 2021; Zhang & Zhang, 2023).

2.2.2. Compliance

Effective data governance processes support an organisation's ability to achieve strategic objectives, operational goals, and individual mandates on a day-to-day basis (Bany et al., 2022; Al-Okaily et al., 2023; Kulkov et al., 2024; Aljumah et al., 2021). Data governance has been expanded to include data stewardship and data quality as essential mechanisms.

Stewardship involves identifying who has the ultimate responsibility and decision-making for data, determining what is the optimal level of control to properly manage and own data, and providing protection to data for the stewardship of the governance framework. The steward framework also includes workflow activities for the offset of master data, as well as data stewardship organisations to work together and manage data processes. Data quality relies on the extension of stewardship by linking data quality to data standards-related processes, monitoring data value, grammar, and structure. (Bany et al., 2022; Al-Okaily et al., 2023; Kulkov et al., 2024; Aljumah et al., 2021; Khan et al., 2022; Ahmad et al., 2022; Chen et al., 2021; Ashaari et al., 2021)

In addition to stewardship, data security and privacy have been raised to a broader level of importance for data governance. Data security generally includes steps taken to protect data from unauthorised access, data breaches, or corruption, while data privacy focuses on ensuring that only the authorised parties have access to the data (Komljenovic, 2022; Thapa & Camtepe, 2021; Michel-Villarreal et al., 2023). Data privacy also addresses privacy issues at the individual level, which must be in compliance with legislative or industry standards, and it emphasises individual details and library functions in the organisation as well.

Among data management services, data security and privacy data handling also includes data security and privacy field-level control, data scrambling, key rotation, and data security capability (Da Xu et al., 2021; Núñez-Canal et al., 2022; Abdelmaboud et al., 2022; Thach et al., 2021). Data governance has also focused on maintaining legislative and regulatory rules to provide data security and compliance. Data quality and rules are replicated from the synthesis rules, as the data quality guidelines originated from the entity structure of the record, the record file sise, the integrity principle level, the mandatory constraints, the dynamic defaults, the default values of the constraints, and permissible multi-domain values (Komljenovic, 2022; Thapa & Camtepe, 2021; Michel-Villarreal et al., 2023; Huang et al., 2023).

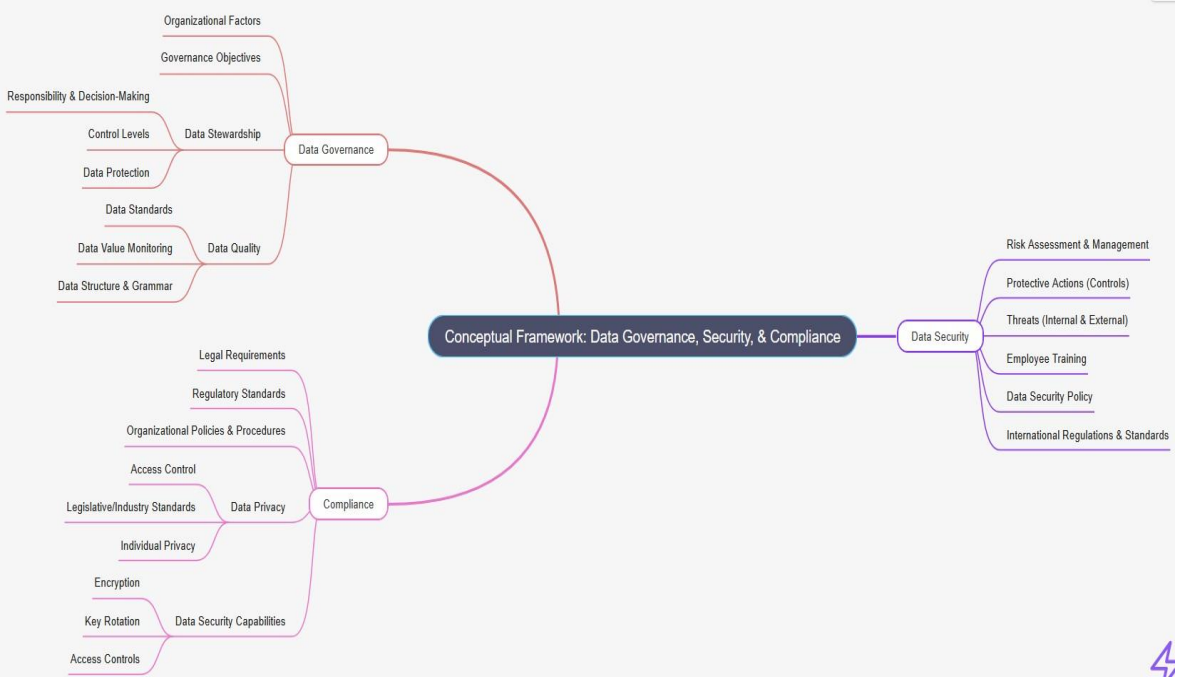

Fig 1: Conceptual framework of Data governance, security, and compliance

3. Data Security and Compliance

Data security and compliance are often used interchangeably to describe the protection, confidentiality, integrity, and availability of an organisation's data. This definition encompasses awareness, adherence to industry regulations and standards, and internal governing policies or procedures that an organisation sustains (Chiara, 2021; Pleger et al., 2021; Taherdoost, 2022; Nowrozy et al., 2024). Many regulations, standards, and internal organisational policies, laws, and contracts require a level of data protection and privacy. The extent of data security and privacy principles can result in significant business risks when controls are not designed and used (Pleger et al., 2021; Taherdoost, 2022; Nowrozy et al., 2024).

The number of reported cases of data breaches is constantly growing, resulting in significant financial losses for the affected organisations. Noncompliance with internal policies, industry standards, and government regulations also results in heavy penalties and drawbacks for the business. To control these risks, organisations implement data security, data privacy, and compliance control objectives, practices, policies, standards, and procedures. Conrad, 2022; McLeod & Dolezel, 2022; Kitsios et al., 2023)

A data governance community ensures that the capabilities to define, produce, and operate data and information artifacts are reinforced. The habit of performing governance tasks makes it easier to resolve related operational, compliance, and security issues, leading to

improved compliance with policies. The close alignment of the three disciplines aids the task of coping with the growing regulatory burden on a uniform and integrated basis. (Viljoen, 2021; Carroll et al., 2023; Ahmad et al., 2022; Aldoseri et al., 2023; Aoun et al., 2021; Spanaki et al., 2021, Carroll et al., 2021)

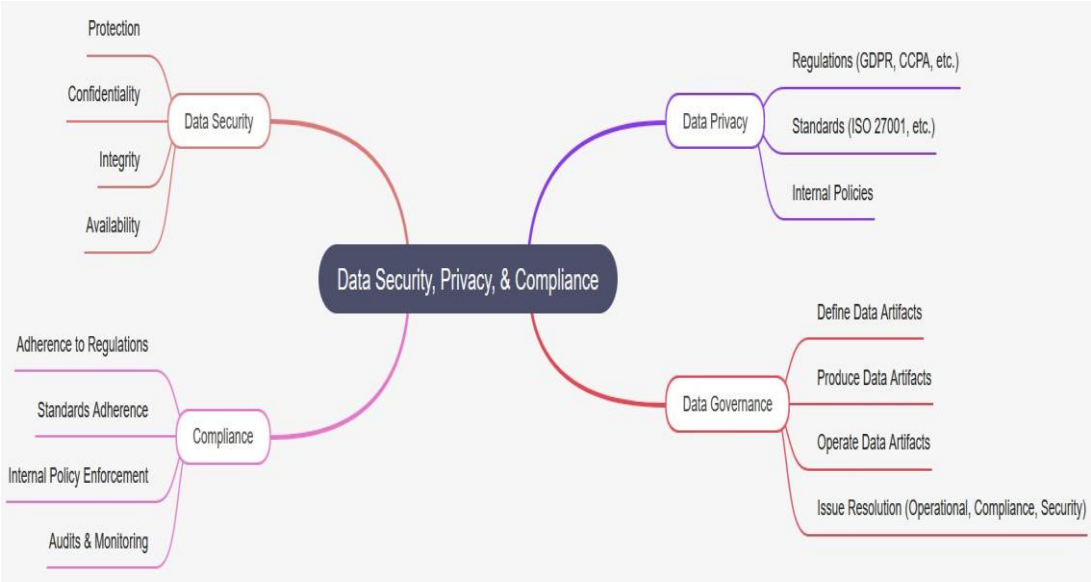

Fig 2: Data Security and Compliance

4. The Intersection of Data Governance, Security, and Compliance

For the purposes of this review, security in a governance context is defined as the ability of an organisation to protect itself from unauthorised access or malicious attacks that could lead to data breaches, data loss, or significant business disruption. Compliance is the extent to which the organisation remains consistent with external laws, regulations, or a spectrum of standards that exist in order to govern behaviours or manage risks of the organisation, e.g., risk management standards, standards for privacy, and information security standards (Telo, 2023; David et al., 2022; Sun et al., 2021; Kure et al., 2022; Bondarenko et al., 2022; Vyas, 2023).

The need to understand and manage personal information held by an organisation has given rise to regulatory requirements in the form of data privacy standards. When this data pertains to citizens of another country, the regulatory environment may include mandates to store data in the country of origin, reduced ability to move data between countries, and the application of laws related to the laws in the country where the data originated (Thapa & Camtepe, 2021; Truong et al., 2021; Andrew & Baker, 2021; Gray et al., 2021). Such requirements are common. In addition, the risks posed to personal safety, health, sustainable

economic well-being, racism, and other forms of humanity's greater good raise the dimension and severity of data misuse exponentially (Andrew & Baker, 2021; Gray et al., 2021; Almeida et al., 2022; Quach et al., 2022; Chawla & Kumar, 2022). The good news is commercial and government organisations have a significant market replete with consultants to address data privacy and to receive external certification of their compliance with any privacy standard that has been accepted as international law. (Thapa & Camtepe, 2021; Truong et al., 2021; Andrew & Baker, 2021; Gray et al., 2021; Almeida et al., 2022; Quach et al., 2022; Chawla & Kumar, 2022).

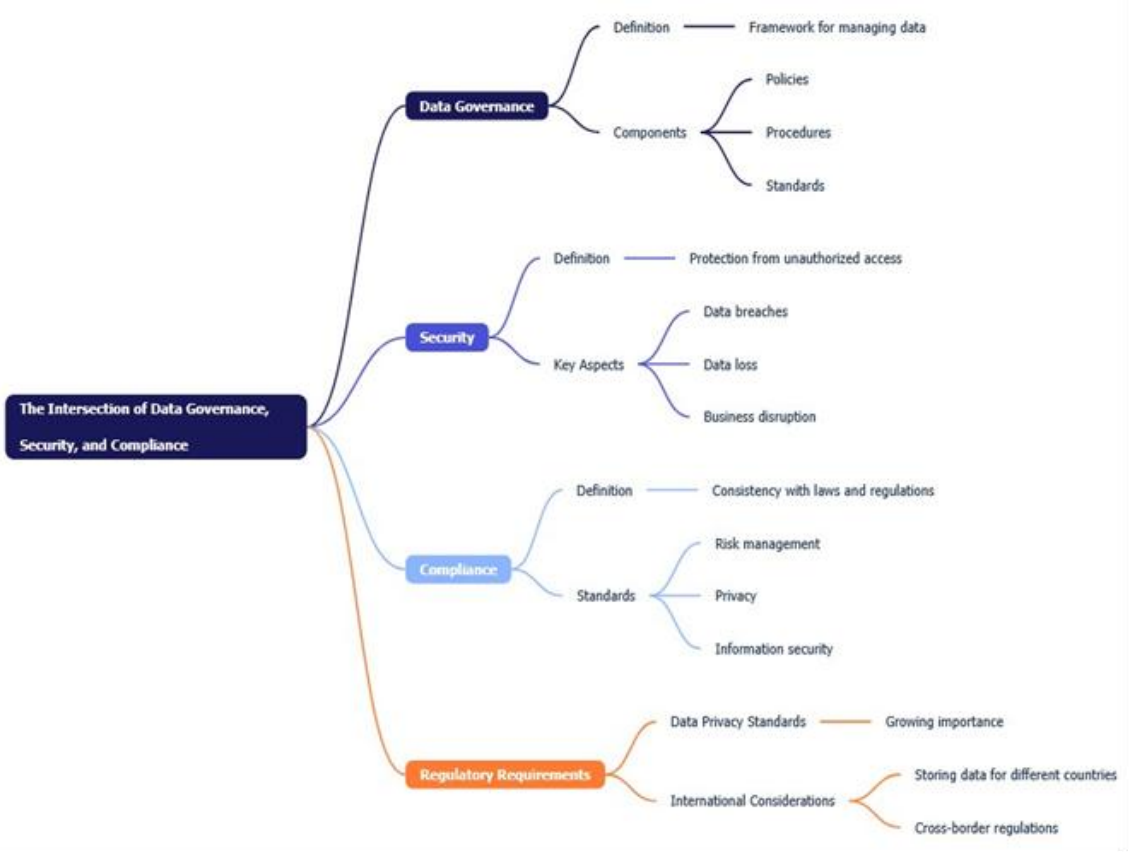

Fig 3: Intersection of Data Governance, Security, and Compliance

4.1. Key Principles and Strategies

Data governance, security, and compliance frameworks often coexist in many organisations but remain unaligned in practice. Several principles and strategies can be used to coordinate the complex issues of data availability for analysis, the protection of sensitive data, and compliance with laws and regulations (Nguyen & Tran, 2023; Mao et al., 2022; Jarvenpaa & Essén, 2023). These principles entail the use of accountability mechanisms, transparency for data access, ongoing improvements to data governance, and organisational knowledge of

regulatory requirements (Jarvenpaa & Essén, 2023; Solomonides, 2023; Farhad, 2024; Obendiek, 2023). Strategies allow firms to create organs of authority, establish policies based on professional practices, provide resources for compliance such as reports and user permission tracking, and services such as training and access requests. Best practice in evaluation also suggests the development of monitoring through data quality and data management practices and the use of performance indicators, audits, and expert feedback for data security and privacy. (Nguyen & Tran, 2023; Mao et al., 2022; Jarvenpaa & Essén, 2023; Solomonides, 2023; Farhad, 2024; Obendiek, 2023).

Data security and compliance can be successfully integrated if the integrated strategy for building a data governance framework addresses data protection and analytics issues. For this to happen, top management should commit to a risk management approach to ensure their information security becomes an integral part of business security and drives a data compliance transformation. Engaging users and stakeholders to shape these changes, organise and run effective communication strategies to ensure successful compliance strategies is a must. Systematic monitoring for meaningful, useful, and sustainable results ensures a return on investment (Pansara, 2023; Zhang et al., 2022; Pansara, 2022). One of the success cases revealed that the strategy used enables compromise where data custodians believe their data are at an acceptable risk and the receiver is able to demonstrate reasonable compliance when they use the data (Pansara, 2023; Zhang et al., 2022; Pansara, 2022; Duggineni, 2023; Ahmad et al., 2022).

5. Methodology

The present SLR adheres to the guidelines of a specific protocol for conducting such a type of review. By considering the best practices proposed, the study aim to produce a process that will guide both future researchers within the IS research field and practitioners who may rely on these reviews to support decision-making. It is believed that the questions used to guide the SLR process serve as critical-to-quality characteristics that provide a solid foundation to guide the planning, execution, and review of this type of literature.

The research team started by defining the research objectives and the scope of the review, as well as the research questions to be answered. Then, the search process was performed. The selection process was carried out in two stages. First, the titles and abstracts of the papers identified in the search were screened against a set of inclusion and exclusion

criteria. Included papers proceeded to the next stage, where their full texts were read. Studies that were deemed relevant and met the quality criteria were included in the data-analysis phase of the review. The research team carefully examined the results, and finally, the reporting of the results was described.

Table 1: Methodology

Stage	Description
1.Research Objectives	Define research objectives, scope of review, and specific research questions
2. Search Process	Conduct systematic search for relevant papers
3. Initial Screening	Screen titles and abstracts using inclusion and exclusion criteria
4. Full Text Review	Read full texts of selected papers and assess quality
5. Data Analysis	Carefully examine and analyse selected studies

5.1. Literature Search Strategy

A systematic literature review (SLR) is an essential evidence-based method to provide authoritative answers to specific research questions or catalyse problem understanding in one domain when results are scarce. The quality of term identification is the first preliminary step to conduct a successful SLR. For the research purpose of pinpointing the investigative potential issues, focusing on the major research themes, and distinguishing classified literature associated with data governance, an SLR was chosen as the prime research method to recognise comprehensive research gaps and decode further research scopes. A comprehensive literature search has to be systematic and confirmable, but also keep a high recall ratio to gather enough primary literature concerning the research topic. Even though SLR is used primarily in the field of software engineering, it is starting to be used in other management and business research. Therefore, in order to associate the research population with the most recent literature, the major databases have to be screened to form potential research priorities.

5.2. Inclusion and Exclusion Criteria

The Inclusion and exclusion criteria was established and refined in the early stages of the review. The study began by discussing which studies in the extant field were relevant, theoretical, and applied, and whether work in progress papers should be included, practitioner

publications, and so forth. Other inclusion factors used include the contributions of the individual studies to the field. Studies excluded at this stage were those that did not meet one or more of the following criteria as established through the consensus and discussions of the four authors: - Empirical research being reported in the text - A summary of a theoretical debate.

This was intended to obviate the risk that the inclusion criteria might too rigidly preclude otherwise important work from contributing to the systematic literature review. Once that phase was completed, the results were collated and an overview of the studies was generated.

Table 2: Inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
• Empirical research • Theoretical studies • Applied research • Significant contributions to the field	• Non-empirical research • Lack of substantial theoretical debate • Minimal field contribution • Work in progress papers • Practitioner publications without rigorous research

5.3. Data Extraction and Synthesis

To address the research questions identified in the study carried out a systematic literature search to collect papers that are related to data security, compliance, and data governance. Given a relatively moderate number of papers that were returned by the initial search, manual extraction of relevant publications was performed. The study further included papers that were cited by some of the manually extracted relevant works to bolster the number of papers included. A citation network was built based on the cited relationships among the papers that were manually collected. After an exhaustive manual extraction procedure, a total of 53 unique papers were eventually included in the review.

Guidelines were followed to conceptualise, extract, and synthesise relevant data reported in the included papers. The abstract, keywords, and author-supplied keywords fields of each paper were used to identify the aim of the paper and its main contributions. The study also used the methods section of the papers to determine the research approaches commonly used in the context of our study. In addition to content analysis, a citation analysis was also conducted to identify the papers that are most frequently referred to in the context of our study. By performing both types of analyses on the papers, the study gained insights into the cumulative knowledge and the underlying structure of the context of our study.

6. Findings and Analysis

The goal of this review is to provide an overview of the existing literature and research on data governance and to justify the importance of applying data governance practices in an organisation to meet regulatory requirements and other market demands, by using a selection of titles and fields of interest relating to data governance and its beneficial purposes. This study has begun by identifying the most relevant and highly cited papers ranging from the year 2017 to 2024. The review of papers has been carefully studied to unearth five key areas of data governance that many scholars have researched.

The study is significant for both practitioners in the industry and future researchers who wish to contribute more literature on data governance. One of the most significant results from this study is to assist practitioners and offer a stepping stone to comprehend the experiences of implementing data governance in terms of ways to provide data security and compliance. This systematic literature review aids in developing the roadmap, which is highly crucial before embarking on a data governance journey.

This study focused on information and technology, business management, and social sciences papers, identifying 37 papers for further literature review. The research analysed and presented the concepts, stakeholders, and domains involved in the data governance literature, in addition to proposing an integrated model of data governance driven by leadership, data capacity, and data governance intermediaries. This study is the first major review of the data governance literature to analyse the trends in different areas and the relationships between these trends and to suggest important directions for future research.

7. Trends

The major findings on research focus over the last 15 years could be summarised as follows. First, the study seems to indicate that the total published articles have been increasing exponentially in this research area and that the main publishing outlets are prominent journals. According to findings, one can easily identify four periods of time where the number of recovered research papers has increased. These periods have 2-year boundaries: 2008-2009, 2011-2012, 2014-2015, and 2017-2018. Consequently, in the last two occasions, there has been an increase of 47% in published documents in comparison with the previous sets. Furthermore, using the exponential model, future evolution could reach 35 papers at 4-year intervals by 2026. Second, regarding the trend of published papers by each kind of document, one should note

that research articles are the most popular in this area; however, the second-best option is the conference paper. As a matter of fact, this research has been enriched by a significant number of conference papers. In comparison, literature reviews, book chapters, theses, and editorials/short communications are scarce and irregular throughout this analysis.

Third, using a term map, the study determines the relevance of major keywords and understand the research progress in terms of keywords. As a result, the Relevancy Algorithm highlights four main themes regarding the frequently and extremely searched keywords over time. These themes correspond to four sets that are mainly composed based on the extraction from the titles, keywords, abstracts, author key terms, and keywords provided by the journals or the academic publishing repositories. Fourth, a critical assessment of the chronology, methodological design, and analysis of each paper allows us to distinguish two significant periods of research focus: before and after 2024. In other words, before the year 2024, researchers concentrated on defining pertinent manifestations of the involved technologies using relevant technologies with parallel databases. However, after 2024, the study reveals an obvious interest that focuses on ensuring security and persistence of those technologies via metadata issues.

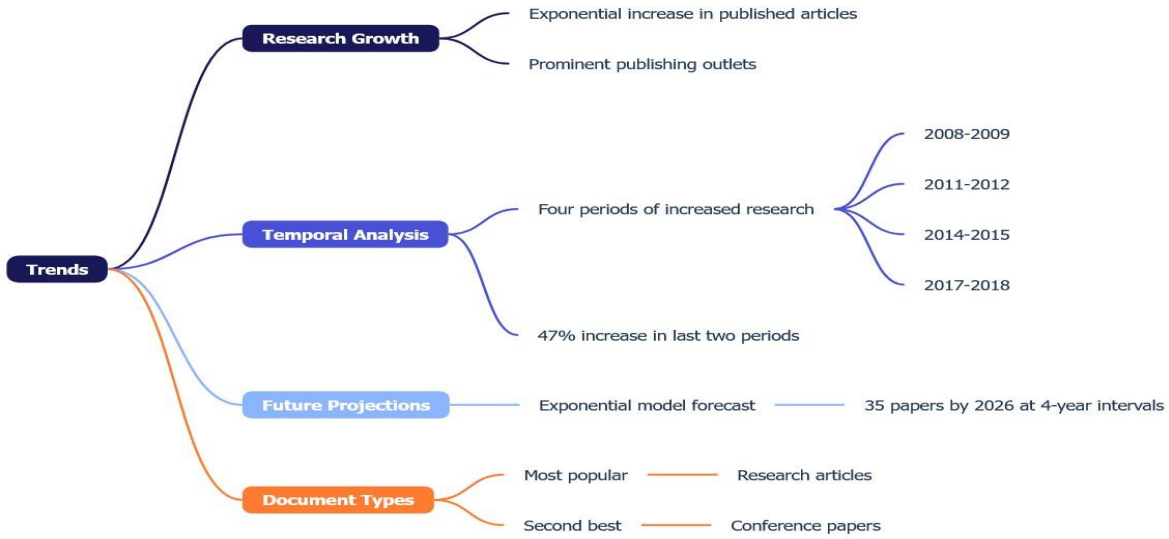

Fig 4: Trends

8. Discussion and Implications

For researchers, it has become necessary to explore more aspects of multiple and complex relationships among big data governance, data security, compliance, and data

management. It is understood that the use of big data in the business context combines an understanding of digital, social media, text analysis, and data sources to compete and create more value (Nassar and Kamal, 2021; Oesterreich et al., 2022; Sebestyén et al., 2021; Cozzoli et al.2022). For this purpose, it is proposed that researchers and practitioners in both the analytical, predictive, and prescriptive analysis sectors are involved in advanced research on big data, data governance, data security, and compliance. Many older, existing IS (Information Systems) and DA (Data Analytics) sources are no longer suitable for the emerging world of big data and the DA communities. The communities developed will create and publicise new knowledge. The study proposes that academics will begin to focus more on the practices of companies that are caregivers and suppliers of insights into governance, security, and compliance of big data. For research, there is need to investigate not only services but also DA applications in more innovative uses.

Future research should focus on unique, non-traditional issues and trends relating to potential shifts in the market, privacy legal issues, personal metadata regulations, competition in big data landscapes, governance and legitimacy strategies for big data, differentiation, certification program assurance, network scalability, DA collaboration, differences in the level of implementation and governance basis, algorithm monitoring, among other variables (Aldboush & Ferdous, 2023; Chinta, 2021; Alam and Mohanty, 2023; Zhang et al., 2022; Sundarakani et al., 2021)

8.1. Theoretical Contributions

The analysis and results cover the methodological contributions that the research makes about the creation of a standardised set of criteria for indexing terms that represent categories for different kinds of data governance models at the worldwide level, while also contributing to theory by presenting an updated historical analysis of the main topics and trends studied in the field of data governance, highlighting authors, countries, journals, papers, collaborations, and creating repositories with all papers, with several levels of scrutiny, among many other initiatives. The study aims to provide an overview of influential research in the field, identify key lines of inquiry in data governance, and chart the road ahead for new and experienced researchers.

Several theoretical contributions can be identified in the results described throughout the study. The different foci of data governance that have emerged in the literature, by means of focus groups at different levels within organisations along with the importance, advantages, drawbacks, costs, complexity, practices, and benefits to solving different organisational requirements are discussed in different parts of the study. The different types of literature

identified are examined toward the theory model, presenting many contributions on the categories of DG models, solving organisational requirements to achieve competitive advantages through performance improvement from the use of quality data to create effective relationships to gain strategic insights into relationships between process objectives and performance outcomes to provide carefully controlled activities to fulfill information and communication expectations through compliance with laws, rules, and regulations, and also with customer, partner, and organisational requirements through effective self-assessment and performing process analysis, using performance data to balance the business units' strategy and operational goals, and planning and budgeting.

9. Conclusion

This systematic literature review study underscores the importance of effective data governance for data security and compliance. Specifically, it finds the need for more research to find effective solutions to leverage data to drive business growth while ensuring its security and compliance. Future research should develop or discover robust data governance tools that leverage data for business growth. This study also suggests the need for industries to begin publishing laws that guide data governance to ensure the safety and compliance of data.

This research may also lead to collaboration between data scientists and ethicists, and the development of pre-designs for data governance in order to ensure that the system protects data and prevents misuse. The research is based on secondary studies, a methodological limit due to the immense complexity of the phenomenon. Data security and compliance are two fundamental principles of a data ecosystem. Although important, they are naturally restricted because data are the heart and soul of the data cycle. Our results can inspire decision-making evaluation rules circumventing the phenomena, making sure to consider individual organisational conditions and contexts. We are convinced that further multidisciplinary studies may wish to investigate the existence of other policies or tools to foresee, address, and repair possible privacy network problems. We hope that future research will address these limitations and the specific nature of the dynamics studied with iterative and qualitative methodologies.

9.1. Summary of Key Findings

The broad range of data security areas shows that multiple and closely related data security areas seek to protect data and systems from integrity, privacy, secrecy, and availability violations. User, process, and system entity access to data is controlled and managed according

to business usage, policy, and regulatory compliance requirements. Virtues in the pursuit of integrity, privacy, secrecy, and availability purposes result from the implementation of information security capabilities that align and enforce access control, audit, and other relevant forms of policy and process management, business intelligence, privacy enhancement, and application-level data management support designed for the protection of sensitive data. The key gap is in the lack of attention to how an organisation can mitigate the security risks presented by the large volume, variety, and velocity of big data in the early stages of the big data accumulation process.

The data security literature focuses on data in its processed state, does not adequately address the growing big data threats, pressures, and challenges at the beginning of the big data lifecycle. Only an informed execution of secure and compliant data governance in big data enables an organisation to mitigate the risks and pursue the privacy and security virtues that exist among data. The desired learning outcome of any learning and scholarly program on securing data is to impart a conceptual understanding of that program, implement secure data governance, build a learning and standards framework, and strengthen the knowledge base of research methodologies in the field of secure data governance. Perspectives such as architectural, systems, outcomes, and institutional need careful consideration to guide the learning process for secure data governance.

Table 3: Summary of Key Findings

Data Security Areas	**Key Aspects**
Protection Domains	Integrity, Privacy, Secrecy, Availability
Access Control Management	User, Process, and System Entity Access Control
Security Implementation Virtues	• Information Security Capabilities • Policy and Process Management • Business Intelligence • Privacy Enhancement • Application-Level Data Management
Big Data Security Challenges	• Volume • Variety • Velocity • Lack of Early Lifecycle Security Attention
Learning Outcomes for Secure Data Governance	• Conceptual Understanding • Secure Data Governance Implementation • Learning and Standards Framework • Research Methodology Knowledge Strengthening

9.2. Future Research Directions

Numerous contributions within the field of data governance point towards future research directions. Future research in data governance is broadly categorised as: areas requiring additional theoretical development; differences in data governance needs; future data governance developments; creating and maintaining data governance principles; and the role of infrastructure incentives and reinforcement of data governance, which includes an examination of the value of data governance.

Although several definitions exist, no broadly recognised standard model or approach to data governance has been established. The data governance area is still in need of concomitant theory development. Data governance risks feature ambiguously in the literature. The establishment of innovative data governance solutions that address critical fragmented and scientific infrastructure categories, and their associated risk, is defined. The data governance and data management requirements that might, or might not, necessarily be accomplished by data governance frameworks are described by empirical results from various areas. Further research into other scientific disciplines is warranted.

Data governance developments were addressed in three cases. Accounting for government data governance configuration and settings is deemed highly necessary as a result of the considerable investment and influence of governance decisions made for government services at local and global levels, demonstrating a diverse experience in government data governance, from manual paper records to consolidation of more fragmented approaches. It is believed that further research on data governance principles, that serve to guide data governance efforts, might offer significant benefits, especially where organisations are paired with research communities and demand an evidence-based understanding of how data governance leads to complex data governance-dependent outcomes. Incentives and enforcement of implementation are seen as part of the data governance challenge that has not been examined.

Weaknesses in the underlying data subjected to data governance efforts are highlighted. There is a clear pattern of declining data quality that happens when data are out of the hands of those that generated them. Furthermore, a research void in what might be done to maintain data governance is identified. Future research directions should take a deeper scientific data governance perspective. Insights from these experiments may put forth standard solutions that can be tailored and form the basis for data governance guidelines. It calls for incentives towards the adoption of standards and best practices, and for the implementation of security aspects with stronger support than what is being done today. Differences among data governance and

linked issues of interest to data stewardship among various scientific disciplines are delineated. Factors that facilitate data governance are considered. Potential directions for future investigation and the further development of data governance principles are proposed. The study also underscores a current deficiency and a topic that suggests independence as a future area of study. The results imply data quality peculiarities that lead to new knowledge in a domain where it has the potential to matter. Churning data for value is named as essential to the success of data governance strategies. What this means or how to support these instrumental initiatives is open to further study.

Table 4: Future Research Directions

Research Categories in Data Governance	Key Insights
Theoretical Development	No broadly recognised standard model exists; Concomitant theory development is needed
ssssResearch Directions	Further exploration in scientific disciplines; Investigate data governance principles and implementation
Governance Configuration	Critical examination of government data governance across different contexts
Data Quality Challenges	Declining data quality when data moves from original source; Need for maintenance strategies
Implementation Support	Call for incentives, adoption of standards, and stronger security implementation

References

[1] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing, 28(1), 59-72.

[2] Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S.A., & Karim, F. K. (2022). Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. Electronics, 11(4), 630.

[3] Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. Computer Science & IT Research Journal, 5(1), 120-140.

[4] Adeniran, I. A., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., & Efunniyi, C. P. (2024). Strategic risk management in financial institutions: Ensuring robust regulatory compliance. Finance & Accounting Research Journal, 6(8), 1582-1596.

[5] Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. Computer Science Review, 43, 100452.

[6] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in IOTbased cloud computing: A comprehensive survey. *Electronics, 11*(1), 16.

[7] Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. *International Journal of Scientific Research in Science Engineering and Technology*.

[8] Alam, A., & Mohanty, A. (2023, January). From Bricks to Clicks: The Potential of Big Data Analytics or Revolutionising the Information Landscape in Higher Education Sector. In International Conference on Data Management, Analytics & Innovation (pp. 721-732). Singapore: Springer Nature Singapore.

[9] Aldboush, H. H., & Ferdous, M. (2023). Building trust in fintech: an analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies*, *11*(3), 90.

[10] Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Applied Sciences.

[11] Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. International Journal of Organisational Analysis, 31(3), 875-888.

[12] Aljumah, A. I., Nuseir, M. T., & Alam, M. M. (2021). Organisational performance and capabilities to analyse big data: do the ambidexterity and business value of big data analytics matter?. Business Process Management Journal, 27(4), 1088 1107.

[13] Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377-387

[14] Al-Okaily, A., Teoh, A. P., & Al-Okaily, M. (2023). Evaluation of data analytics-oriented business intelligence technology effectiveness: an enterprise-level analysis. Business Process Management Journal, 29(3), 777-800.

[15] Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*, 565-578.

[16] Antony, J., Psomas, E., Garza-Reyes, J. A., & Hines, P. (2021). Practical implications and future research agenda of lean manufacturing: a systematic literature review. Production planning & control, 32(11), 889-925.

[17] Aoun, A., Ilinca, A., Ghandour, M., & Ibrahim, H. (2021). A review of Industry 4.0characteristics and challenges, with potential improvements using blockchain technology. Computers & Industrial Engineering, 162, 107746.

[18] Ashaari, M. A., Singh, K. S. D., Abbasi, G. A., Amran, A., & Liebana-Cabanillas, F. J. (2021). Big data analytics capability for improved performance of higher education institutions in the Era of IR 4.0: A multi-analytical SEM & ANN perspective. Technological Forecasting and Social Change, 173, 121119.

[19] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive reviewof cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333

[20] Awan, U., Sroufe, R., & Shahbaz, M. (2021). Industry 4.0 and the circular economy: A literature review and recommendations for future research. Business Strategy and the Environment, 30(4), 2038-2060.

[21] Baima, G., Forliano, C., Santoro, G., & Vrontis, D. (2021). Intellectual capital and business model: a systematic literature review to explore their linkages. Journal of Intellectual Capital, 22(3), 653-679.

[22] Bandari, V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organisation types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11.

[23] Bany Mohammad, A., Al-Okaily, M., Al-Majali, M., & Masa'deh, R. E. (2022). Business intelligence and analytics (BIA) usage in the banking industry sector: an application of the TOE framework. Journal of Open Innovation: Technology, Market, and Complexity, 8(4), 189.

[24] Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalisation. Journal of Information Technology Management, 14(Special Issue: Digitalisation of Socio Economic Processes), 25-58.

[25] Brown, I., & Marsden, C. T. (2023). *Regulating code: Good governance and better regulation in the information age*. MIT press.

[26] Butler, C. C., Hobbs, F. R., Gbinigie, O. A., Rahman, N. M., Hayward, G., Richards, D. B. & Zafar, A. (2023). Molnupiravir plus usual care versus usual care alone as early treatment for adults with COVID-19 at increased risk of adverse outcomes (PANORAMIC): an open label, platform-adaptive randomised controlled trial. The Lancet, 401(10373), 281-293.

[27] Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S. & Hudson, M. (2023). The CARE principles for indigenous data governance. *Open Scholarship Press Curated Volumes: Policy*.

[28] Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific data*, *8*(1), 108.

[29] Chauhan, C., Parida, V., & Dhir, A. (2022). Linking circular economy and digitalisation technologies: A systematic literature review of past achievements and future promises. Technological Forecasting and Social Change, 177, 121508.

[30] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, *180*(2), 581-604.

[31] Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocessors and Microsystems*, *81*, 103722.

[32] Chinta, S. (2021) Integrating Machine Learning Algorithms in Big Data Analytics: A Framework forEnhancing Predictive Insights. 2145-2161.

[33] Chukwurah, N., Ige, A. B., Idemudia, C., & Adebayo, V. I. (2024). Strategies for engaging stakeholders in data governance: Building effective communication and collaboration. Open Access Research Journal of Multidisciplinary Studies, 8(01),057-067.

[34] Conrad, S. S. (2022). Integrating data privacy principles into product design: Teaching" privacy by design" to application developers and data scientists. *Journal of Computing Sciences in Colleges*, *38*(3), 132-142

[35] Cozzoli, N., Salvatore, F. P., Faccilongo, N., & Milone, M. (2022). How can big data analytics be used or healthcare organisation management? Literary framework and future research from a systematic review. BMC health services research, 22(1), 809.

[36] Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*, *8*(13), 10452-10473.

[37] Dastres, R., & Soori, M. (2021). A review in recent development of network threats and security measures. *International Journal of Information Sciences and Computer Engineering*.

[38] David, D. S., Anam, M., Kaliappan, C., Selvi, S., Sharma, D. K., Dadheech, P., & Sengan, S. (2022). Cloud Security Service for Identifying Unauthorised User Behaviour. Computers, Materials & Continua, 70(2).

[39] De Bem Machado, A., Secinaro, S., Calandra, D., & Lanzalonga, F. (2022). Knowledge management and digital transformation for Industry 4.0: a structured literature review. Knowledge Management Research & Practice, 20(2), 320-338.

[40] Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R. & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. Future Generation Computer Systems, 131, 209-226.

[41] Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to addressdata privacy concerns when using social media data in conservation science. Conservation Biology, 35(2), 437-446.

[42] Di Vaio, A., Palladino, R., Pezzi, A., & Kalisz, D. E. (2021). The role of digital innovation in knowledge management systems: A systematic literature review. *Journal of business research*, *123*, 220-231.

[43] Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion, 99, 101896.

[44] Duggineni, S. (2023). Impact of controls on data integrity and information systems. *Science and Technology*, *13*(2), 29-35.

[45] Dutta, A., & Fischer, H. W. (2021). The local governance of COVID-19: Disease prevention andsocial security in rural India. *World development*, *138*, 105234.

[46] El Khatib, M., Al Mulla, A., & Al Ketbi, W. (2022). The role of blockchain in e-governance and ecision-making in project and program management. *Advances in Internet of Things*, *12*(3), 88-109.

[47] El Khatib, M., Al Mulla, A., & Al Ketbi, W. (2022). The role of blockchain in e-governance and decision-making in project and program management. *Advances in Internet of Thin*, *12*(3), 88-109.

[48] Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy*, *48*(9), 102836

[49] Fathi, M., Haghi Kashani, M., Jameii, S. M., & Mahdipour, E. (2022). Big data analytics inweather forecasting: A systematic review. Archives of Computational Methods in Engineering, 29(2), 1247-1275.

[50] Fernandez, C. B. (2022). Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse. arXiv preprint arXiv:2204.01480.

[51] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

[52] Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021, May). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In Proceedings of the 2021 CHI conference on human factors in computing systems (pp. 1-18).

[53] Halchenko, Y. O., Meyer, K., Poldrack, B., Solanky, D. S., Wagner, A. S., Gors, J & Hanke, M. (2021). DataLad: distributed system for joint management of code, data, and their relationship. Journal of Open Source Software, 6(63), 3262.

[54] Hamid, R. A., Albahri, A. S., Alwan, J. K., Al-Qaysi, Z. T., Albahri, O. S., Zaidan, A. A. & Zaidan, B. B. (2021). How smart is e-tourism? A systematic review of smart tourism recommendation system applying data management. Computer Science Review, 39, 100337.

[55] Hazmi, N. R., Abrisah, A., & Idaya, A. Y. (2023). Research data governance activities for implementation in Malaysia research performing organisations: insights from data practitioners via

[56] Delphi study. Malaysian Journal of Library and Information Science, 28(3), 37-60. Housawi, A., & Lytras, M. D. (2025). Data governance in healthcare organizations. In *Next Generation eHealth* (pp. 13-32). Academic Press.

[57] Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, *6*(2), 234-247.

[58] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22.

[59] Jarvenpaa, S. L., & Essén, A. (2023). Data sustainability: Data governance in data infrastructures across technological and human generations. *Information and Organization*, *33*(1), 100449.

[60] Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420.

[61] Karunarathna, I., De Alvis, K., Gunasena, P., & Dissanayake, D. (2024). Critical approaches to riting literature reviews: Guidelines for success.

[62] Karunarathna, I., De Alvis, K., Gunasena, P., & Jayawardana, A. (2024). Creating value through literature reviews: Techniques for identifying research gaps.

[63] Khan, A. A., Laghari, A. A., Gadekallu, T. R., Shaikh, Z. A., Javed, A. R., Rashid, M. & Mikhaylov, A. (2022). A drone-based data management and optimisation using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers and Electrical Engineering, 102, 108234.

[64] Komljenovic, J. (2022). The future of value in digitalised higher education: why data privacy should not be our biggest concern. *Higher Education*, *83*(1), 119-135.

[65] Kulkov, I., Kulkova, J., Rohrbeck, R., Menvielle, L., Kaartemo, V., & Makkonen, H. (2024). Artificial intelligence-driven sustainable development: Examining organisational, technical, and processing approaches to achieving global goals. Sustainable Development, 32(3), 2253 2267.

[66] Kumar, S., Kar, A. K., & Ilavarasan, P. V. (2021). Applications of text mining in services management: A systematic literature review. International Journal of Information Management Data Insights, 1(1), 100008.

[67] Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241-15271.

[68] Lăzăroiu, G., Andronie, M., Iatagan, M., Geamănu, M., Ștefănescu, R., & Dijmărescu, I. (2022). Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the internet of manufacturing things. ISPRS International Journal of Geo-Information, 11(5), 277.

[69] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176 8186. Mao, Z., Wu, J., Qiao, Y., & Yao, H. (2022). Government data governance framework based on a data middle platform. Aslib Journal of Information Management, 74(2), 289-310.

[70] McGilvray, D. (2021). *Executing data quality projects: Ten steps to quality data and trusted information (TM)*. Academic Press.

[71] McLeod, A. & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviours?. Computers & Security.

[72] Michel-Villarreal, R., Vilalta-Perdomo, E., Salinas-Navarro, D. E., Thierry-Aguilera, R., & Gerardou, F. S. (2023). Challenges and opportunities of generative AI for higher education as explained by ChatGPT. Education Sciences, 13(9), 856.

[73] Miyachi, K. & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information processing & management.

[74] Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, *32*(2), 241-268.

[75] Nassar, A., & Kamal, M. (2021). Ethical dilemmas in AI-powered decision-making: a deep dive into big data-driven ethical considerations. International Journal of Responsible Artificial Intelligence, 11(8), 1-11.

[76] Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: an indepth analysis of legal and regulatory frameworks impacting cybersecurity practices. International Journal of Intelligent Automation and Computing, 6(5), 112.

[77] Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., & McIntosh, T. R. (2024). Privacy preservation of electronic health records in the modern era: A systematic survey. ACM Computing Surveys, 56(8), 1-37.

[78] Núñez-Canal, M., de Obesso, M. D. L. M., & Pérez-Rivero, C. A. (2022). New challenges in higher education: A study of the digital competence of educators in Covid times. Technological Forecasting and Social Change, 174, 121270.

[79] Nzeako, G., Akinsanya, M. O., Popoola, O. A., Chukwurah, E. G., Okeke, C. D., &Akpukorji,I. S. (2024). Theoretical insights into IT governance and compliance in banking: Perspectives from African and US regulatory environments. International Journal of Management & Entrepreneurship Research, 6(5), 1457 1466.

[80] Obendiek, A. S. (2023). *Data governance: Value orders and jurisdictional conflicts*. Oxford University Press.

[81] Oesterreich, T. D., Anton, E., & Teuteberg, F. (2022). What translates big data into business value? A meta-analysis of the impacts of business analytics on firm performance. *Information & Management*, *59*(6), 103685.

[82] Pansara, R. (2023). Unraveling the complexities of data governance with strategies, challenges, and future directions. *Transactions on Latest Trends in IoT*, *6*(6), 46 56.

[83] Pansara, R. R. (2022). Cybersecurity Measures in Master Data Management: Safeguarding Sensitive Information. International Numeric Journal of Machine Learning and Robots, 6(6), 1-12.

[84] Pansara, R. R. (2022). Edge computing in master data management: Enhancing data processing at the source. *International Transactions in Artificial Intelligence*, *6*(6), 1-11.

[85] Pestana, J. S. (2023). *Data Governance Valuation: A Model for Assessing the Impact on Organisations´ Business* (Master's thesis, Universidade NOVA de Lisboa (Portugal)).

[86] Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citisens' perception of data protection and data security. *Computers in Human Behavior*, *122*, 106830.

[87] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299 1323.

[88] Rathore, M. M., Shah, S. A., Shukla, D., Bentafat, E., & Bakiras, S. (2021). The role of AI, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities. IEEE Access, 9, 32030-32052.

[89] Sebestyén, V., Czvetkó, T., & Abonyi, J. (2021). The applicability of big data in climate change research: The importance of system of systems thinking. Frontiers in Environmental Science, 9, 619092.

[90] Secinaro, S., Calandra, D., Secinaro, A., Muthurangu, V., & Biancone, P. (2021). The role of artificial intelligence in healthcare: a structured literature review. BMC medical informatics and decision making, 21, 1-23.

[91] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4), 1927.

[92] Solomonides, A. (2019). Research data governance, roles, and infrastructure. *Clinical research informatics*, 291-310.

[93] Spanaki, K., Karafili, E., & Despoudi, S. (2021). AI applications of data sharing in agriculture 4.0: A framework for role-based data access control. International Journal of Information Management, 59, 102350.

[94] Sun, L., Zhang, H., & Fang, C. (2021). Data security governance in the era of big data: status, challenges, and prospects. *Data Science and Management*, *2*, 41-44.

[95] Sundarakani, B., Ajaykumar, A., & Gunasekaran, A. (2021). Big data driven supply chain design and applications for blockchain: Action research using case study approach. Omega.

[96] Taherdoost, H. (2022). Cybersecurity vs. information security. Procedia Computer Science.

[97] Tandon, A., Kaur, P., Mäntymäki, M., & Dhir, A. (2021). Blockchain applications i management: A bibliometric analysis and literature review. Technological Forecasting and Social Change, 66, 120649.

[98] Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. International Journal of Information Management, 60, 102356.

[99] Telo, J. (2023). Smart city security threats and countermeasures in th context of emerging technologies. International Journal of Intelligent Automation and Computing, 6(1), 31-45.

[100] Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. International Journal for Quality Research, 15(3), 845.

[101] Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, 104130.

[102] Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Computers & Security*, *110*, 102402. Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security.

[103] Vegesna, V. V. (2021). Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage. Middle East Journal of Applied Science & Technology, 4(2), 163-178.

[104] Viljoen, S. (2021). A relational theory of data governance. Yale LJ.

[105] Vyas, B. (2023). Security Challenges and Solutions in Java Application Development. Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal, 12(2), 268-275.

[106] World Health Organization. (2023). *Exposure to lead: a major public health concern. Preventing disease through healthy environments*. World Health Organization.

[107] Yallop, A. C., Gică, O. A., Moisescu, O. I., Coroș, M. M., & Séraphin, H. (2023). The digital traveller: implications for data ethics and data governance in tourism and hospitality. Journal of Consumer Marketing, 40(2), 155-170.

[108] Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernised European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137-155.

[109] Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernised European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137-155.

[110] Zhang, J., & Zhang, Z. M. (2023). Ethics and governance of trustworthy medical artificial intelligence. *BMC medical informatics and decision making*, *23*(1), 7.

[111] Zhang, Q., Gao, B., & Luqman, A. (2022). Linking green supply chain management practices with competitiveness during covid 19: The role of big data analytics. Technology in Society.

Citation: Jude Osakwe, Iyaoo Haitula-Waiganjo. (2025). Data Security and Compliance Through Effective Data Governance. International Journal of Information Security (IJIS), 4(1), 69-97.

Abstract Link: https://iaeme.com/Home/article_id/IJIS_04_01_004

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJIS/VOLUME_4_ISSUE_1/IJIS_04_01_004.pdf

✉ **editor@iaeme.com**