Advanced Research in Economics and Business Strategy Journal

E-ISSN : 2773-3807
P-ISSN : 2716-9421

Vol.06 No.01 (2025)

237-252

The Analysis of the Criticality of Data Integrity in Human Resources Information Systems

Dickson Mdhlalose[1*]

Received: 09/06/2025 Accepted : 28/06/2025 Published : 30/06/2025

https://doi.org/10.52919/arebus.v6i1.85

ABSTRACT

Introduction: In the fields of information technology and data management, data integrity is a fundamental concept. Data integrity ensures the accuracy, consistency, and dependability of data throughout its existence. This study aims to establish best practices for preserving accurate and trustworthy HR data and to assess the importance of information integrity in HRIS, examining its impact on business decisions, compliance with regulations, and employee confidence. Method: Data from secondary sources were used in this investigation. To assist the study, relevant textbooks were reviewed, and secondary material was gathered online, utilising various search engines. Results: Due to the diverse sources and processes from which HR inputs come, data integrity in HRIS is seldom attained. Organisations can save time, money, and resources by establishing and maintaining data integrity, thereby preventing critical decisions from being made based on incomplete or erroneous data. A fundamental gap with major organisational consequences is the lack of research on data integrity in human resource information systems. The usefulness of this study lies in its thorough presentation of data integrity challenges in the human resources information system. This analysis was limited to secondary data and the limited scholarly literature. Conclusion: For HRIS to manage employee data accurately, consistently, and securely, data integrity is essential. It is essential for upholding compliance, facilitating informed decision-making, and fostering trust within businesses. HRIS runs the danger of operational failures, legal issues, and reputational harm in the absence of strong data integrity controls. Data integrity must therefore be given top priority if HR operations are to continue succeeding and the organisation is to expand.

Keywords: Data Integrity, Data Management, Human Resources, HR Information System, Human Resource Management.

JEL Codes: J24, M14

How to cite this article

Mdhlalose, D. (2025). The Analysis of the Criticality of Data Integrity in Human Resources Information Systems. Advanced Research in Economics and Business Strategy Journal, 6(1), 237-252. https://doi.org/10.52919/arebus.v6i1.85

[1*] Corresponding author: Doctor of Business Administration (DBA), Department of Information and Communication Technology, National Electronic Media Institute of South Africa, Johannesburg, South Africa, dsskosana@gmail.com

1. INTRODUCTION

Human Resources Information Systems (HRIS) are essential tools for managing employee data, optimizing human resources (HR) processes, and informing strategic decisions in the digital age. Since these systems store confidential data, including payroll administration, performance, incentives, and personal details, information integrity — defined as the reliability, precision, and dependability of data throughout its lifecycle — becomes a pressing concern. A breach in data integrity can have serious repercussions, including reduced operational effectiveness, fines, and damage to one's reputation. Notwithstanding its significance, data integrity in HRIS is frequently undervalued, which exposes businesses to dangers. One important research gap with major ramifications for organisations is the scarcity of studies on data integrity in HRIS. Organisations that lack a thorough understanding of data integrity concerns are susceptible to errors, non-compliance with regulations, and inefficiencies that can be avoided with appropriate insights. This raises a research question for this study: "How will data integrity affect organisations' HRIS decisions, confidence among employees, and compliance with regulations?".

Technological breakthroughs in HR may result from identifying the causes of this research gap and exploring potential research topics. Consider the potential impact of developing innovative techniques and technological solutions that transform how organisations manage and protect their valuable HRIS data. Human resource management (HRM) now plays a more strategic role overall, replacing its previous function as traditional personnel management. Quaosar and Rahman (2021) state that the HRIS defines the integration of HRM with the Information System (IS). Human resource departments no longer need to be involved in decision-making processes due to new technology, which provides decision-makers and strategy-makers within an organisation with a means to access HR information (Weeks, 2013). An ever-growing volume of data is created, collected, and utilised daily by organisations all over the world to make crucial business choices (Duggineni, 2023). The term "data integrity" refers to the overall precision, consistency, and dependability of the data stored in a computerized database, data archive, or other data storage system. Ensuring the accuracy, timeliness, and suitability of the data utilised by an organisation is a crucial component of data management (Sluzki, 2023). In addition to identifying information that could be desirable to criminals, HR data is a treasure mine of information that an organisation should safeguard (White, 2019).

The need for effective data management and the implementation of digital transformation plans have led to a significant increase in reliance on HRIS in recent years. Marler and Boudreau (2017) assert that by automating procedures, facilitating data accessibility, and facilitating data-driven decision-making, HRIS plays a critical role in improving HR activities. Data integrity has become an issue, though, due to the growing complexity of these systems and the amount of data they manage. Stone and Deadrick (2015) stress that to preserve organisational legitimacy and conformity to regulations, HRIS must guarantee the integrity and precision of data. Recent studies have highlighted the dangers associated with interfering with data integrity in HRIS. For example, Johnson et al. (2021) found that inaccurate payroll processing, inadequate employee benefit administration, and subpar performance reviews can result from data breaches and errors in HRIS systems. These problems undermine employee happiness and trust, in addition to interfering with HR procedures.

Meanwhile, Martinez and Rodriguez (2023) contend that organisations may face severe legal and financial repercussions for failing to comply with data protection laws, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Its influence on strategic HR decision-making further emphasises how important data integrity is in HRIS. Bondarouk et al. (2017) argue that inadequate or erroneous data can result in subpar organisational outcomes, inadequate workforce planning, and ineffectual talent management.

Despite these obstacles, thorough research on the importance of data integrity in HRIS and its effects on organisational performance is lacking. Kavanagh and Johnson (2018) point out that data integrity is crucial to preserving the legitimacy of HR analytics, which are being increasingly utilised to drive competitive advantage and guide organisational plans. The necessity for a thorough examination of the variables influencing data integrity in HRIS, the repercussions of compromising data integrity, and the tactics that organisations can use to protect data integrity are highlighted by this vacuum in the literature. By addressing these issues, this study aims to contribute to the growing body of research on HRIS and provide valuable insights to businesses seeking to enhance the data integrity maintained by their HR systems. The problem this study identifies is that the susceptibility to illicit access and data breaches in HRIS poses a serious challenge to the effectiveness of data integrity. Even with the most sophisticated security mechanisms in place, HRIS often stores extremely private and professional information that, if compromised, could result in serious privacy breaches and have a negative financial impact on both individuals and companies.

Performance reviews, compensation and benefits management, payroll processing, and other vital HR tasks can all be impacted by erroneous or erratic information in an HRIS. They result in legal and regulatory problems, such as breaking labour laws and rules. Researching the underlying reasons for these weaknesses and creating more complex, impenetrable security processes may prove fruitful and influential, revolutionising how HR departments protect their important information. There are disadvantages to HRIS, especially when considering the expenses and assistance needed for such measures to be implemented effectively in organisations (Alomari, 2019). This study aims to establish best practices for preserving accurate and trustworthy HR data and to assess the importance of information integrity in HRIS by examining its impact on business decisions, compliance with regulations, and employee confidence. This goal aligns with the study's emphasis on understanding the importance of data security in HRIS, the consequences of its breaches, and risk-reduction techniques.

2. RESEARCH METHODS

According to Fox and Bayat (2007), this study utilised manuscripts, books, journals, and secondary sources. Information accessible online materials were collected through what has been frequently referred to as virtual methodologies, methods used via the internet to obtain secondary sources (Markham & Baym, 2009). Research requires the use of secondary data because it offers an economical and effective means of gaining access to a multitude of material that has previously been gathered, examined, and verified by other scholars or institutions. Without the scheduling and financial constraints imposed by primary data collection, secondary data enables researchers to confirm ideas, identify trends, and build upon existing knowledge. Smith and Watson (2020) assert that because secondary data often contain extensive datasets spanning several years or geographical areas, they are especially useful for conducting comprehensive research or comparative assessments.

Furthermore, Johnson et al. (2021) note that by facilitating cross-validation with previous research, secondary data can enhance the validity of study findings. Secondary data is essential for answering complex research questions and guiding rational choices in domains such as organisational studies, policy evaluation, and healthcare. Utilising secondary data enables academics to focus on interpreting and synthesising information, thereby advancing their understanding of their respective subjects. To ensure accuracy, consistency, and transparency in reporting, this work employed PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) criteria (Page et al., 2021).

To enhance the comprehensiveness, precision, and transparency of meta-analyses and systematic reviews, the PRISMA recommendations are frequently employed (Page et al., 2021). PRISMA reduces bias and improves consistency in research analysis by providing an organized framework for reporting techniques and outcomes. Its structured criteria and flow chart enable critical evaluation and ensure full recording of review procedures, making it beneficial for scientists, peer reviewers, and readers (Moher et al., 2009). The author maintains methodological rigour and promotes confidence in conclusions grounded in evidence by adhering to the PRISMA guidelines. The entries were created using the databases Scopus, Business Source Complete (EBSCO), and Google Scholar. A thorough, evidence-based synthesis was ensured by screening sources for relevance to organisational implications, validity of data structures, and HRIS problems. Using the PRISMA concept and information from the paper, this is a detailed, step-by-step procedure for gathering, screening, reviewing, and analysing the literature for the study:

- Identification
    - Methods: Using three databases, Google Scholar, Business Source Complete (EBSCO), and Scopus, the researcher found four hundred and eighty documents in all.
    - Search Strategy: To find pertinent literature, keywords related to organisational implications, confidentiality of information frameworks, and HRIS problems were employed.
    - Output: Many possible studies for preliminary screening were produced by this stage.
- Screening
    - Method: Abstracts as well as titles were used to determine the relevancy of the four hundred and eighty items.
    - Criteria: Studies were assessed based on their attention to organisational results, data integrity, and HRIS.
    - Output: After eliminating redundant or unnecessary research, one hundred records were kept for additional analysis.
- Eligibility
    - Procedure: To ascertain eligibility, a full-text evaluation of the one hundred scanned documents was conducted.
    - Criteria:

        - Pertinence to the goals of the research (for example, HRIS integrity of data, consequences, structures, or difficulties).
        - Methodological rigour (for example, reliable sources, reviewed by experts, articles).
        - Exclusion of research with no theoretical foundation or empirical support.
    - Result: Fifty full-text publications were judged suitable for in-depth examination.
- Inclusion
    - Methods:
        - Out of the fifty suitable publications, the most recent studies were chosen.
        - Conformity to the research questions is one of the criteria.
        - A commitment (such as case research, recommended practices, or analytic methods) to the understanding of data integrity in HRIS.
    - Result: The comprehensive review contained thirty-eight studies.

This systematic methodology enables readers to evaluate the assessment process and findings. The researcher employed a research strategy created by Dolowitz et al. (2008) to identify the most pertinent resources for this study. This approach is centred around the researcher's goals, the substantially instructive search phrases, and the most helpful instruments that would prove beneficial during the research.

3. LITERATURE REVIEW

3.1 Human Resource Data Integrity Cruciality

While maintaining the integrity of HR data is crucial when utilising HR systems, it is seldom achieved since HR inputs originate from a variety of sources and procedures (ZeroedIn, 2021). Establishing and upholding data integrity can help organisations avoid wasting time, money, and resources by making informed decisions based on accurate data. Data-driven judgments, after all, are only as good as the data they are founded on. Should there be any breach of data integrity in the organisation, the consequences might be severe and profound (Cote, 2021). Organisations must be able to recover quickly from a data integrity breach and have confidence that the recovered data is accurate, comprehensive, and virus-free, allowing them to continue operating. Corporate data, particularly emails, personnel records, financial information, and consumer data, has been infiltrated by well-publicised data integrity assaults brought on by unlawful insertion, erasure, or alteration. Systemic assaults have forced several organisations to suspend operations (Tobin et al., 2016) temporarily.

One reason why data quality remains a problem may be the existence of training gaps. Humans make too many mistakes, which lowers the quality of the data and erodes employees' faith in the system. This runs counter to upper management's faith in the system. The statistical analyses and reports produced by the system are also impacted by the alleged poor quality of the data (Udekwe & De la Harpe, 2017). In any situation, exposed data is harmful and of little use. Data integrity can be compromised in several ways, including machine malfunctions, human errors, transcription errors, malware, virus infections, hacking, unauthorized access, and natural disasters such as flooding and fires (White, 2019). Data integrity can be easily compromised during the implementation of an HRIS, whether it involves a complete switch to a new system or the conversion of an existing manual system to an automated one. A single misplaced number or an erroneous calculation can compromise the integrity of several bits of information. Payroll, performance evaluations, learning and development, productivity monitoring, the organisation's public image, and efficiency can all be impacted by erroneous or inaccurate HR data (Rietsema, 2023).

3.2 Consequences of Compromised Data Integrity

The precision, uniformity, and dependability of data throughout its lifecycle are referred to as data integrity. There may be significant repercussions for individuals, organisations, and society as data integrity is compromised. The eight argumentation paragraphs that follow, supported by current scholarly sources, address the repercussions of compromising data integrity. The faith in electronic systems, which are essential to contemporary economies, is weakened by compromised data integrity. End users might abandon faith in digital platforms, which could result in lower acquisition and participation if they are unable to trust the accuracy of the data. The viability of digital ecosystems depends heavily on trust, and any compromise of data integrity can have a prolonged impact on user behavior (Almadhoun et al., 2021). For example, clients may resort to outdated, ineffective banking practices if financial institutions fail to ensure the accuracy of transaction records. Organisations may suffer significant financial losses due to data integrity violations. Legislative fines, operational inefficiencies, and poor decision-making can all result from inaccurate data. According to Smith and Watson (2020), supply chain management data integrity issues can lead to inventory inconsistencies, shipment delays, and lost profits. The costs of expensive litigation and reputational damage to corporations may also exacerbate financial hardship.

National security is seriously compromised by data integrity issues, particularly in critical infrastructure sectors such as defence, healthcare, and energy. Acts of malicious intent can alter data to interfere with operations, inflict physical harm, or deceive decision-makers (Khan et al., 2022). For instance, changing data in an authority grid's control panel may result in extensive blackouts, putting national stability and the safety of citizens at risk. In the medical field, poor data integrity may result in potentially fatal outcomes. To ensure appropriate care, documentation of patients' plans for therapy and diagnostic findings must all be accurate. Even minor changes to health information can lead to inaccurate diagnoses, ineffective therapies, and adverse effects on patients (Johnson et al., 2021). For example, altering drug dosage information may lead to overdoses or unsuccessful therapies. Businesses that disregard data integrity risk harsh legal and regulatory repercussions. Strict requirements for data security and accuracy are mandated by data protection regulations such as the CCPA and the GDPR. Martinez and Rodriguez (2023) emphasise that breaking these rules can lead to significant fines, legal action, and the cancellation of business licenses. A business convicted of misrepresenting financial data, for instance, can face millions of dollars in fines and be prohibited from doing business in some areas.

The credibility of an organisation can be seriously harmed by a data integrity violation, which can result in the loss of partners and customers. As indicated by Lee and Kim (2022), stakeholders view data integrity violations as an indication of incapacity or carelessness, which can damage an organisation's reputation. For instance, a retail business that is discovered to have falsified sales figures or feedback from consumers may lose the trust of its customers and be subject to boycotts. By making data untrustworthy, compromised data integrity can impede scientific research and innovation. Falsified or altered data in academic and industry research can result in erroneous results, wasted resources, and delayed advancement, as noted by Brown et al. (2021). For example, a pharmaceutical business may create harmful or ineffective medications based on faulty clinical trial data, endangering both innovation and public health. Substantial moral and ethical problems are brought up by compromised data integrity, especially when it comes to manipulation and false information. According to Zhang et al. (2023), manipulated data can be used to disseminate misleading information, influence public opinion, and undermine democratic processes. Manipulated social media data, for instance, might be used as a weapon to influence elections or provoke violence, endangering social order and moral leadership. The consequences of compromised data integrity are profound and multifaceted, affecting trust, financial stability, national security, healthcare, legal compliance, reputation, research, and societal ethics. As organisations and societies become increasingly reliant on digital systems, safeguarding data integrity must be a top priority to mitigate these risks and ensure a secure and trustworthy digital future.

3.3 Managing Data Integrity

A key component of contemporary data management is maintaining data integrity, ensuring that information remains reliable, accurate, and consistent throughout its existence. Data integrity has never been more important or more challenging to maintain in an era of increasing data growth and growing reliance on digital technologies. Recent studies have shown that the widespread adoption of large-scale data, cloud computing, and Internet of Things (IoT) devices has created new vulnerabilities that can jeopardize data integrity, including data corruption, illicit access, and cyberattacks (Zhang et al., 2023). Organisations must adopt a multifaceted approach to address these issues, incorporating robust policies, effective personnel training, and innovative technology solutions. This is especially crucial in sectors such as healthcare and finance, where public trust, regulatory compliance, and decision-making are all directly influenced by data integrity. Innovations in technology are crucial for maintaining data integrity.

Among the most effective methods for protecting against unauthorised changes and ensuring data authenticity are the use of encryption, restricted access, and blockchain technology. For example, blockchain makes it practically hard to change data without being detected by using decentralised consensus processes and cryptographic hashes to produce immutable records (Kumar et al., 2023). Parallel to this, deep learning algorithms are increasingly being employed to identify irregularities in real time, detecting possible corruption or breaches before they escalate (Li & Chen, 2023). These technologies are especially useful in settings such as supply chains or cooperative research networks, where data is exchanged among multiple stakeholders. Organisations may preserve the integrity of their data ecosystems and proactively address risks by utilising these technologies. The correctness, consistency, and dependability of employee data are essential for making well-informed HR decisions, which is why managing data integrity in HRIS is so crucial. Wang's (2024) study revealed that strategic planning and informed decision-making are facilitated for HR departments by the predictive insights and actionable knowledge provided by data analytics.

These technical developments also introduce new ethical concerns, particularly regarding algorithmic bias, data privacy, and security. These problems require a thoughtful and careful response. The advanced ecosystem and framework that Tobin et al. (2016) suggest for ensuring data integrity within the organisation are shown in Figure 1. The components of data integrity solutions consist of but are not limited to, tools for user activity monitoring, data retraction, configuration administration, record versioning, file authenticity evaluation, record security supervisors and journaling, versioning, and snapshotting capabilities of virtual machines. The functions must be automated as part of the data integrity aqueous solutions are hacking evaluation, identification, and occasion log harvesting; reliable data integrity tracking and notification of information (verification checks, off-site, hard copies); identification and analysis for every record adjustment, projects, and deleterious mutations; connection of changes to files and users; activity by users storing; unusual user action recognition; and configuration administration tracking (Tobin et al., 2016).

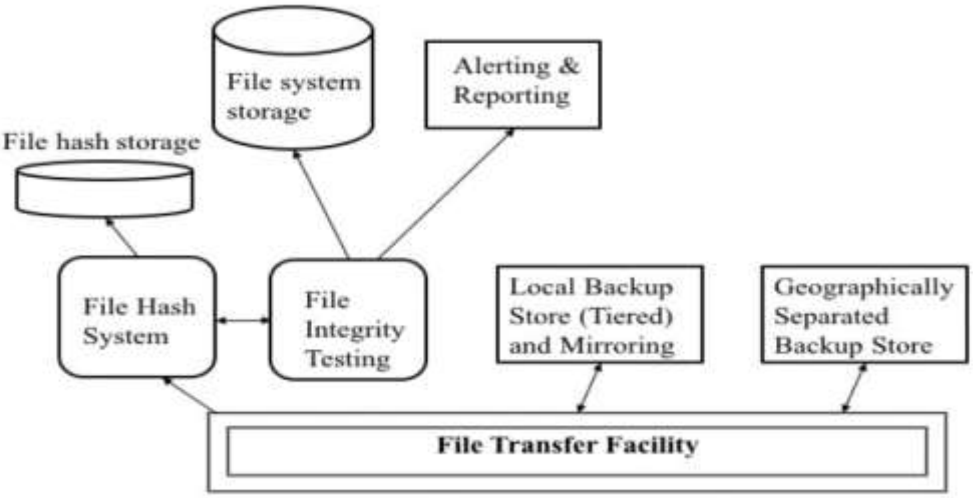

Figure 1. Data Integrity Building Block high-level architecture (Tobin et al., 2016)

Frameworks for data governance are yet another crucial element in maintaining data integrity. By defining precise guidelines, roles, and responsibilities for data handling, these frameworks ensure accountability and transparency throughout the organization. Garcia et al. (2023) emphasise the importance of integrating data governance with emerging technologies, such as AI and the IoT, to automate integrity checks and streamline regulatory compliance procedures. AI-powered systems, for instance, can track data flows in real-time and identify irregularities or illegal access attempts. Furthermore, following global guidelines, like the International Organisation for Standardisation's (ISO) 27001 for information security management, offers a methodical way to preserve data integrity and build stakeholder trust. Finally, building an environment of data integrity across organisations is vital for future sustainability.

Employees play a vital role in ensuring data integrity, as human error remains one of the primary sources of data leaks and corruption. Patel et al. (2023) propose that training programs and education campaigns can equip employees with the necessary information and skills to identify and mitigate risks, including phishing attacks and unintentional data mishandling. Additionally, firms can stay ahead of new risks by collaborating with peers in the industry and participating in international data integrity initiatives. In a more closely linked world, maintaining data integrity will require a comprehensive strategy that combines technological innovation, effective management, and human awareness as data volume and level of detail continue to increase.

3.4 Best Practices for Maintaining Accurate and Reliable HR Data

Maintaining accurate and dependable HR data is crucial for ensuring legal compliance, fostering employee trust, and making informed decisions. HR data includes highly confidential information such as beneficiary details, performance reports, earnings and compensation, and employment records. Inaccurate or inconsistent data can lead to operational inefficiencies, legal ramifications, and damage to one's reputation. Here is a list of the top ten techniques, supported by recent academic research, for ensuring the correctness of HR data. A robust data governance framework is crucial for ensuring the accuracy of HR data. As stated by Tallon et al. (2019), data governance includes establishing policies, procedures, and accountability frameworks to ensure data security, accuracy, and consistency. This involves defining roles and responsibilities for data management, establishing high standards for data quality, and regularly evaluating data processes within HR departments to ensure optimal performance. The integrity of HR data may be at risk due to the error-prone nature of human data entry. To increase the efficiency of data entry processes, Davenport and Ronanki (2018) suggest using automation techniques and artificial intelligence (AI). For example, AI-powered solutions can reduce human error, identify mistakes, and verify data instantly, ensuring that HR records are accurate and up-to-date. Periodic information audits are required to identify and correct problems in HR data.

According to Johnson et al. (2021), routine audits enable companies to identify anomalies, ensure compliance with regulations, and maintain data integrity. Audits should entail cross-referencing personnel files, payroll data, and perk information with the original documentation. HR staff need to be trained in good information management practices to ensure data accuracy and consistency. Training programs should address data entry techniques, data security protocols, and the importance of data integrity (Kavanagh & Johnson, 2018). Regular training helps staff members stay current with evolving information management standards and technological advancements. Protecting HR data from unlawful access and cyber threats is essential to preserving its integrity. Smith and Watson (2020) recommend implementing contemporary safety measures such as encryption, multi-factor authentication, and intrusion detection systems. These safeguards ensure the reliability of critical HR data and shield it from security breaches.

Standardising data input processes lowers the likelihood of mistakes and anomalies in HR data. Bondarouk et al. (2017) advise using consistent designs, selectable options, and validation rules to ensure consistency in data submission. This process reduces the likelihood of record duplication, formatting errors, and missing data. Disjointed HR systems can lead to data silos and inconsistencies. According to Marler and Boudreau (2017), the integration of HR systems is recommended to enable seamless data transmission between departments. By guaranteeing that modifications made to one module (such as payroll) are automatically incorporated into other modules (like benefits), integrated systems reduce the likelihood of inconsistencies. Measuring data quality is necessary to preserve the integrity of HR data. Lee and Kim (2022) suggest establishing key performance indicators (KPIs) such as timeliness, correctness, and completeness to assess the quality of data.

Organisations that regularly monitor these indicators can ensure the accuracy of their data and identify areas for development. Employees can play a vital role in maintaining the accuracy of HR data by verifying their self-reports. Self-service portals should be established to enable employees to review and update their information, according to Martinez and Rodriguez (2023). This process reduces the strain on HR staff while ensuring that data is accurate and current. Compliance with data protection regulations, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), is necessary to maintain the integrity of HR data. Zhang et al. (2023) emphasise that adherence to these guidelines ensures data security, accuracy, and transparency while reducing the likelihood of penalties and reputational loss. To maintain accurate and dependable HR data, a combination of strong management structures, contemporary technology, employee training, and regulatory compliance is required. By implementing these ideal practices, organisations can enhance decision-making procedures, protect the privacy of HR data, and promote trust among stakeholders and employees.

4. RESULTS AND DISCUSSION

Several significant findings from the study indicate that data integrity in HRIS is crucial for business performance, ensuring legal and regulatory compliance, and fostering employee trust. These findings, which highlight the intricate consequences of compromised data integrity in HRIS, are supported by recent academic studies. According to the report, reliable and accurate HR data is essential for effective decision-making. According to Marler and Boudreau (2017), HRIS is a crucial tool for workforce planning, talent management, and strategic HR initiatives. Poor recruiting decisions or inappropriate training programs are just two examples of how inaccurate information can lead to bad decisions that eventually affect an organisation's success. Disparities in employee performance data, for instance, could lead to biased advertising campaigns or unfair performance appraisals, ultimately reducing worker productivity and satisfaction. If the integrity of HRIS data is compromised, there could be severe legal and regulatory consequences. Martinez and Rodriguez (2023) point out that for organisations to adhere to data protection regulations such as the CCPA and the GDPR, they must maintain correct and secure HR data. Noncompliance may result in severe fines, legal action, and damage to one's reputation. For example, inaccurate payroll data can lead to labour law infractions, which could expose companies to fines and legal action.

As stated by Johnson et al. (2021), inaccurate payroll information or improperly administered incentives are examples of HR data errors that might erode employees' trust in the company. These results demonstrate the close relationship between data integrity and employee confidence and satisfaction. Employees who feel their data is being handled incorrectly are more likely to quit or seek employment elsewhere. This demonstrates how important it is for companies to prioritise data accuracy to maintain a positive employer brand and attract and retain top personnel. Inaccurate data can lead to inefficient operations and increased costs. Time and money can be wasted while processing paychecks, administering benefits, and filing regulatory documents due to inaccurate HR data (Smith & Watson, 2020). For example, correcting errors in employee records or payment irregularities can strain HR teams and divert attention from strategic objectives. The need to use technology to protect the confidentiality of data in HRIS is emphasised in the paper. According to Davenport and Ronanki (2018), advanced technologies such as artificial intelligence (AI) and machine learning can reduce human error, systematise data validation, and spot anomalies. For instance, AI-powered systems can detect disparities in employment records or predict potential information breaches, enabling proactive measures to preserve data integrity.

This study highlights the importance of robust data governance mechanisms in maintaining the accuracy of HR data. Organisations should establish clear data management policies, roles, and accountability frameworks, according to Tallon et al. (2019). Regular audits, information quality metrics, and staff training are essential elements of sound data governance. For example, assigning data stewards to oversee HR data can help ensure its accuracy and consistency. Data integrity is also crucial for important HR tasks, such as workforce analytics and talent management, according to this report. As noted by Bondarouk et al. (2017), inaccurate data can undermine the credibility of HR analytics, lead to poor personnel planning, and have negative business effects. For instance, erroneous employee skill and competency data may result in ineffective talent development programs that hinder the organisation's growth.

This study emphasizes the importance of flexibility and continuous development in maintaining the accuracy of HR data. According to Kavanagh and Johnson (2018), companies must stay informed about evolving legal requirements and technological advancements to safeguard their HR data. For example, implementing cloud-based HRIS systems can enhance data availability and security. At the same time, regular training sessions can ensure that HR staff members are adequately prepared to manage the data effectively. The study's findings underscore the importance of data integrity in HRIS for fostering employee trust, ensuring legal compliance, and driving commercial success. By addressing the problems associated with compromised data integrity and implementing best practices such as robust data governance, modern technology, and continuous improvement, organisations may ensure the accuracy and reliability of their HR data. As a result, this enhances operational effectiveness, fosters a positive work environment, and facilitates easier decision-making.

5. CONCLUSION

The goal of this study was to examine the significance of data integrity in human resources (HR) information systems. This study successfully achieved its objective by closely examining the role that data integrity plays in ensuring the accuracy, reliability, and assurance of HR data. Using a range of secondary sources, the study identified key causes of data integrity issues, such as human error, technology defects, and inadequate data management practices. The findings highlighted the importance of implementing robust data validation protocols, conducting regular audits, and providing staff training programs to mitigate risks and maintain data integrity. By providing helpful recommendations and demonstrating how it directly impacts organisational effectiveness and decision-making, the study effectively emphasised the significance of data integrity in HRIS, fulfilling its primary objective. The quality of the primary research cited in secondary sources and review papers, which establishes their accuracy and reliability, was one of the investigation's shortcomings.

Any biases or errors in the original data will be carried over into the secondary assessment. Secondary sources and review papers are unable to address specific research topics or explore new patterns that were not included in the original study because they do not generate original information. Review article or secondary source authors may incorporate their biases while selecting, analysing, or synthesising prior research, which could skew the findings. A few strategies were implemented to overcome the limitations of review papers and secondary sources: Examine the quality, correctness, and authenticity of the primary research that forms the basis of the analysis using strict evaluation criteria. The scientific integrity of the original studies was thoroughly evaluated using PRISMA criteria. Examine several secondary sources and articles to cross-check your findings. Finding discrepancies and producing a more impartial perspective can be facilitated by combining data from many sources. To identify and address any potential biases or methodological errors, secondary analyses and review papers underwent thorough peer review.

A thorough understanding of data management, cleaning techniques, and the nuances of the data being used is necessary to secure high-quality data. Lack of training is one reason why data quality is still a persistent problem. Inadequate training could lead to incorrect data handling practices, a lack of knowledge about data standards, and insufficient competence with data quality tools. This could lead to errors, incomplete records, and a lack of confidence in the accuracy of the information. Without data integrity, HR professionals could encounter it challenging to make educated decisions about workforce management, talent development, and other crucial HR initiatives. HR practitioners face several difficulties, including high conversion costs from traditional to automated HRM, inadequate employee training, and a lack of technological and infrastructure expertise (Hashim, 2015; Quaosar, 2018; Zafar, 2013).

Improper data integrity can lead to improper payroll calculations, compliance issues, and legal issues. Data integrity must be maintained in human resources information systems, as it has a direct impact on employee trust, compliance, and informed decision-making. Accurate data ensures that legal requirements are met, payroll processes are accurate, and benefits are distributed in a timely and appropriate manner. Any compromise carries the risk of significant errors, substantial financial losses, and potentially severe legal consequences. Additionally, preserving data integrity fosters employee confidence in the HR system, which makes the workplace more transparent and reliable. Think about the consequences of a single personnel record error. This demonstrates the intricate web of connections that exist within an organisation and the necessity of maintaining absolute data integrity.

Organisations should implement thorough data verification and validation processes, regularly audit, sterilise the data, and train HR staff on data management best practices to ensure data integrity in an HRIS. Future research should focus on examining strategies for maintaining data integrity, like frequent audits, validation standards, and data encryption. These can demonstrate how technology enhances the efficiency of HR processes while safeguarding sensitive employee data. This topic also sparks an intriguing discussion about how emerging technologies, such as blockchain, could further enhance data integrity in HRIS.

Although a study note is useful for quickly conveying first findings or observations, it has certain disadvantages. It usually provides a less comprehensive analysis than complete research articles; as a result, it may omit important background information, methodology, or material. The depth of discussion and the range of data presented may be limited because they are often shorter. Future studies can concentrate on (i) Examining how blockchain technology can be integrated with HRIS to build an impenetrable system that enhances data integrity and security.

(ii) Assess the effectiveness of various software tools and technologies to improve data integrity in information systems related to human resources. (iii) Analyse the connection between high data integrity in HRIS and staff retention rates, paying special emphasis to how accurate data may boost employee confidence and loyalty.

ACKNOWLEDGEMENTS

I am grateful to the Nkangala District Municipality for allowing me to conduct this study within their organisation.

FUNDING STATEMENT

This study was not supported by any grants from funding bodies in the public, private, or not-for-profit sectors.

AUTHORS' CONTRIBUTION

D.S. Mdhlalose (Conceptualization; Formal analysis; Visualisation; Supervision); D.S. Mdhlalose (Methodology; Data curation; Writing - original draft; Resources)

AVAILABILITY OF DATA AND MATERIALS

The data supporting this study's findings are available on request from the corresponding author.

CONFLICTS OF INTEREST

The author declares no conflicts of interest.

REFERENCES:

Almadhoun, R., Kadry, S., & Balakrishnan, V. (2021). Trust in Digital Systems: A Review of Challenges and Solutions. Journal of Information Security and Applications, 58, 102735.

Alomari, A. S. (2019). The Role of Human Resources Information Systems in Improving the Performance of Human Resources Management. *Indian Journal of Science and Technology*, *12*(35), 01–06. https://doi.org/10.17485/ijst/2019/v12i35/147859

Bondarouk, T., Parry, E., & Furtmueller, E. (2017). Electronic HRM: Four Decades of Research on Adoption and Consequences. International Journal of Human Resource Management, 28(1), 98–131. https://doi.org/10.1080/09585192.2016.1245672

Brown, T., Green, R., & White, P. (2021). The Consequences of Data Integrity Breaches in Scientific Research. Research Policy, 50(3), 104-118.

Cote, C. (2021). What Is Data Integrity and Why Does It Matter? https://online.hbs.edu/blog/post/what-is-data-integrity

Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World. Harvard Business Review, 96(1), 108-116. https://www.bizjournals.com/boston/news/2018/01/09/hbr-artificial-intelligence-for-the-real-world.html

Dolowitz, D. P., Buckler, S., & Sweeney, F. (2008). *Researching online*. Red Globe Press.

Duggineni, S. (2023). Data Integrity and Risk. *Open Journal of Optimisation*, 12, 25-33. https://doi.org/10.4236/ojop.2023.122003

Fox, W., & Bayat, M. S. (2007). *A Guide to: Managing Research*. Cape Town: Juta & Co Ltd.

Garcia, M., Rodriguez, L., & Martinez, P. (2023). Integrating AI and IoT in Data Governance Frameworks. Data Science and Management, 18(1), 45-60.

Hashim, J. (2015). Information Communication Technology (ICT) Adoption among SME Owners in Malaysia. International Journal of Business and Information, 2, 221-240.

Johnson, M., Smith, K., & Williams, L. (2021). The Impact of Data Integrity Breaches on Healthcare Quality and Patient Safety. Journal of Medical Systems, 45(4), 1-10.

Kavanagh, M. J., & Johnson, R. D. (2018). Human Resource Information Systems: Basics, Applications, and Future Directions. SAGE Publications.

Khan, R., McLaughlin, K., & Laverty, D. (2022). Data Integrity Attacks on Critical Infrastructure: A Review of Risks and Mitigation Strategies. Computers & Security, 113, 102557.

Kumar, R., Singh, S., & Gupta, P. (2023). Blockchain for Data Integrity: A Comprehensive Review. International Journal of Distributed Systems, 12(2), 89-102.

Lee, H., & Kim, S. (2022). The Impact of Data Integrity Breaches on Organisational Reputation and Consumer Trust. Journal of Business Ethics, 175(2), 345-360.

Li, X., & Chen, Y. (2023). Machine Learning for Anomaly Detection in Data Integrity Management. IEEE Transactions on Knowledge and Data Engineering, 35(4), 567-580.

Markham, A. N., & Baym, N. K. (2009). *Internet inquiry: Conversations about method*. L A. Los Angeles: Sage Publications.

Marler, J. H., & Boudreau, J. W. (2017). An Evidence-Based Review of HR Analytics. International Journal of Human Resource Management, 28(1), 3-26. https://doi.org/10.1080/09585192.2016.1244699

Martinez, A., & Rodriguez, P. (2023). Legal Implications of Data Integrity Breaches in the Era of GDPR and CCPA. Journal of Cybersecurity and Privacy, 3(1), 45-60.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & the PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & McGuinness, L. A. (2021). The PRISMA 2020 statement: an Updated Guideline for Reporting Systematic Reviews. British Medical Journal, 372(71). https://doi.org/10.1136/bmj.n71

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Patel, S., Brown, T., & Lee, K. (2023). Building a Culture of Data Integrity: Strategies and Best Practices. Journal of Organisational Cybersecurity, 14(2), 210-225.

Quaosar, G. M. A. A. (2018). Adoption of Human Resource Information Systems in Developing Countries: An Empirical Study. *International Business Research*, 11, 133. https://doi.org/10.5539/ibr.v11n4p133

Quaosar, G. M. A. A., & Rahman, Md. S. (2021). Human Resource Information Systems (HRIS) of Developing Countries in 21st Century: Review and Prospects. *Journal of Human Resource and Sustainability Studies*, 9, 470-483. https://doi.org/10.4236/jhrss.2021.93030

Rietsema, D. (2023). Maintaining Data Integrity Throughout HRIS Implementation. https://matchr.com/hris-software/maintaining-data-integrity-throughout-hris-implementation/

Sluzki, N. (2023). Data Integrity Issues: Examples, Impact, And 5 Preventive Measures. https://databand.ai/blog/data-integrity-issues-examples-preventive-measures/

Smith, J., & Watson, R. (2020). The Financial Impact of Data Integrity Breaches in Supply Chain Management. *International Journal of Production Economics, 220*, 107460.

Stone, D. L., & Deadrick, D. L. (2015). Challenges and Opportunities Affecting the Future of Human Resource Management. Human Resource Management Review, 25(2), 139-145. https://doi.org/10.1016/j.hrmr.2015.01.003

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2019). The Role of Data Governance in Ensuring Data Quality and Integrity. Journal of Management Information Systems, 36(4), 1241-1265.

Tobin, D., Stone, M. J., Townsend, A., Perper, H., & Weeks, S. (2016). Data Integrity: Recovering from A Destructive Malware Attack. http://www.nist.gov

Udekwe, E., & De la Harpe, A. C. (2017). The use of human resource information systems in two retail organisations in the Western Cape, South Africa. *SA Journal of Human Resource Management/SA Tydskrif vir Menslikehulpbronbestuur*, 15(0), a827. https://doi.org/10.4102/sajhrm.v15i0.827

Wang, A. (2024). Enhancing HR management through HRIS and data analytics. *Applied and computational engineering*, 64(1), 223-229. https://doi.org/10.54254/2755-2721/64/20241394

Weeks, K. O. (2013). An Analysis of Human Resource Information Systems Impact on Employees. *Journal of Management Policy and Practice*, 14(3), 35 – 49.

White, D. (2019). Why Data Integrity is Critical for Human Resources. https://www.techfunnel.com/hr-tech/why-data-integrity-is-critical-for-human-resources/

Zafar, H. (2013). Human Resource Information Systems: Information Security Concerns for Organizations. *Human Resource Management Review*, 23, 105-113. https://doi.org/10.1016/j.hrmr.2012.06.010

ZeroedIn. (2021). Achieving HR Data Integrity is Easier Than You Think. https://www.zeroedin.com/how-to-achieve-hr-data-integrity/

Zhang, Y., Wang, H., & Liu, J. (2023). Big Data Security and Integrity: Challenges and Solutions. Journal of Information Systems, 45(3), 123-135.

Zhang, Y., Wang, L., & Chen, X. (2023). The Social and Ethical Implications of Data Integrity Breaches in the Digital Age. Ethics and Information Technology, 25(1), 1-15.