E-HR Records in Zimbabwe: Balancing Data Privacy, Security, and Regulatory Compliance

Nothando Tutani[1], Getrude Mavunga [1]

[1]Zimbabwe Open University

*Corresponding Author's Email: mavungag@zou.ac.zw

Received: 15 March 2025| Accepted: 5 May 2025| Published: 31 May 2025

Abstract

The adoption of electronic Human Resource (e-HR) records is transforming HR management globally, offering enhanced efficiency, accessibility, and decision-making. However, in Zimbabwe, organisations face significant challenges in data privacy, cybersecurity, and regulatory compliance, hindering the full realisation of e-HR benefits. This study examined the current state of e-HR adoption in Zimbabwe, comparing it to global best practices and identifying critical gaps in technological infrastructure, legal enforcement, and cybersecurity readiness. Using a Systematic Literature Review (SLR), the study applied the Technology-Organisation-Environment (TOE) framework, GDPR principles, and the CIA Triad model to analyse Zimbabwe's HR digitalisation landscape. Findings revealled uneven adoption rates, with large organisations progressing faster than SMEs, weak regulatory enforcement, and high vulnerability to cyber threats due to limited security investments. The study proposed strategic interventions, including strengthening regulatory oversight, enhancing cybersecurity measures, and aligning HR practices with international standards. The findings contributed to the discourse on HR digital transformation in emerging economies, offering policy recommendations to ensure a secure and efficient transition to digital HR records in Zimbabwe.

Keywords: Cybersecurity, Data privacy, Regulatory compliance, HR digitalisation, TOE framework, CIA Triad

Introduction

The rapid digital transformation of Human Resource Management (HRM) has fundamentally reshaped how organisations manage employee records. Across the globe, the transition from paper-based to Electronic Human Resource (e-HR) records has revolutionised efficiency, accessibility, and decision-making in HR operations (Bondarouk et al., 2011). In Zimbabwe, organisations are gradually embracing e-HR systems to streamline HR processes, ensure regulatory compliance, and align with international best practices (Mutumwa et al., 2024; Tapiwa et al., 2022). However, despite the potential benefits, the widespread adoption of digital HR systems presents significant challenges, particularly concerning data privacy, cybersecurity vulnerabilities, and regulatory compliance gaps. As Chigada and Madzinga (2021) caution, while organisations increasingly rely on electronic platforms to store and process sensitive employee information, the risk of data breaches, cyber threats, and legal non-compliance has become a pressing concern.

A critical issue facing Zimbabwean organisations is their struggle to implement robust cybersecurity measures due to insufficient investment in digital infrastructure and a shortage

of technical expertise (Chigada, 2021; Chingoriwo, 2022). Moreover, the absence of a comprehensive data protection framework exacerbates these challenges, leaving HR practitioners navigating an inconsistent and fragmented regulatory landscape (Moyo et al., 2024). Although the Cyber and Data Protection Act (2021) marked a significant step toward formalising data governance, enforcement remains weak, and many organisations continue to operate with minimal safeguards. Additionally, as globalisation increases cross-border HR data exchanges, Zimbabwean businesses must align with stringent international standards, such as the General Data Protection Regulation (GDPR), which adds another layer of complexity and compliance risk (GDPR, 2016).

While studies have explored general HR digitalisation trends in Africa, a few provided a comprehensive, context-specific analysis that integrates data privacy, cybersecurity, and regulatory compliance within Zimbabwe's evolving digital landscape. This study addresses this critical gap by offering a systematic examination of Zimbabwe's e-HR operational framework, identifying contextual barriers, and proposing strategic interventions tailored to resource-constrained environments.

By employing a Systematic Literature Review (SLR) approach, this study ensures a rigorous, transparent, and replicable synthesis of existing research, uncovering practical insights for HR practitioners, policymakers, and researchers. Unlike previous works, which often focus on isolated aspects of digital HR transformation, this research takes a holistic approach by examining the interplay between cybersecurity risks, data privacy regulations, and HR operational efficiency in Zimbabwe. The findings contribute to the broader HRM discourse by providing evidence-based recommendations for securing HR records, strengthening regulatory compliance, and fostering a sustainable digital HR ecosystem in Zimbabwe and similar emerging economies.

While e-HR adoption in Zimbabwe enhances efficiency and decision-making, it also introduces significant risks related to data privacy, cybersecurity, and regulatory compliance. Many organisations lack the technical expertise and financial resources to implement robust cybersecurity measures, leaving sensitive employee data vulnerable to breaches and unauthorised access (Chigada & Madzinga, 2021). These risks are compounded by a fragmented regulatory framework and inconsistent enforcement of the Cyber and Data Protection Act (2021) (Moyo et al., 2024; Poshai et al., 2023). This study examines how Zimbabwean organisations can navigate these challenges and achieve a balance between digital transformation, data security, and regulatory compliance in managing e-HR records.

The study was guided by the following research objectives:

- To assess the current state of e-HR records adoption in Zimbabwe.
- To evaluate the data privacy concerns associated with e-HR records in Zimbabwe
- To examine the cybersecurity risks faced by Zimbabwean organisations in managing e-HR records.
- To analyse the regulatory compliance challenges encountered by organisations in aligning their HR data management practices with both local legislation, such as the Cyber and Data Protection Act, and international standards, such as the General Data Protection Regulation (GDPR).
- To identify best practices and strategic interventions that organisations can adopt to enhance data security, privacy, and regulatory compliance in e-HR records management.

Literature Review

State of e-HR Records Adoption in Zimbabwe

Globally, the digitalisation of HR records has gained significant traction, with organisations across various industries adopting advanced HR Information Systems (HRIS) to manage their workforce more effectively. This trend is particularly relevant in emerging economies like Zimbabwe, where organisations are increasingly recognising the need to modernise their HR practices to keep pace with global standards (Mutumwa et al., 2024). The adoption of e-HR records in Zimbabwe is driven by the desire to enhance operational efficiency, improve data accuracy, and ensure compliance with evolving regulatory frameworks. However, this transition is not without its challenges, as many Zimbabwean organisations grapple with issues such as limited technological infrastructure, cybersecurity concerns, and a lack of technical expertise (Vusumuzi, 2024). Despite these hurdles, the potential benefits of e-HR records make them a critical component of HRM in Zimbabwe, offering a pathway to improved organisational performance and competitiveness. However, the current state of HRIS adoption in Zimbabwe remains uneven, with larger organisations and multinational corporations leading the way, while small and medium-sized enterprises (SMEs) lag due to resource constraints and limited technological infrastructure (Mukuze, 2023; Vusumuzi, 2024).

Additionally, the introduction of the Cyber and Data Protection Act (2021) has created a regulatory imperative for Zimbabwean organisations to adopt secure e-HR data management systems. Despite these drivers, the adoption process is fraught with challenges. Many Zimbabwean organisations face significant challenges in aligning the collection, storage and dissemination of e-HR records in line with the requirements of the Act given the high implementation costs, a lack of technical expertise, and resistance to change among employees (Vusumuzi, 2024). Furthermore, the fragmented nature of the country's technological infrastructure exacerbates these challenges, particularly in rural areas where internet connectivity and access to digital tools are limited (Mukuze, 2023).

Data Privacy and e-HR Records in Zimbabwe

The protection of employee data is a critical aspect of Human Resource Management (HRM), particularly given the sensitive nature of personal information contained in HR records, such as personally identifiable details, medical records, and performance evaluations (Zafar, 2023). In Zimbabwe, the adoption of electronic HR systems has heightened concerns over data privacy, as many organisations lack robust cybersecurity measures, leaving employee data vulnerable to breaches and unauthorised access (Chigada & Madzinga, 2021). Similarly, in South Africa, the implementation of the Protection of Personal Information Act (POPIA) has emphasised the need for stringent data protection measures, yet challenges persist in ensuring compliance and safeguarding sensitive information. Effective data privacy frameworks are essential to mitigate risks such as identity theft, financial fraud, and reputational damage, which can have severe consequences for both employees and organisations (Kajongwe, 2020). In both contexts, balancing digitisation with ethical data handling remains a pressing priority.

Regulatory Compliance Issues in e-HR Document Management

Ensuring compliance with data protection regulations is critical for HR data management, particularly as organisations transition from traditional paper-based records to electronic HR systems. Regulatory frameworks must address key concerns such as data privacy, security, and cross-border data transfers, aligning with global standards to protect employee information. However, in Zimbabwe, compliance challenges persist due to gaps in legal enforcement, weak institutional oversight, and misalignment with international best practices. As noted previously,

the Cyber and Data Protection Act (2021) was introduced to provide a structured regulatory framework, but its implementation remains problematic. The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), as the primary data protection authority, plays a crucial role in overseeing compliance; however, its failure to ensure robust enforcement and international alignment has significantly hindered progress.

Zimbabwe's approach to data privacy has been characterised by a fragmented and evolving regulatory landscape. Historically, the country lacked comprehensive data protection laws, leaving organisations to navigate a complex web of sector-specific regulations and international guidelines (Moyo et al., 2024). This regulatory inconsistency has led to significant gaps in data privacy enforcement, making it difficult for businesses to implement standardised HR data management practices. Therefore, many organisations in Zimbabwe struggle with balancing compliance requirements while leveraging electronic HR systems for efficiency and decision-making (Poshai et al., 2023).

In fact, the absence of a unified legal framework that incorporates HR such as the POPII Act in South Africa has further complicated matters, as Zimbabwean organisations must reconcile conflicting obligations under local and international standards, such as the General Data Protection Regulation (GDPR) (Boshe et al., 2022). This regulatory ambiguity has resulted in uneven adoption of data protection measures, with some organisations prioritising compliance while others lag due to resource constraints or lack of awareness.

The enactment of the Cyber and Data Protection Act (2021) in Zimbabwe marked a significant milestone in the country's data governance framework as it represents the first comprehensive legislation aimed at regulating the collection, storage, and processing of personal data, including HR records (Government of Zimbabwe, 2021). The Act introduces critical provisions to safeguard employee privacy, such as requiring data controllers and processors to obtain consent before collecting personal information, ensuring data accuracy, and implementing security measures to prevent unauthorised access or breaches (Kajongwe, 2020). It also establishes accountability mechanisms, mandating organisations to maintain records of data processing activities and report data breaches to the relevant authorities. Penalties for non-compliance, including fines and legal sanctions, are outlined to deter violations and promote adherence to data protection standards.

Despite the existence of the Cyber and Data Protection Act (2021), Zimbabwean organisations face significant implementation challenges. POTRAZ (the Postal and Telecommunications Regulatory Authority of Zimbabwe) has notably failed to provide clear compliance frameworks and capacity-building initiatives for organisations adopting electronic HR systems (Poshai et al., 2023). This failure stands in stark contrast to Kenya's Communications Authority, which has established comprehensive guidelines and training programmes following their Data Protection Act implementation, resulting in 65% higher compliance rates among organisations. As Kajongwe (2022) reports, many Zimbabwean HR departments lack awareness of legal requirements, complicating compliance efforts. Similarly, POTRAZ has not established effective monitoring and enforcement mechanisms. While South Africa's Information Regulator conducts regular audits and has imposed penalties on over 30 non-compliant organisations since 2020, POTRAZ's enforcement remains inconsistent despite stipulated penalties in the Act. This regulatory vacuum in Zimbabwe allows organisations to operate without meeting necessary data security standards, exposing employee data to unauthorised access, breaches, and misuse - issues that neighbouring Botswana has largely avoided through its Data Protection Commission's proactive compliance verification programme.

Given the global nature of electronic HR systems, Zimbabwean organisations must also be aligned with international data protection frameworks, such as the General Data Protection Regulation (GDPR). The GDPR mandates strict data protection measures, including lawful processing, data minimisation, and obtaining explicit employee consent in HR data handling (European Union, 2016). These requirements set a high standard for data privacy and security, which many Zimbabwean organisations struggle to meet due to differences in regulatory structures, resource limitations, and inadequate cybersecurity infrastructure (Chingoriwo, 2022). For instance, the GDPR's emphasis on data minimisation and the right to erasure poses challenges for organisations accustomed to less stringent local regulations. Without alignment with global practices, Zimbabwean organisations risk non-compliance, which could lead to reputational damage, financial penalties, and legal repercussions in global HRM practices. However, POTRAZ has failed to align Zimbabwe's data protection policies with international best practices, leaving organisations with legal uncertainties and compliance risks (Kajongwe, 2020). Without international alignment, Zimbabwean businesses face barriers to global partnerships and trade, as international stakeholders require compliance with GDPR or equivalent standards (Chigada & Madzinga, 2021). Many Zimbabwean organisations lack data protection officers, cybersecurity training, and adequate digital infrastructure, further complicating compliance efforts (Moyo et al., 2024).

Cybersecurity Risks in HR Digitalisation

The risk of unauthorised access, data breaches, and cyberattacks has escalated as organisations increasingly rely on digital platforms to store and process sensitive employee information (Chigada & Madzinga, 2021). Common cybersecurity threats include phishing attacks, ransomware, and insider threats, all of which can compromise the confidentiality, integrity, and availability of HR data (Whitman & Mattord, 2009). The consequences of such breaches are severe, ranging from identity theft and financial fraud to reputational damage and legal liabilities, underscoring the critical need for robust cybersecurity measures in HR digitalisation (Kajongwe, 2020).

In Zimbabwe, the adoption of e-HR record management has exposed organisations to heightened cybersecurity risks, exacerbated by a lack of investment in cybersecurity infrastructure and expertise (Maponga, 2016; Kajongwe, 2020). Many Zimbabwean organisations operate with limited resources, prioritising immediate operational needs over long-term cybersecurity investments (Chingoriwo, 2022). This has resulted in inadequate protection mechanisms, such as weak encryption protocols, insufficient access controls, and a lack of regular security audits. Furthermore, the absence of skilled cybersecurity professionals in the country has left organisations ill-equipped to detect and respond to cyber threats effectively (Vusumuzi, 2024). These gaps in cybersecurity infrastructure and expertise have made HR e-records particularly vulnerable to attacks, with potentially devastating consequences for both employees and organisations.

Theoretical Framework

This study adopted a multidisciplinary theoretical framework that integrates insights from technology adoption, data privacy regulations, and information security principles to examine the challenges and opportunities of electronic HR (e-HR) records adoption in Zimbabwe. The framework was structured around three key components: the Technology-Organisation-Environment (TOE) framework, the General Data Protection Regulation (GDPR) and Zimbabwe's Cyber and Data Protection Act (2021), and the CIA triad (Confidentiality, Integrity, and Availability) for cybersecurity risk management.

Technology-Organisation-Environment (TOE) Framework

The TOE framework (Tornatzky et al., 1990) serves as the foundation for analysing e-HR adoption by examining the factors influencing digital transformation in organisations. It provided a structured approach by categorising influences into:

- Technological Context – Infrastructure readiness, cybersecurity measures, and digital literacy in Zimbabwean organisations.
- Organisational Context – HR competencies, financial capacity, and leadership commitment to digital transformation.
- Environmental Context – The regulatory landscape, government policies, and competitive pressures affecting e-HR adoption.

GDPR and Cyber & Data Protection Act (2021)

This study incorporated principles from GDPR (European Union, 2016) and Zimbabwe's Cyber and Data Protection Act (2021) to evaluate how organisations adhere to data privacy, security, and compliance standards. The analysis will focus on:

- Data Minimisation and Consent – Assessing whether Zimbabwean organisations collect only essential employee data and obtain proper consent.
- Accountability and Transparency – Evaluating whether HR departments have clear policies for handling, processing, and storing employee records.
- Regulatory Enforcement – Investigating gaps in POTRAZ's enforcement of Zimbabwe's Cyber and Data Protection Act and its alignment with global best practices.

By incorporating these frameworks, the study explored compliance gaps, regulatory challenges, and potential areas for policy improvement in Zimbabwe.

The CIA Triad (Confidentiality, Integrity, Availability)

Cybersecurity risks remained a major barrier to e-HR adoption. The CIA triad (Whitman & Mattord, 2009) provides a foundation for assessing data protection measures in HR digitalisation:

- Confidentiality – Investigates whether HR records are protected from unauthorised access through encryption and access controls.
- Integrity – Analyses data accuracy and protection against unauthorised modifications in HR systems.
- Availability – Examines system uptime, backup mechanisms, and disaster recovery plans for HR data accessibility.

By applying the CIA triad, organisations can create a multi-layered defence against cyber threats, reducing the likelihood of data breaches and ensuring the secure management of HR records.

Balancing Data Privacy, Security, and Regulatory Compliance

Cybersecurity, and regulatory compliance in e-HR records management, organisations must adopt a multi-faceted approach that combines technological, organisational, and cultural interventions to address the challenges of data privacy. Strengthening cybersecurity infrastructure is a critical first step in protecting HR e-records from breaches and unauthorised access. This included implementing advanced encryption protocols, multi-factor authentication, and regular security audits to identify and mitigate vulnerabilities (Whitman & Mattord, 2009). Additionally, organisations should invest in robust HR Information Systems (HRIS) with built-in security features, such as access controls and audit trails, to ensure the

confidentiality, integrity, and availability of employee data (Chigada & Madzinga, 2021). By prioritising cybersecurity infrastructure, organisations could reduce the risk of data breaches and build a secure foundation for HR digitalisation.

Enhancing regulatory compliance is another essential component of effective HR data management. This can be achieved through targeted training programmes that educate employees and HR professionals on data protection laws, such as Zimbabwe's Cyber and Data Protection Act (2021) and the General Data Protection Regulation (GDPR) (European Union, 2016). Training should focus on practical aspects of compliance, such as obtaining employee consent, minimising data collection, and reporting data breaches. Furthermore, organisations must develop and implement clear data protection policies that align with regulatory requirements. These policies should outline roles and responsibilities, establish procedures for data handling, and provide guidelines for responding to security incidents (Moyo et al., 2024). By fostering a culture of compliance, organisations can minimise legal risks and build trust with stakeholders.

Adopting international best practices in HR data security is also crucial for organisations seeking to align with global standards. This includes benchmarking against frameworks such as the ISO/IEC 27001 standard for information security management and the GDPR's principles of data minimisation and accountability (Namalawa, 2023). Organisations should also consider partnering with cybersecurity experts and leveraging emerging technologies, such as artificial intelligence and blockchain, to enhance data security and transparency.

Finally, developing a data protection culture within organisations is essential for sustaining long-term compliance and security. This involves promoting awareness of data privacy and cybersecurity at all levels of the organisation, from leadership to frontline employees. Leadership must champion data protection initiatives, allocate resources for cybersecurity, and lead by example in adhering to policies (Vusumuzi, 2024). Regular communication, training, and awareness campaigns can help embed data protection principles into the organisational culture, ensuring that employees understand their role in safeguarding HR e-records. By fostering a culture of accountability and vigilance, organisations can create a sustainable framework for managing e-HR records securely and ethically.

Synthesis of Literature and Knowledge Gap

A critical issue emerging from the literature is the tension between the benefits of e-HR records and the associated risks, particularly concerning data privacy and cybersecurity. While electronic systems offer advantages such as real-time data access, automation, and improved data integrity (Bondarouk et al., 2011; Zveushe, 2023), they also expose organisations to heightened risks of data breaches, unauthorised access, and cyberattacks (Chigada & Madzinga, 2021). In Zimbabwe, these risks are exacerbated by inadequate cybersecurity infrastructure, limited technical expertise, and a fragmented regulatory landscape (Chingoriwo, 2022; Kajongwe, 2020). Despite the introduction of the Cyber and Data Protection Act (2021), which aims to regulate data collection, storage, and processing, implementation challenges persist, leaving many organisations struggling to align their HR practices with legal requirements (Moyo et al., 2024; Poshai et al., 2023). This highlights a gap in understanding how Zimbabwean organisations, particularly SMEs, can navigate the complexities of regulatory compliance while ensuring robust data protection.

Furthermore, the literature reveals a lack of alignment between Zimbabwe's data protection laws and international standards such as the General Data Protection Regulation (GDPR).

While the GDPR sets stringent requirements for data privacy and security, including lawful processing, data minimization, and employee consent (European Union, 2016), Zimbabwe's regulatory framework remains underdeveloped and inconsistently enforced (Kajongwe, 2020; Vusumuzi, 2024). This regulatory ambiguity underscores the need for research that explores how Zimbabwean organisations can harmonise their HR data management practices with global standards, particularly in the context of cross-border data transfers and international partnerships.

Cybersecurity risks also emerge as a pressing concern, with HR e-records being particularly vulnerable to exploitation due to the sensitive nature of the data they contain (Whitman & Mattord, 2009). In Zimbabwe, limited investment in cybersecurity infrastructure and a shortage of skilled professionals have left organisations ill-equipped to address these risks effectively (Maponga, 2016; Chingoriwo, 2022). While frameworks such as the CIA triad (Confidentiality, Integrity, and Availability) offer foundational strategies for securing HR e-records, their implementation in resource-constrained environments like Zimbabwe remains underexplored. This gap highlights the need for research that identifies cost-effective and context-specific cybersecurity measures for Zimbabwean organisations, particularly SMEs, to protect HR e-records from breaches and unauthorised access.

This study adopts a PRISMA-based Systematic Literature Review (SLR) methodology to address these gaps. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) provides a rigorous, transparent, and replicable framework for synthesising existing research, ensuring that findings are grounded in credible evidence. By systematically analysing academic literature and legal frameworks, this study aims to identify best practices, highlight implementation challenges, and provide evidence-based recommendations for Zimbabwean organisations.

Research Methodology

This study employed a PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses)-based Systematic Literature Review (SLR) methodology to explore the challenges and opportunities associated with e-HR records in Zimbabwe. Specifically, the focus was on data privacy, cybersecurity, and regulatory compliance within the context of emerging economies. The PRISMA framework ensured a rigorous, transparent, and replicable approach to synthesising existing research, enabling the identification of key themes, gaps, and trends in the literature. The SLR approach was particularly suited to this research, as it enables the integration of insights from multiple disciplines, offering a comprehensive understanding of the complexities of e-HR records management in a Zimbabwean context. This makes room for the study to address the identified gaps and contribute to the broader discourse on e-HR use in emerging economies. In line with the tenets of the PRISMA approach, the methodology in this study followed four main phases:

Data sources and search strategy

In this phase, a comprehensive search for academic literature, industry reports, and legal frameworks related to e-HR records, data privacy, cybersecurity, and regulatory compliance in Zimbabwe was conducted. Key databases such as Scopus, Web of Science, PubMed, and Google Scholar were searched using a combination of keywords and Boolean operators. Search terms included "electronic HR records,", "e-HR records" "HRIS," "data privacy," "cybersecurity," "regulatory compliance," "Zimbabwe," and "emerging economies." To ensure relevance and currency, the search was limited to peer-reviewed articles, conference papers, and grey literature published from 2010 to 2024. Additionally, legal documents such

as Zimbabwe's Cyber and Data Protection Act (2021) and the General Data Protection Regulation (GDPR) were included to provide regulatory context.

The study selection process followed the PRISMA framework and was conducted in four stages:

1. Identification: A total of 68 studies were retrieved through database searches and reference list reviews.
2. Screening: After total 19 items were excluded as there were deemed to be duplicates leaving 49 records for further evaluation.
3. Eligibility: A title and abstract review led to the exclusion of a further 18 studies that did not directly address e-HR records in a Zimbabwean context leaving 31 items for detailed assessment. A further 12 records were also excluded as they were not available as full-title versions.
4. Final Inclusion: After applying the inclusion and exclusion criteria, 19 studies were selected for synthesis. A PRISMA flow diagram summarising this process is presented below:

Table 1: PRISMA flow diagram

Stage	Number of Studies
Studies retrieved from databases	68
Screening: Number of duplicates removed	19
Eligibility: Studies excluded after title and abstract review	18
Studies excluded due to non-availability of full text	12
Final studies included in the systematic review	19

Inclusion and Exclusion Criteria

Inclusion Criteria

- Studies that focus on electronic HR records, HRIS, data privacy, cybersecurity, or regulatory compliance in Zimbabwe or similar emerging economies.
- Studies published in peer-reviewed journals, conference papers.
- Research discussing regulatory frameworks like Zimbabwe's Cyber and Data Protection Act (2021) and the GDPR.
- Studies published in English.

Exclusion Criteria

- Studies focusing solely on non-HR contexts (e.g., electronic records in healthcare or finance).
- Articles without empirical or theoretical grounding (e.g., opinion pieces or purely descriptive reports).
- Studies that are not published in English or do not meet quality standards.
- Duplicate publications or studies that do not contribute new data or insights.

Data Extraction and Synthesis

The selected studies underwent a structured data extraction process using a standardised template as recommended by Kitchenham and Brereton, (2013). The key information extracted included the study's objectives, methodologies, findings, and recommendations. The data were organised into thematic categories, which were identified through thematic analysis. The primary themes included:

- Adoption of e-HR records in Zimbabwe.

- Data privacy concerns and cybersecurity risks.
- Challenges related to regulatory compliance.
- Best practices and strategic interventions for managing e-HR records.

The thematic categories allowed for a focused synthesis of the literature and facilitated the identification of recurring patterns, gaps, and trends across the selected studies.

Analysis and Reporting of Findings

The extracted and synthesised data were analysed to address the research objectives and derive evidence-based recommendations. The analysis focused on understanding how data privacy, cybersecurity, and regulatory compliance interplay in e-HR records management in Zimbabwe. The findings were reported following PRISMA guidelines to ensure transparency, reproducibility, and accuracy

Results and discussion

The findings of this study revealled critical insights into the adoption, challenges, and opportunities associated with e-HR records in Zimbabwe, particularly in the areas of data privacy, cybersecurity, and regulatory compliance. These findings were contextualised within the broader global landscape, highlighting both alignments and deviations from international best practices.

Adoption of Electronic HR Records in Zimbabwe

The reviewed literature revealled that the adoption of e-HR records in Zimbabwe was progressing, albeit unevenly. Larger organisations were reported to be leading the transition, e-HR record keeping to streamlining HR processes, enhance data accuracy, and improve decision-making (Mutumwa et al., 2024; Zveushe, 2023). However, smaller organisations lag significantly due to resource constraints, limited technological infrastructure, and a lack of technical expertise (Mukuze, 2023; Vusumuzi, 2024). These findings were reflected in Table 2.

Table 2: Comparative analysis of Zimbabwe's e-HR adoption trends

Adoption Factor	Zimbabwe	Global Best Practices
Adoption Rates	Increasing but uneven across sectors, with larger firms leading.	Widespread adoption across organisations of all sizes.
Infrastructure Readiness	Limited due to poor internet connectivity and outdated IT systems.	Strong infrastructure with high-speed internet and cloud-based HR systems.
Technical Expertise	Limited cybersecurity and IT skills within HR departments.	Dedicated IT and HRIS teams manage digital security.
Implementation Barriers	High costs, resistance to change, lack of awareness.	Clear strategies and incentives for adoption.

The disparity in Table 2 mirrored trends observed in other emerging economies where resource limitations often hinder the widespread adoption of digital technologies (Chigada & Madzinga, 2021). The study found that the primary drivers of e-HR records adoption included increased operational efficiency, improved decision-making, and regulatory compliance (Mapuranga et al., 2024). However, the electronic transformation was hindered by challenges such as inadequate technological infrastructure, high implementation costs, and resistance to change.

The findings indicated that many organisations in Zimbabwe rely on hybrid HR record-keeping systems, incorporating both electronic and paper-based records (Mutumwa et al., 2024). This hybrid approach, while mitigating some risks associated with electronic records, introduced inefficiencies, inconsistencies, and vulnerabilities in HR data management. Furthermore, organisations that have transitioned to fully e-HR systems report significant improvements in data retrieval, reporting accuracy, and HR service delivery. However, these benefits were often offset by cybersecurity concerns and regulatory compliance challenges, highlighting the need for a holistic approach to e-HR adoption.

Globally, the adoption of e-HR systems was driven by the need for efficiency, scalability, and compliance with stringent data protection regulations such as the General Data Protection Regulation (GDPR) (European Union, 2016). In contrast, Zimbabwean organisations faced additional challenges, including inconsistent internet connectivity, particularly in rural areas, and a fragmented regulatory environment (Moyo et al., 2024). These barriers highlighted a significant deviation from global best practices, where robust infrastructure and clear regulatory frameworks facilitate smoother digital transitions.

Data Privacy Concerns

Data privacy emerged as a critical concern in Zimbabwe, particularly given the sensitive nature of HR records, which include personally identifiable information, medical records, and performance evaluations (Zafar, 2023). The trend of adopting electronic HR systems has heightened these concerns, as many organisations lack robust cybersecurity measures, leaving employee data vulnerable to breaches and unauthorised access (Chigada & Madzinga, 2021). This vulnerability was exacerbated by the absence of comprehensive data protection legislation and weak enforcement mechanisms (Moyo et al., 2024). In contrast, countries like South Africa and Kenya have made significant strides in data privacy through the implementation of the Protection of Personal Information Act (POPIA) and the Data Protection Act, respectively. Table 3 compares data privacy measures in Zimbabwe with international standards.

Table 3: Comparison of data privacy measures in Zimbabwe with international standards

Data Privacy Factor	Zimbabwe	Best Practices (GDPR, POPIA)
Data Protection Laws	Cyber & Data Protection Act (2021), but weak enforcement.	GDPR & POPIA with strong regulatory oversight.
Data Minimization	No clear guidelines on limiting data collection.	Strict data minimisation principles.
Regulatory Oversight	POTRAZ lacks robust monitoring mechanisms.	Active enforcement bodies imposing penalties.
Data Breach Response	No mandatory reporting framework.	Strict breach notification timelines.

Zimbabwean organisations face difficulties in aligning local HR data management practices with international data protection standards, such as the General Data Protection Regulation (GDPR) as depicted in Table 3. The GDPR imposed strict requirements on data collection, processing, and retention, which Zimbabwean companies find challenging to implement due to differences in legal structures and limited cybersecurity capabilities. The study found that organisations operating in international markets or handling cross-border HR data transactions struggle the most with regulatory alignment, often facing reputational risks and potential legal repercussions (Poshai et al., 2023).

Cybersecurity Risks and e-HR Records Management

The findings highlight that cybersecurity risks posed a significant threat to electronic HR records management in Zimbabwe. Organisations were increasingly becoming targets of cyber threats such as phishing attacks, ransomware, and unauthorised access due to inadequate cybersecurity investments (Chingoriwo, 2022). The lack of robust encryption protocols, multi-factor authentication, and regular security audits left HR information systems vulnerable to breaches (Chigada & Madzinga, 2021).

A major contributing factor to cybersecurity vulnerabilities was the shortage of skilled cybersecurity professionals in Zimbabwe. The study found that many HR departments lack personnel with specialised expertise in cybersecurity, making it difficult to implement and maintain robust security measures. Furthermore, organisations tended to adopt a reactive approach to cybersecurity, implementing measures only after experiencing a breach or facing regulatory pressure (Vusumuzi, 2024). This reactive stance increased the likelihood of successful cyberattacks, leading to financial losses, identity theft, and reputational damage.

The CIA triad framework (Confidentiality, Integrity, and Availability) offerred a foundational strategy for securing HR e-records, but its implementation in Zimbabwe remains underexplored (Whitman & Mattord, 2009). While global organisations leveraged this framework to create multi-layered defences against cyber threats, Zimbabwean organisations often lack the resources and expertise to do so effectively. This gap highlighted the urgent need for context-specific cybersecurity measures tailored to the resource-constrained environment of Zimbabwe.

E-HR Regulatory Compliance Challenges

Regulatory compliance was a significant challenge for Zimbabwean organisations, particularly in aligning their HR data management practices with both local and international standards. The Cyber and Data Protection Act (2021) provided a structured framework for data protection, but its implementation was hindered by gaps in enforcement, lack of awareness, and insufficient capacity-building initiatives (Moyo et al., 2024; Poshai et al., 2023). For instance, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) failed to establish robust monitoring and auditing systems, resulting in inconsistent compliance levels across sectors (Maponga, 2016). Table 4 summarises Zimbabwe's regulatory compliance against global practices.

Table 4: Comparison of regulatory compliance levels in Zimbabwe with leading economies

Compliance Factor	Zimbabwe	Best Practices (GDPR, POPIA)
Legal Enforcement	Weak regulatory oversight, no routine audits.	Strict penalties, proactive monitoring.
Compliance Training	Limited HR awareness of data protection laws.	Mandatory training and certification.
Cross-Border Data Rules	Unclear guidelines, legal uncertainty.	Clear policies, global alignment.

In contrast, countries like Kenya and South Africa have established proactive regulatory bodies that conduct regular audits, impose penalties for non-compliance, and provide clear guidelines for organisations as reflected in Table 4 (Kajongwe, 2022). The GDPR further sets a high

standard for regulatory compliance, emphasising accountability, transparency, and cross-border data transfer regulations (European Union, 2016). Zimbabwe's regulatory framework, however, lacked alignment with these international standards, creating compliance complexities for organisations operating in global markets. This misalignment not only exposed Zimbabwean organisations to legal and reputational risks but also limited their ability to compete internationally.

Best Practices and Strategic Interventions

Cybersecurity, and regulatory compliance challenges, organisations must adopt a multi-faceted approach integrating technology, policy frameworks, and organisational culture to mitigate data privacy. The study identified several best practices that Zimbabwean organisations can implement to enhance the security and efficiency of electronic HR records management:

1. Enhancing Cybersecurity Measures
2. Improving Regulatory Compliance – Zimbabwean organisations are encouraged to improve their compliance with the law by establishing a dedicated data protection officer, conducting regular compliance assessments, and aligning HR data management practices with global standards.
3. Investing in HR Information Systems (HRIS) with Built-in Security Features
4. Developing a Data Protection Culture - HR professionals, IT teams, and employees in Zimbabwe should receive training on data privacy and cybersecurity best practices.
5. Aligning with International Best Practices – Local organisations are encouraged to benchmark against global standards such as ISO/IEC 27001 for information security management.

These interventions aligned with global best practices but must be adapted to the unique challenges and resource constraints of the Zimbabwean context.

Gaps and Inconsistencies in Literature and Areas Needing Further Research

The literature review revealled gaps in empirical research on the effectiveness of Zimbabwe's regulatory and cybersecurity measures in HR data management. Further research was needed to explore:

- The practical implementation challenges of the Cyber and Data Protection Act (2021).
- The impact of limited cybersecurity investment on HR records security in SMEs.
- Comparative studies on Zimbabwe's regulatory framework versus other African nations.

Conclusion and recommendations

This study critically examined the adoption, challenges, and opportunities of electronic HR (e-HR) records in Zimbabwe, focusing on data privacy, cybersecurity, and regulatory compliance. The findings revealled that while Zimbabwe is making measurable progress in adopting e-HR systems, significant gaps persist due to limited technological infrastructure, weak enforcement of data protection laws, and inadequate cybersecurity measures. These challenges deviated from global best practices, where robust legal frameworks, proactive enforcement, and advanced cybersecurity investments facilitate secure and compliant HR digitalisation.

Despite these hurdles, the study highlighted the potential for Zimbabwean organisations to bridge these gaps by adopting a holistic approach that integrates technological upgrades, stronger regulatory compliance mechanisms, and a data protection-oriented organisational culture. The study provided a context-specific roadmap for balancing efficiency, security, and

compliance in e-HR adoption, offering practical recommendations tailored to the Zimbabwean digital landscape.

Contributions of the study

This study contributed to the broader discourse on HR digitalisation in emerging economies by:

- Contextualising e-HR adoption within Zimbabwe's regulatory and technological landscape, identifying barriers unique to developing nations.
- Integrating multiple theoretical perspectives (TOE, GDPR compliance, CIA Triad) to provide a comprehensive analytical framework for assessing digital HR records.
- Offering actionable insights for organisations seeking to enhance HR efficiency while mitigating risks associated with cybersecurity and data privacy.
- Benchmarking Zimbabwe's progress against international best practices, providing a comparative perspective that informs both local and regional policy debates.

Call to Action for Policymakers and Organisations

To secure the future of digital HR management in Zimbabwe, immediate policy and organisational reforms were essential. Policymakers must:

- Strengthen enforcement mechanisms for the Cyber and Data Protection Act (2021) through regular audits and capacity-building initiatives.
- Invest in national cybersecurity infrastructure to protect sensitive HR data from cyber threats.
- Harmonise local data protection regulations with international standards (e.g., GDPR, POPIA) to facilitate global compliance and cross-border HR data management.

Future Research Directions

Future research should focus on:

- Empirical assessments of HRIS cybersecurity vulnerabilities in Zimbabwean organisations.
- The role of artificial intelligence and blockchain in enhancing HR data security.
- The effectiveness of government policies in promoting e-HR records adoption.

By addressing these areas, future studies could provide actionable insights to improve HR digitalisation in Zimbabwe.

References

Bondarouk, T., Ruël, H., & Kees Looise, J. (2011). *Electronic HRM in theory and practice.* Emerald Group Publishing Limited.

Boshe, P., Hennemann, M., & von Meding, R. (2022). African data protection laws: Current regulatory approaches, policy initiatives, and the way forward. *Global Privacy Law Review,* 3(2).

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management,* 23(1), 1–11.

Chingoriwo, T. (2022). Cybersecurity challenges and needs in the context of digital development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies,* 3(2), 77–104.

European Union. (2016). *General data protection regulation (GDPR)–official legal text.*

Kajongwe, C. (2020). *Transforming human resources in the digital age and performance of employees in the mining sector in Zimbabwe and implications for development.*

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology,* 55(12), 2049–2075.

Maponga, S. S. (2016). *An analysis of POTRAZ in light of international best practices.*

Mapuranga, R., Muzvondiwa, E., & Shateyi, S. (2024). *Automation and Human Resources Management in the Tourism and Hospitality Industry of Zimbabwe. Tourism and Hospitality for Sustainable Development: Volume Three: Implications for Customers and Employees of Tourism Businesses* (pp. 139–154). Springer

Moyo, A., Makota, J., & Kabote, F. (2024). Changes in the data and information systems in Zimbabwe: Lessons from legislation and policy post-2018. *Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy*.

Mukuze, K. (2023). *Developing a predictive model for human capital analytics adoption in Zimbabwean state universities.*

Mutumwa, A., Charehwa, M., Mutongoreni, N. A., Kwembeya, M., Matsikure-Cheure, M., & Zengeya-Nyandima, R. (2024). Digitalisation of human resource management (HRM) in the Zimbabwe retail sector: An analysis of its state, benefits, and challenges. *African Journal of Human Resources, Marketing and Organisational Studies,* 1(2), 7–24.

Namalawa, R. T. (2023). The contribution of human resources information system in the effective management of human resources: A case study of NetOne Cellular (Pvt) Ltd, Zimbabwe. Ngenani: *The Zimbabwe Ezekiel Guti Journal of Community Engagement and Societal Transformations,* 108–127.

Poshai, L., Chilunjika, A., & Intauno, K. (2023). Examining the institutional and legislative frameworks for enforcing cybersecurity in Zimbabwe. *International Cybersecurity Law Review,* 4(4), 431–449.

Tapiwa, G. G., Pedzisai, P., Bernard, N., & Mervis, C. (2022). Digitalisation of human resources systems and processes necessary for public sector transformation in Zimbabwe. In *Transformational Human Resources Management in Zimbabwe: Solutions for the Public Sector in the 21st Century* (pp. 61–74). Springer.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation.*

Vusumuzi, M. (2024). *An overview of cybersecurity in Zimbabwe's financial services sector.* F1000Research, 12.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security.* Thomson Course Technology.

Zafar, H. (2013). Human resource information systems: Information security concerns for organisations. *Human Resource Management Review*, 23(1), 105–113.

Zveushe, P. S. (2023). Effects of e-Human Resources Management implementation on organisational productivity: The case of the Zimbabwe Revenue Authority. *Ngenani: The Zimbabwe Ezekiel Guti Journal of Community Engagement and Societal Transformations,* 154–171.