

Bridging the Digital Divide: Reimagining HRM Education for an AI-Driven Workplace

Mark Joseph B. Chua ^{1,2}, Grecebio Jonathan D. Alejandro ¹

¹ *The Graduate School, University of Santo Tomas, España Blvd., 1008 Manila, Philippines*

² *School of Management and Information Technology, De La Salle – College of Saint Benilde, Taft Ave., Manila, Philippines*

Abstract – Human resource management (HRM) is undergoing a profound transformation at the intersection of Artificial Intelligence (AI), digital transformation, and cybersecurity. Despite these shifts, higher education curricula remain largely anchored in traditional paradigms, producing graduates insufficiently prepared for contemporary organizational realities. This review synthesizes peer-reviewed literature (2021–2025) to identify critical misalignments between academic preparation and workplace demands. Three interrelated gaps emerge: Insufficient cybersecurity literacy among HR practitioners, rapid AI-driven workforce transformation, and misalignment between curriculum and practice. In response, this study proposes a four-pillar framework for strategic HRM education integrating AI literacy, workforce analytics, organizational security, and ethical leadership. The framework advances a systemic redesign approach to ensure HR graduates possess technological fluency, analytical capability, risk awareness, and moral discernment. The findings underscore the urgency of curriculum innovation aligned with accelerating technological change.

Keywords – Curriculum innovation, data-driven HR analytics, digital transformation, ethical AI leadership, organizational cybersecurity.

DOI: 10.18421/TEM153-80

<https://doi.org/10.18421/TEM153-80>

Corresponding author: Mark Joseph B. Chua,
The Graduate School, University of Santo Tomas,
España Blvd., 1008 Manila, Philippines

Email: markjoseph.chua@ust.edu.ph

Received: 06 December 2025.

Revised: 17 February 2026.

Accepted: 04 March 2026.

Published: 27 August 2026.



© 2026 Mark Joseph B. Chua & Grecebio Jonathan D. Alejandro; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

1. Introduction

The field of human resource management (HRM) has undergone a significant shift. In the first half of this decade, rapid technological advancements have transformed the way businesses attract, train, assess, and retain employees. Nowadays, Artificial Intelligence (AI) is embedded in recruitment processes, performance management systems, predictive analytics, and HR cybersecurity, which is now regarded as a primary HR function rather than a secondary IT function [1], [2]. However, despite these technological advancements, HR education systems have undergone minimal transformations.

HR education systems are based on the tenets of old curricula, designed when HR functions are purely administrative. They focus on the traditional system of motivation, compensation management, and industrial relations (though these are still very important, in today's technology-filled environment, they are highly inadequate) [3]. These days, graduates enter organizations equipped with cognitive frameworks and minimal technical competency to assess recruitment tools for algorithmic bias, analyze workforce data, and possess the appropriate level of cybersecurity to safeguard employees' sensitive data [4].

This gap between educational preparation and professional requirements has become increasingly evident through multiple converging trends (Figure 1). Organizations have reported difficulty in finding HR professionals who can bridge the technological and human domains [5]. The cybersecurity workforce faces a staggering shortage of 4.8 million professionals globally, with educational institutions cited as particularly vulnerable sectors [6], [7]. Simultaneously, AI adoption in HRM has surged, with tools transforming everything from candidate screening to personalized learning. However, educators have expressed uncertainty about integrating these technologies into teaching practices [8], [9], [10].

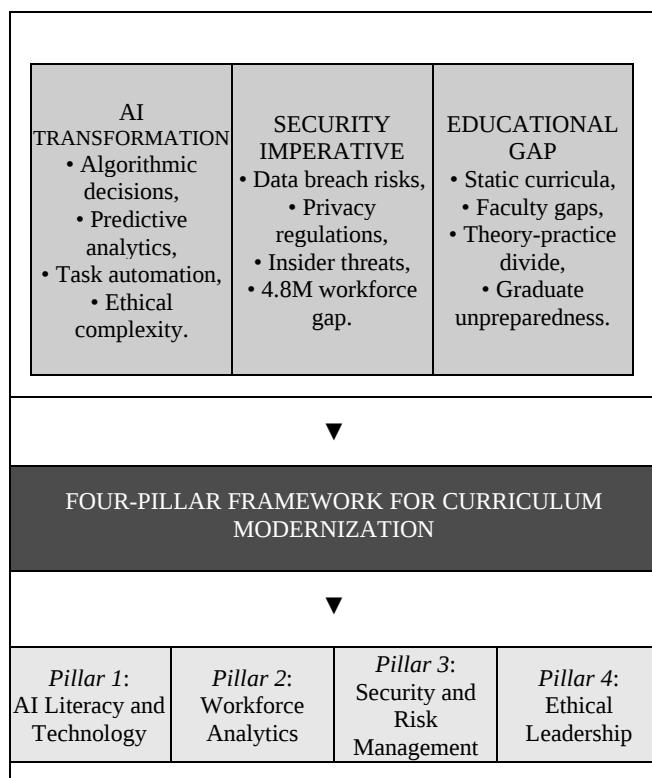


Figure 1. Conceptual framework illustrating the three interconnected challenges in HRM education converging toward a comprehensive four-pillar solution for curriculum modernization

The effects of this educational gap extend beyond the individual's career preparedness. Organizations use AI-based HR systems with no training or personnel assigned to them, which could worsen the algorithms' biases rather than address them [11]. Cybersecurity breaches are increasingly common and target HR departments, which hold the most sensitive information. However, most of these professionals are HR illiterate [12]. The promise of evidence-based HR remains unattained, while practitioners in the field continue to lack the critical analytical competencies needed to convert data into decisions [13].

This comprehensive review aims to address a question that, to date, has not received sufficient attention in the academic literature. *How should Strategic HRM academic programs be reconfigured to prepare graduates for an organizational paradigm that is reordered by the influences of AI, data analytics, and cybersecurity?* By combining recent interdisciplinary scholarship on the adoption of AI in higher education, the digitalization of HRM, organizational security, and modern pedagogy, a conceptual model is offered for the redesign of curricula that is situated in both theory and organizational needs.

This undertaking is subject to deadlines from all perspectives. Universities are the main pipeline for graduate HR talent; however, fresh graduates require extensive training to acquire the fundamental skills they should have learned in school [14].

This training is overly burdensome for early-career professionals and for companies already overloaded with rapidly changing technologies. This misalignment represents a structural deficiency in higher education systems that prepare future HR leaders. Its most basic goal is to prepare students for the workplaces of the future, not the past.

2. Contextual Background

This section examines how strategic HRM as a profession has evolved and the current factors shaping its nature. It will be possible to trace HRM from its administrative roots to its technologically mediated form, see the significant changes AI has caused, address the cybersecurity imperative, and examine the widening skills gap between academic preparation and professional practice.

2.1. The Evolution of Human Resource Management

Throughout its history as a distinct field and section of management, human resource management has undergone several paradigm shifts. Early on in personnel administration, migration management tracked basic transactional activities, calculated payrolls, and ensured compliance with fundamental labor laws [5]. The 1980s brought the strategic movement in HRM, which rested on the assumption of human resources as human administrative costs and, from there, repositioned them as a potential source of competitive advantage. This was later developed in the 90s with the rise of human capital, which treated employees as assets businesses ought to invest in and further develop.

The 21st century has brought forth the theory of digital HRM. This theory applies various Internet technologies and tools to build work efficiency. Some of these tools have been used in self-portals, automated workflows, and data banks [15]. In contemporary HRM, the efficiency-centered theory of digital HRM has led to the brink of a future history of HRM in the fields of Artificial Intelligence and high analytics, and to the need to work in and concern ourselves with a more secure and vulnerable digital world [1].

2.2. *The AI Revolution in Workforce Management*

Once experimental, the application of Artificial Intelligence in human resource management has become essential in record time. The recruitment phases of human resource management use AI-enabled applicant tracking systems to screen candidates and process thousands of applications in record time, leveraging natural language processing and pattern recognition [3]. Performance management systems utilize AI to determine productivity patterns and predict future outcomes. In learning and development functions, AI systems design adaptive learning pathways to respond to individual differences in the learning process and fill competency gaps [16].

The ability of these systems represents the opportunity to process even a small fraction of the total data. The potential to reduce the time to hire and expand the pool of high-potential candidates at a nominal opportunity cost through predictive analytics. Such systems may also predict future employee turnover and help develop strategies to improve employee retention. Enhanced learning systems provide customized training to respond to individual and organizational educational needs [17].

Insufficient safety measures exacerbate these risks. There is a risk of bias in the training data used for discriminatory hiring practices, which can deepen prejudices [11]. There are privacy issues with advanced technologies that can be used to monitor employees. Trust can be lost, and there is a risk of legal challenges due to the black-box nature of some AI systems, which prevents the discourse on AI systems used to make adverse employment decisions [2].

From a practical perspective, the issue is not whether AI should be incorporated into HRM, this issue has already been settled as a function of supply and demand, but the way in which this incorporation should be managed to facilitate the balancing of technological advancements with the protection of people, values, and morals (organizational ethics) [14].

2.3. *The Cybersecurity Imperative*

As functions within human resources have incorporated digitized processes, the potential for cyberattacks has increased. Human resources are responsible for the care, maintenance, and protection of employee records, including sensitive information such as social security numbers, birth dates, physical addresses, salary information, health records, and performance evaluations [18].

With an average cost of \$4.8 million per incident, data breaches are increasing annually, and the human resources divisions of organizations are among the most frequent targets [18].

External cybersecurity threats to employee data are worrying but potentially less transformative than the risks presented by employees. Employee data, even within organizations as large as the EU Parliament, was and still is breached more than 40% of the time [12]. Additionally, most human resources employees are not trained in cybersecurity, which, to them, is an IT problem, further compounding this vulnerability.

With a shortfall of almost 5 million professionals in the cybersecurity field, the deficiency is particularly severe in the education, government, and healthcare sectors [6]. These organizations have an even larger shortfall of professionals with specialized cybersecurity training than of employees, resulting in a seemingly endless cycle of work for the cybersecurity professionals already in place and work-related burnout [7].

This scenario presents a dual challenge for human resources. First, HR professionals must have a sufficient understanding of cybersecurity to safeguard the information in their care adequately [19]. Second, the HR division must support the organizational cybersecurity plan by implementing secure hiring practices, developing programs that enhance organizational security awareness, and fostering an environment in which security is viewed as a collective responsibility of all employees, rather than the sole domain of technical specialists [20].

2.4. *The Skills Gap Crisis*

These security and technological changes have fostered closer connections to an extreme skills gap in the workforce. Lightcast's research shows that 32% of an average job's skills have changed over the past three years, with predictions that this percentage will reach 50% worldwide by 2030 and 68% in an accelerated timeline due to generative AI [13]. Organizations have identified the most in-demand technology-related skills as data analytics (36%), AI (31%), and cybersecurity (21%), which many HR professionals currently lack [13]. Table 1 presents a detailed comparison of traditional and modern HRM competencies across several key functional areas.

Table 1. Comparison of traditional HRM competencies versus contemporary competencies required in AI-driven organizations (demand percentages from [13])

Domain	Traditional Competencies	Required Contemporary Competencies
Recruitment	Job posting, Resume screening, Interview techniques.	AI-powered applicant tracking, Algorithmic bias detection, Predictive candidate fit analysis.
Performance Management	Annual appraisals, Goal setting, Feedback delivery.	Real-time analytics dashboards, Predictive performance modeling. AI-generated feedback synthesis
Data and Analytics	Basic reporting, Headcount tracking, Turnover rates.	Workforce analytics (36% demand), Predictive turnover modeling, Data visualization and storytelling.
Technology	HRIS data entry, Basic system navigation, Report generation.	AI literacy (31% demand), System configuration and optimization AI ethics and bias mitigation.
Security	Password management, Physical file security, Compliance awareness.	Cybersecurity literacy (21% demand), Data governance & privacy Incident response protocols.

There are consequences to this skills gap, as many organizations are unable to implement AI-powered HR systems due to a shortage of qualified staff to configure, oversee, and fine-tune them.

HR data repositories contain abundant workforce data that ultimately fail to yield valuable insights because HR teams lack the analytical skills to derive them. Security measures are insufficient because HR staff do not fully grasp the risks, or the integral role they can play in reducing them.

The response of educational authorities to these issues has been subpar. Some universities have included data analysis or technology modules in their HRM programs; however, these changes have been more supplementary than integrated. It has been argued that few programs focus on developing AI competency, understanding the nuances of technology decision-making frameworks on ethics, and integrating programs that offer the basics of technology crime (cybersecurity) [21]. This explains the phenomenon in which programs continue to churn out unprepared graduates, organizations need to spend more on remedial training, and the discrepancies between educational programs and the skills the workforce demands continue to grow in the Philippines.

3. Methodology

This comprehensive review employs a systematic synthesis approach to examine the intersection of AI integration, organizational security, and human resource management education. The methodology follows established protocols for qualitative evidence synthesis while adapting them to the interdisciplinary nature of this inquiry [22], [23].

3.1. Literature Selection and Scope

The review focuses on peer-reviewed scholarly articles from 2021 to 2025, with a particular focus on 2023-2025, as this area of study is exceptionally fast-moving. The selection of this specific time frame is not arbitrary, as the adoption of AI in HRM and higher education began to explode during the period under review, especially after the release of generative AI in late 2022.

Literature was identified through systematic searches of major academic databases, including Scopus, Web of Science, Google Scholar, and discipline-specific repositories. Search strings combined key terms across multiple domains: AI and education ("Artificial Intelligence" OR "AI" OR "machine learning") AND ("higher education" OR "curriculum" OR "pedagogy"); HRM and technology ("human resource management" OR "HRM" OR "talent management") AND ("digital transformation" OR "AI" OR "automation"); Security and workforce ("cybersecurity" OR "organizational security" OR "digital risk") AND ("workforce" OR "human resources").

In addition to database analyses, auxiliary references from pivotal publications were reviewed to uncover further pertinent materials using previous citation tracking. Using forward citation tracking, newer articles that referenced the foundational works in the discipline were identified.

For this review, this procedure provided a composite of 25 core academic works, as well as reputable trade publications from ISC2, the World Economic Forum, SHRM, and Deloitte, which reviewed the context relevant to the challenges and trends faced by practitioners.

3.2. Analytical Approach

The study analyzed data using thematic synthesis, one of the most effective frameworks for integrating diverse streams of scholarship on complex, multilayered topics and phenomena. This process was performed over several cycles [22].

First, each article in the study was carefully read to extract its central ideas, findings, and contributions to the field. Initial coding captured the main arguments and, in some cases, the more subtle, less prominent positions the researcher(s) could take. Special focus was given to the various ways in which different fields describe the same issues. For instance, the framing differences in the computer science literature regarding AI and ethics versus those in management scholarship, or the differences in the educational technology and organizational change literature regarding the challenges of implementation.

Second, provisional themes were created from the codes through an iterative process of sorting and re-sorting. During this step, patterns began to emerge across what seemed to be unrelated literature, for example, parallel concerns about algorithmic bias in AI and digital equity in education, and challenges in cybersecurity workforce development and technical training for other workforce development.

Third, the provisional themes were validated and further refined by returning to the source texts to ensure an accurate representation and that the researcher(s) had not imposed foreign frameworks on them. Finally, the synthesis shifted from being primarily a descriptive summary to an interpretative one, interrogating the relations among the themes and what the interrelations could mean for the development of curricula in HRM.

3.3. Ensuring Rigor and Credibility

Several factors aided the credibility and rigor of this synthesis. Since the synthesis drew on multiple disciplinary perspectives (management, education, computer science, security studies) and all fields encountered the same problems, the risk of blind spots in any one discipline was reduced. The synthesis did not merely present evidence and explanations in support of the thesis but also deliberately searched for counterevidence and alternative explanations. The synthesis identifies the scope and purpose of this study.

The synthesis considers only the strategic HRM curricula in higher education. Important but related questions regarding executive education, organizational training programs, and professional development also exist but are outside the scope of this synthesis.

4. Results

One of the main priorities of the literature synthesis was to identify and describe the current gaps and trends in the HRM education sector. These are not standalone gaps and trends; instead, they reflect synchronous changes across industries. These changes are documented in Table 2, along with the findings and educational impacts of each pattern in the sector.

Table 2. Summary of four major thematic clusters identified through synthesis of 25 peer-reviewed scholarly articles (2021-2025) and authoritative industry reports

Theme	Key Findings	Educational Implications
Security-Intelligent HRM	• HR manages sensitive data vulnerable to cyberattacks, • 4.8M global cybersecurity workforce gap, • 41% increase in employee data breaches (2023), • Security culture depends on HR policies.	Integrate cybersecurity literacy as core competency, Cover data governance, privacy regulations, incident response Develop security-conscious culture builders.
AI as Transformative Force	• AI permeates all HRM functions, • Algorithmic bias risks in hiring/promotion, • Generative AI creates new opportunities and challenges, • Skills requirements changing 68% by 2030.	Develop AI literacy: capabilities, limitations, bias detection, Provide hands-on experience with AI tools, Cultivate critical evaluation skills.
Curriculum-Practice Gap	• Curricula emphasize classical theories over contemporary tools, • Technology topics remain peripheral, • Faculty lack AI/analytics expertise, • Graduates require extensive on-job training.	Systematically integrate technology throughout curriculum, Invest in faculty development, Shift from knowledge transmission to skill development.
Ethical Dimensions	• Algorithmic bias perpetuates discrimination, • Privacy concerns with employee monitoring, • Transparency / explainability challenges, • Novel ethical questions without clear precedents.	Embed ethical reasoning throughout curriculum, Use case-based learning for ethical dilemmas, Develop technological wisdom.

A review of the literature reveals four interconnected themes that significantly challenge the current HRM paradigm; security intelligence, AI transformation, misalignment between curriculum and practice, and ethical complexity that define the landscape of strategic HRM education and the future curricula will need to address.

4.1. The Need for Security-Intelligent HRM

The literature over the past few years has overwhelmingly focused on the view that an organization's security is no longer an ancillary concern but an imperative within HRM. This shift can be attributed to several factors. The digitalization of employee information, increasing legislation and privacy regulations governing employee information, the rise of cyber-attacks targeting HR functions, and the growing understanding that a cultivated security posture is rooted in the users of a system, not the system itself.

As shown by [19], the shift is as follows: Today's organizations seek HR that is not just germane to talent management but also encompasses the fast-growing scope of organizational security, which includes risk management, protection of the organization from within, employee surveillance, and control of the response to a situation. The implications of this for education are self-evident and significant.

The new HR must have a basic understanding of security breaches, but not at the level of a specialist; instead, they must be able to recognize risks and know which measures to put in place to engage with security personnel and establish a security posture within the organization.

4.2. AI as Transformative Force in Workforce Systems

The second major theme revolved around the growing role of Artificial Intelligence. AI is no longer used as an efficiency tool. AI is transforming all aspects of HRM. As demonstrated in [3], this impact is multifaceted. AI is used at various stages of processes, including recruitment and analytics (talent), evaluation (performance), engagement (employee), development (learning), workforce (predictive), and planning.

These diverse perspectives converge on a crucial insight: AI competency for HR professionals goes beyond merely knowing how to operate specific tools. This requires an understanding of AI capabilities and limitations, the critical evaluation of algorithmic outputs, the recognition and mitigation of bias, ethically sound decisions regarding AI implementation, and appropriate human oversight of automated systems. However, current HRM curricula rarely address these competencies systematically [21].

4.3. The Educational Gap: Curriculum Lagging Behind Practice

The most prominent theme in the literature is the disconnect between changing workplace demands and the inability of educational programs to adapt. Several researchers claim that HRM programs continue to focus on outdated theories of the discipline and offer very little in terms of teaching current theory and practice [21], [8], [14].

Such an educational imbalance has the following gaps: First, there is a shortage of focus on the necessary technological skills. Second, when the curriculum includes technology content, it is often limited in scope and poorly integrated into the primary curriculum. Third, teaching practices tend to emphasize knowledge over skill development. Fourth, the teaching staff's lack of current knowledge results in a lack of confidence in teaching emerging skills.

4.4. The Ethical Dimensions of Technology-Mediated HRM

The last important aspect to discuss concerns the potential moral complexities of having algorithms mediate personnel decision-making. Unlike other HR problems, where ethics have been understood over long periods of time, the use of technology to make decisions raises first-time concerns about fairness, discrimination, accountability, secrecy, and ultimately, the role of humans.

Vis-à-vis HRM pedagogy, its complexities should not be regarded as an isolated subject to be covered in one class titled 'ethics of AI.' The very framing of ethics demands that it be real and not a thin concept sprinkled in as an afterthought to existing AI and technology courses [24]. This should stimulate students to reflexively ask, '*Who is likely to be disadvantaged by the use of this technology?*' '*What prejudices are embedded in the information or algorithms?*', and '*Are there mechanisms in place to foster accountability and transparency?*'

5. Discussion

This convergence of evidence provides a strong rationale for fundamental changes in the education of strategic HRM. The identified gaps in academic preparedness and workplace demands offer clear directions for curriculum innovation that bridge the gap between technologically competent and human-centered practice. This article translates research insights into practical implications for designing education, pedagogies, and core competencies in AI-organized work environments.

The themes uncovered through the literature synthesis yield preliminary conclusions regarding appropriate guidance for strategic HRM education.

It is beyond doubt that curricula must change; however, the question is how to change them to equip graduates for the organizational environment adapted to automation and Artificial Intelligence while still building on the core of compassionate HR practice.

Collectively, these findings support reconceptualizing strategic HRM education as a dynamic capability system rather than a knowledge-transmission model. Drawing from capability theory and sociotechnical systems perspectives, curriculum reform must integrate human competencies with evolving technological infrastructures. The failure to align these domains risks institutional obsolescence.

5.1. From Technology as Tool to Technology as Context

One implication is the need to reconceptualize the role of technology in HRM education. The traditional view is to consider technology as a set of tools to be adopted, for instance, by human resources (HR) professionals. However, this view is becoming increasingly problematic for several reasons. The current and future HRM practices are situated within a set of technological systems. This shift from tools to context calls for different pedagogical strategies. Rather than having a set of unintegrated technology courses, a practical curriculum design embeds technological dimensions across all core HRM courses.

5.2. Building Bridges Between Technical and Human Capabilities

The second implication focuses on the relationship between technical and traditional human competencies in HR. The practice of effective HR in AI-empowered organizations entails a fusion of sophisticated human competencies and technical skills. This implies that curricula deliberately build a fusion of capabilities. Ethical grounding must accompany technical skills to avoid producing professionals who can optimize metrics without critically reflecting on what the metrics should be.

5.3. Security as Core Competency, Not Specialized Knowledge

The third issue concerns cybersecurity and the associated organizational risks. Most organizational behavior management courses, if they address security, treat it as a specialized topic relevant only to specific job functions or sectors. The synthesis of the literature reflects the inadequacy of this approach. HR functions in most organizations handle confidential information. Therefore, basic cybersecurity literacy is not an optional or specialized topic but a core competency required of all HR practitioners.

5.4. Ethics as Lived Practice, Not Abstract Principle

The complexity of teaching ethics, the use of algorithms, digital monitoring, predictive models, and AI raises ethical concerns that existing frameworks only partially address. This indicates that the use of a pedagogy that makes ethics real, multifaceted, and personal, with students having to articulate and defend their positions, gain exposure to different stakeholder perspectives, and build their individual ethical frameworks, is as follows.

5.5. Pedagogy Matching Content: Active, Applied, Integrative Learning

The final implication concerns pedagogy. Using a traditional lecture format is particularly ineffective for developing a learner's technological fluency, as well as their analytical and judgment skills. Students cannot gain meaningful HRM competencies without an environment that fosters active participation with fundamental tools, technologies, and problems.

6. A Framework for AI-Integrated Strategic HRM Curriculum

Drawing on the literature synthesis and discussion, this study proposes a four-pillar framework for modernizing strategic HRM education. These pillars are not independent modules but rather interconnected dimensions that together prepare graduates for technology-mediated, security-conscious, and data-driven HR. Table 3 presents a comprehensive overview of the framework, detailing the core content areas and the expected learning outcomes for each pillar.

Rather than adding supplementary content, each pillar represents a critical dimension of contemporary HRM practice that must be systematically integrated. The framework identifies the interdependencies among technical competence, analytical capabilities, security awareness, and ethical leadership as necessary for the operation of organizations in technology-mediated environments.

Table 3. Comprehensive four-pillar framework for Strategic HRM curriculum modernization, detailing core content areas and expected learning outcomes for each pillar

Pillar	Core Content Areas	Key Learning Outcomes
PILLAR 1: AI Literacy & Applied Technology	- Fundamental AI concepts and capabilities, - AI applications across HRM functions, - Hands-on tool experience (ATS, analytics, chatbots) - Critical AI evaluation frameworks, - Emerging AI trajectories.	- Understand AI capabilities and limitations, - Configure and use AI-enabled HR tools, - Critically evaluate AI appropriateness - Adapt to emerging technologies.
PILLAR 2: Workforce Analytics & Evidence-Based Decision Making	- Data literacy and statistical foundations, - HR metrics and KPIs, - Analytical methods (descriptive, diagnostic, predictive, prescriptive), - Analytics platform proficiency, - Data-to-decisions translation, - Analytics ethics.	- Conduct workforce analyses using appropriate methods, - Determine when analytics add value, - Translate findings into actionable recommendations, - Communicate effectively with stakeholders.
PILLAR 3: Organizational Security & Risk-Aware Practice	- Digital risk landscape and threat vectors, - Data governance and privacy frameworks, - Security-conscious HR practices, - Security culture and training development, - Incident response protocols, - Vetting and insider threat management.	- Understand key cybersecurity risks, - Apply security principles to HR decisions, - Collaborate with security specialists, - Foster security-conscious culture.
PILLAR 4: Ethical & Transformational Leadership	- AI ethics frameworks and principles, - Algorithmic fairness and bias mitigation, - Transparency and explainability, - Human-centered technology design, - Change leadership capabilities, - Future of work preparation.	- Analyze ethical dilemmas systematically, - Guide technology implementation humanely, - Ensure technology serves organizational values, - Lead change effectively.

6.1. Framework Integration and Implementation

Although the components are presented in their own subsections in Table 3, in practice, it is necessary to synthesize the elements required to integrate the pillars in the previous example. For instance, suppose the module includes an AI-enabled recruitment. In that case, teaching technology operational competencies by focusing on how applicant tracking systems work and how to adjust screening parameters to fit employers' criteria. Similarly, touching on analytical competencies by having participants interpret the generated candidate rankings and fit scores, and engage with score systems. Data security is always a civic competency principle; therefore, it includes applicant data security and the review of vendor security measures. Ethical and civic competencies must also address the detection of algorithmic bias and transparency in the use of AI with candidate communications. Each pillar also reflects the inefficiency of treating skills and competencies in isolation. Multiple touchpoints necessitate considering interlinked, complex systems in the design process.

Considering how the previous example highlighted the pillars of active learning, integrated the various systems, and grounded the design in relevant industry practices, it is also grounded in the following. Among the diverse and complex technology systems being used, challenge-based learning and collaborative problem-solving to address open-ended real-world organizational problems will also enhance skills and competencies in systems thinking and adaptive learning, helping students prepare to address technologies and systems challenges that are not yet visible.

Incorporating these components also means considering and scoping the faculty development components. Expertise gained as technologies evolve will help faculty navigate advanced technologies pedagogically to active-based learning systems. Cutting-edge technologies will be available to faculty who use older pedagogical models, ensuring curriculum development remains ongoing and iterative to prevent stagnation. Graduates need competencies in rapid adaptive learning; therefore, the systems and technologies used must evolve continuously.

7. Conclusion

The above commentary illustrates the evident discrepancy between the qualifications required to be an effective HR manager and what one is trained to do in the many academic programs offered in this regard. Most educational programs do not address the role of AI in recruitment, performance management, learning development, or workforce planning.

Most educators do not address cybersecurity, which has shifted from a peripheral IT risk to a core focus for organizations, a shift for which HR plays a critical role. It is also evident that data analytics is a powerful tool for evidence-based decision-making in addressing the numerous challenges organizations face with their workforce. Therefore, it is perplexing that educators have not adapted their programs to the workplaces in which their graduates will enter.

This lack of readiness also affects the organization as a whole. Organizations that use AI in HR lack trained personnel to oversee its use. Thus, AI is likely to exacerbate the biases it is supposed to eliminate. HR functions are often targets of data breaches; however, HR professionals receive little to no security training. Without the ability to turn data into actionable strategies, the promise of evidence-based HRM will remain unfulfilled. The core of the problem is not technological but educational. This will prepare HR practitioners to lead technology-mediated organizational transformations while maintaining a focus on people.

The proposed four-pillar framework comprising AI literacy and applied technology, workforce analytics and evidence-based decision-making, organizational security and risk-aware practice, and ethical leadership in technology-driven contexts provides a foundation for curriculum modernization from both academic and pragmatic organizational perspectives. Modernizing HR subjects should not simply entail providing additional technology modules. Viewing technology as a fundamental component of contemporary HRM, rather than an optional one, is essential. The framework also advocates for merging technical and traditional human-focused skills, treating security consciousness as normative, integrating ethical reasoning rather than leaving it as an afterthought, and employing active pedagogical methods.

The importance of this task is evident in today's society. The rate of technological change is outpacing the rate at which educational institutions can update their curricula and pedagogical frameworks, leaving a sizable gap in the prep-work and practice end of the spectrum. Institutions cannot afford to wait for graduates to arrive with the right competencies for their degrees. They require educational institutions to scaffold and systematically prepare graduates to enter the workforce with the necessary competencies for technology-integrated practices.

The higher education sector finds itself at a crossroads: To take the initiative in sculpting the way in which future HR practitioners will understand the marriage of technology with the human element of work and to drive the change and stay ahead, or to observe from a distance and respond defensively when the value of their educational practice is diminished.

The first option requires a bold vision, aligned investments, and a willingness to change. The latter is a free option and, unfortunately, the reality today, as graduates enter the workforce with immense internal frustration due to a disconnect from actual work.

The synthesis of recent studies across multiple disciplines, such as pedagogical innovation, workforce development in cybersecurity, digital transformation in HRM, and the adoption of AI in education, provides a strong foundation for integrating empirical data to develop the proposed framework. Future studies should focus on the proposed framework within pedagogy, the interrelation between technological competencies and HRM disciplines, the educational changes required to incorporate adaptive, evolving curricula, and the continuous development of faculty to illustrate the framework's importance in practice.

It is unequivocal that the question is not whether strategic HRM education should change. The more pertinent question is how long it will take for such changes to occur, and whether educational institutions will be at the forefront of them within their domain or remain on the periphery of the AI revolution. The reviewed literature indicates that the gap between preparation and practice is restrictive. The more pertinent consideration is that technology is not separable from effective HRM but, in fact, lies at its very center, and that graduates should be suitably prepared for it.

The sustainability of strategic HRM as a discipline will depend not only on incremental curricular adjustments but also on systemic transformation that embeds technological competence, ethical governance, and adaptive learning into its institutional core.

References:

- [1]. Gong, Q., Fan, D., & Bartram, T. (2025). Integrating artificial intelligence and human resource management: a review and future research agenda. *The International Journal of Human Resource Management*, 36(1), 103-141.
- [2]. Chowdhury, S., et al. (2023). Unlocking the value of artificial intelligence in human resource management through AI capability framework. *Human resource management review*, 33(1), 100899. Doi: 10.1016/j.hrmr.2022.100899
- [3]. Ekuma, K. (2024). Artificial intelligence and automation in human resource development: A systematic review. *Human Resource Development Review*, 23(2), 199-229.
- [4]. Dima, J., et al. (2024). The effects of artificial intelligence on human resource activities and the roles of the human resource triad: opportunities and challenges. *Frontiers in Psychology*, 15, 1360401. Doi: 10.3389/fpsyg.2024.1360401
- [5]. Fenwick, A., Molnar, G., & Frangos, P. (2024). Revisiting the role of HR in the age of AI: bringing humans and machines closer together in the workplace. *Frontiers in artificial intelligence*, 6, 1272823.
- [6]. ISC2. (2024). *2024 ISC2 Cybersecurity Workforce Study*. ISC2. Retrieved from: <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study> [accessed: 15 January 2026]
- [7]. World Economic Forum. (2024). *Strategic cybersecurity talent framework*. World Economic Forum. Retrieved from: https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf [accessed: 17 January 2026]
- [8]. Gârdan, I. P., et al. (2025). Adopting AI in education: optimizing human resource management considering teacher perceptions. *Frontiers in Education*, 10, 1488147.
- [9]. Parker, L., et al. (2024). Graduate instructors navigating the AI frontier: The role of ChatGPT in higher education. *Computers and Education Open*, 6, 100166. Doi: 10.1016/j.caeo.2023.100166
- [10]. Daniels, C. P. (2025). Exploring artificial intelligence literacy and engagement in higher education stakeholders. *Issues in Information Systems*, 26(1), 201-216.
- [11]. Budhwar, P., et al. (2023). Human resource management in the age of generative artificial intelligence: Perspectives and research directions on ChatGPT. *Human Resource Management Journal*, 33(3), 606-659.
- [12]. Miteva, R. (2024). *4 HR digital transformation trends in 2025*. OneSpan. Retrieved from: <https://www.onespan.com/blog/4-hr-digital-transformation-trends-2025> [accessed: 20 January 2026]
- [13]. Society for Human Resource Management. (2025). *2025 talent trends: HR skills*. SHRM. Retrieved from: <https://www.shrm.org/topics-tools/research/2025-talent-trends/hr-skills> [accessed: 22 January 2026]
- [14]. Anastasiou, S. (2025). Integrating human resource management and artificial intelligence in educational leadership: Pathways toward transformational change. *Academic Journal of Interdisciplinary Studies*, 14(3), 7-24.
- [15]. Malik, A., et al. (2023). Employee experience—the missing link for engaging employees: Insights from an MNE's AI-based HR ecosystem. *Human Resource Management*, 62(1), 97-115.
- [16]. Ekuma, K. (2024). Artificial intelligence and automation in human resource development: A systematic review. *Human Resource Development Review*, 23(2), 199-229.
- [17]. Brynjolfsson, E., & Mitchell, T. (2017). What can machine learning do? Workforce implications. *Science*, 358(6370), 1530-1534. Doi: 10.1126/science.aap8062
- [18]. Helios HR. (2024). *What's next for HR tech? 7 trends to have on your radar*. Helios HR. Retrieved from: <https://www.helioshr.com/blog/7-hr-technology-trends-that-will-change-everything> [accessed: 24 January 2026]
- [19]. Ciekanowski, Z., et al. (2023). *Human resources in organizational security management*. *European Research Studies Journal*, 26(4), 802-812.

- [20]. Nowicka, J., et al. (2024). Managing organizational security in the era of digital transformation. *European Research Studies Journal*, 27(3), 460-471.
- [21]. Southworth, J., et al. (2023). Developing a model for AI Across the curriculum: Transforming the higher education landscape via innovation in AI literacy. *Computers and Education: Artificial Intelligence*, 4, 100127.
Doi: 10.1016/j.caeai.2023.100127
- [22]. Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.
- [23]. Snyder, H. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 104, 333-339.
- [24]. Slimi, Z., & Carballido, B. V. (2023). Navigating the Ethical Challenges of Artificial Intelligence in Higher Education: An Analysis of Seven Global AI Ethics Policies. *TEM journal*, 12(2).