Digital HR Systems: Cyber Risk Management, Compliance, and Ethical Regulation

Zoriana Dvulit[1,*,†], Liana Maznyk[2,†], Kyrylo Maznyk [3,†], Lesia Brych[1,†], Pavlo Yatchenko[2,†], Khrystyna Peredalo[1,†]

[1] *Lviv Polytechnic National University, Bandera str. 12, Lviv, 79000, Ukraine*
[2] *National University of Food Technologies, Volodymyrska Str. 68, Kyiv, 01601, Ukraine*
[3] *Jacobian Engineering Inc., 2381 Mariner Square Dr, Alameda, CA 94501, United States*

Abstract

The digitalization of human resources management has led to the widespread introduction of digital HR systems (ATS, HRIS, payroll, LMS) that process vast amounts of sensitive personal, financial, and professional data. This transformation increases exposure to socio-technical cybersecurity risks, information leaks, and ethical challenges, necessitating robust management mechanisms to ensure the cyber resilience of the broader organizational infrastructure. The article provides a comprehensive classification of regulatory acts applicable to digital HR systems, covering the legal regimes of Ukraine, the EU, the UK, the USA, and Canada, alongside international standards. A Layered Compliance Framework is proposed, structuring requirements into six critical dimensions: privacy, security, eID/e-sign, AI governance, monitoring governance, and third-party governance. To quantify compliance maturity, the study introduces the Compliance Maturity/Coverage Index, formalized through Multi-Criteria Decision Analysis (MCDA) and the Analytic Hierarchy Process (AHP). The practical application of this model is demonstrated through a Compliance Heat Map, which provides a comparative visualization of implementation levels across functional HR modules. The research highlights that the primary causes of incidents remain socio-technical: phishing, compromised credentials, human error, and vulnerabilities in third-party interactions. Finally, ethical post-mortem analysis is substantiated as a vital mechanism for risk management and organizational learning, promoting a transparent, non-blame culture essential for protecting employee rights in modern digital and smart industrial ecosystems.

Keywords

Digital HR systems; cybersecurity; personal data protection; compliance; HR analytics; phishing; risks; management; AI governance; employee monitoring.

1. Introduction

Digitalization of HR processes is accompanied by the active implementation of digital HR systems and HR analytics, which are based on the processing of significant amounts of personal data of employees and candidates. Such approaches are widely used in modern organizations and correspond to global trends in human resources management development [1, 2].

Digital transformation of human resources management is one of the most important areas of development of modern organizations today. The HR function has long ceased to be an exclusively administrative sphere, as digital technologies are actively changing approaches to recruiting, training, employee performance assessment and talent management. In this context, digital HR systems are becoming key tools to support strategic business decisions, ensuring the speed of information processing and increasing the efficiency of personnel processes. However, along with

1*SmartIndustry 2026: 3rd International Conference on Smart Automation & Robotics for Future Industry, March 26-27, 2026, Lviv, Ukraine*
* Corresponding author.
† These authors contributed equally.
zoriana.p.dvulit@lpnu.ua (Z. Dvulit); lianafibo2019@gmail.com (L. Maznyk); maznykaws@gmail.com (K. Maznyk); lesia.v.varunkiv@lpnu.ua (L. Brych); yatchenkopavlo@gmail.com (P. Yatchenko); khrystyna.s.peredalo@lpnu.ua (K. Peredalo)
0000-0002-2157-1422 (Z. Dvulit); 0000-0002-5387-7442 (L. Maznyk); 0009-0003-5922-4623 (K. Maznyk); 0000-0001-8338-9573 (L. Brych); 0009-0007-3905-1031 (P. Yatchenko); 0000-0001-5840-9210 (K. Peredalo)

the growth of the role of digital platforms, the issue of risks and threats that accompany their implementation and use is becoming more relevant. Modern organizations are increasingly dependent on data, and HR systems are among the most sensitive information resources, as they contain personal information about employees, performance data, salary figures, evaluation results and other confidential materials. That is why such digital HR systems are becoming not only a tool for optimizing human resources management, but also an object of increased attention from cybercriminals. In such conditions, there is a need for a comprehensive approach to risk management of digital HR systems, which includes both technical and ethical aspects.

Constant change in HR management is a defining characteristic of the modern environment. As Stone and Dulebohn (2019) point out, the only constant in HR today is «change», as technological innovations and new organizational formats of work force HR departments to adapt to the digital reality [3]. Digital HR systems provide new opportunities for human resource management, but at the same time create additional challenges related to data security, cyber risk management, and compliance with ethical standards.

One of the factors that increases the relevance of digital HR solutions is the spread of virtual teams and remote work. Global trends indicate that the future of organizations is increasingly connected with virtual forms of collaboration, where employees interact through digital platforms, being in different countries and time zones. Alkoud and Qatamin (2025) in their bibliometric analysis emphasize that the development of virtual teams is one of the leading trends that will determine the future directions of human resource management [4].

Regulatory and legal requirements for the processing and protection of personal data in digital HR systems are determined by the EU General Data Protection Regulation (GDPR) and the national legislation of Ukraine [5, 6]. Further clarifications on data subjects' rights and organisations' responsibilities can be found in the materials of the European Data Protection Commission [7]. Violation of established requirements can lead to significant financial penalties, lawsuits, and loss of trust from employees and candidates .

In academic and regulatory sources, digital ethics in HR is viewed as a set of principles of legality, transparency, and responsible use of personal data of employees and candidates. These approaches directly follow from the requirements of the GDPR and the European Commission's recommendations on personal data protection [6]. SHRM and ENISA analytical materials indicate that the most sensitive HR data are identification, financial, and medical data, as well as employee performance evaluation results, as their compromise can lead to discrimination and serious legal consequences [1, 8].

Social media and knowledge sharing platforms play an important role in digital collaboration. Leonardi (2017) describes the “social media revolution” that is facilitating new forms of learning and communication in organizations. In the HR context, this means that employees are actively using digital channels to interact, which increases the speed of information exchange, but at the same time can lead to the unintentional dissemination of confidential data or privacy violations [9]. These issues become particularly relevant in the context of hybrid and military threats, when, according to the SIPRI Yearbook 2025 and analytical materials from the Razumkov Center, the role of social engineering, phishing attacks, and insider actions is growing sharply [10, 11].

According to the OECD's approaches to digital risk management, cybersecurity should be viewed as a continuous risk management process that encompasses technical, organizational and human factors [2]. One of the main threats to digital HR systems is cybersecurity. HR platforms contain large amounts of personal data, making them an attractive target for cyberattacks, including phishing, malware, or data leaks. Stone and Dulebohn (2019) emphasize that the

digitalization of HR processes requires increased attention to information security, as risks increase proportionally to the amount of data being processed [3].

In the practice of operating HR platforms, threats related to the human factor dominate: phishing, social engineering, personnel errors, insider actions, as well as weak password policies and insufficient access control. A separate source of risk for HR systems is misconfiguration of cloud services and excessive access rights to shared document repositories; such scenarios are considered in recommendations for personal data protection and cyber hygiene of organizations [12]. Ukrainian professional sources also emphasize the importance of organizational and technical measures for cyber protection and digital technologies for incident analysis and support of response procedures, which is relevant for HR departments [14].

In addition to external cyber threats, there are also internal risks associated with the human factor. Employees can inadvertently violate security rules or perform intentional actions that lead to the loss of information. In this context, risk management should include not only technical solutions, but also the development of a cybersecurity culture and staff training. An additional challenge is the use of HR analytics and artificial intelligence algorithms. Digital systems increasingly use automated mechanisms for candidate selection, performance forecasting or employee turnover risk assessment. While these tools increase efficiency, they carry the risk of bias, discrimination and opacity of decisions [3].

The virtuality of teams implies not only geographical dispersion, but also high electronic dependence, structural dynamism and cultural diversity. Gibson and Gibbs (2006) emphasize that such characteristics can positively affect innovation, but at the same time create additional risks for communication security and information protection. It is digital HR systems that become the main environment for coordinating the work of such teams, which makes the issue of cybersecurity and risk management particularly important [14].

In this regard, the study of cybersecurity and digital ethics of HR platforms is an urgent scientific and practical task that requires the use of formalized risk assessment models taking into account legal, organizational and military factors. for enterprises of modern digital HR platforms, since the combination of technological, organizational and ethical approaches allows ensuring the stability and reliability of digital HR systems [15]. The authors note that the ethical dimension of digital HR is becoming a key issue, as algorithms can influence the fate of employees [3].

To reduce risks, it is necessary to implement international standards that ensure the systematic management of digital HR processes. One of the important standards in the field of HR is ISO 30414, which establishes requirements for reporting and disclosure of information on human capital. ISO (2025) emphasizes that the transparency of HR data contributes to increased accountability of organizations and improves human resource management [16]. ISO 30414 emphasizes the importance of the reliability and security of HR information, since high-quality reporting is impossible without effective data control mechanisms. Thus, digital HR systems must meet not only technological requirements, but also international human capital management standards.

However, information security standards are key to managing the risks of digital HR systems. ISO/IEC 27001:2022 defines the requirements for an information security management system (ISMS). This standard is of particular importance for HR, as it allows organizations to implement policies for protecting personal data, controlling access to HR platforms, incident response mechanisms and regular audits. ISO/IEC 27001 certification increases employee trust by demonstrating the employer's responsibility in the field of cybersecurity [17]. ISO/IEC 27000:2018 is the basic standard that forms the conceptual framework of information security [19]. In the HR context, it provides an understanding of the key categories of threats, vulnerabilities and risks that arise when processing employee data. This standard helps HR professionals integrate cybersecurity principles into HR policies and management processes. A similar point of view is held by the authors of publications that emphasize the importance of training personnel in cybersecurity and the relevance of acquiring general digital skills [19-21]. Of particular relevance to HR is ISO/IEC 27701:2025, which focuses on privacy and personal data management. HR platforms handle

sensitive information, so ISO/IEC 27701 helps organizations align with GDPR and other regulatory requirements. It sets out principles for transparency, data minimization, and responsible use of personal information, which are critical to creating an ethical digital HR environment [17].

In general, digital HR systems are an important element of modern organizations, but their use is accompanied by significant risks and threats. Managing these risks requires a comprehensive approach that combines cybersecurity, ethical principles, standardization and international recommendations. Only under the conditions of implementing such mechanisms can digital HR become not only an effective, but also a safe tool for managing human resources in the era of digital transformation. In the context of smart industry and digital manufacturing environments, HR systems are increasingly integrated into the broader digital infrastructure of enterprises. Smart factories rely on digital identity management, contractor access control, industrial training platforms, and workforce analytics to support automated production processes and safety-critical operations. As a result, cybersecurity risks in HR systems may directly affect industrial environments through compromised credentials, unauthorized contractor access, or manipulation of personnel data related to operational roles. Therefore, the governance of digital HR systems becomes an important component of cyber resilience in smart enterprises and industrial automation ecosystems.

2. Methods

The research is based on a conceptual and analytical methodology combining regulatory analysis, systems modeling, and multi-criteria decision analysis. The methodological design of the study includes three main stages.

First, a comparative regulatory analysis was conducted to identify the main legal and governance requirements relevant to digital HR systems. The analysis included regulatory frameworks of the European Union, Ukraine, the United Kingdom, the United States, and Canada, as well as international standards related to cybersecurity, privacy protection, and digital governance. Regulatory sources were selected according to three criteria: relevance to HR data processing, applicability to digital platforms, and international recognition.

Second, a conceptual modeling approach was applied to construct the Layered Compliance Framework for Digital HR Systems. The framework organizes compliance requirements into six analytical layers: privacy, security, electronic identification and trust services (eID/e-sign), AI governance, monitoring governance, and third-party governance. The layered structure reflects the multi-dimensional nature of compliance risks in digital HR platforms and allows systematic assessment of governance mechanisms.

Third, a multi-criteria decision analysis (MCDA) approach was used to formalize the proposed Compliance Maturity/Coverage Index. The Analytic Hierarchy Process (AHP) was selected to determine the relative importance of compliance layers through pairwise comparison of criteria. This method allows the integration of heterogeneous indicators related to cybersecurity, privacy governance, and organizational risk management.

To illustrate the applicability of the framework, the study analyzes selected incident scenarios related to HR systems using publicly available analytical materials from cybersecurity and enterprise software providers. These cases are used as exploratory examples to demonstrate how the proposed layered model can be applied to identify vulnerabilities and improve governance mechanisms.

The methodological approach therefore combines regulatory analysis, conceptual modeling, and decision-analysis tools to provide a structured framework for assessing cyber risks and compliance maturity in digital HR systems.

3. Results

Within the framework of this study, digital HR systems are considered as a key object of analysis, since they are the main environment for processing personal data of employees, implementing HR processes and implementing analytical and automated management solutions. At the same time, the literature review showed the presence of a certain terminological inconsistency in the use of concepts related to digital technologies in the field of personnel management. In particular, in scientific sources, the terms HR systems, HR platforms, digital HR tools or HR technologies are often used in parallel, which are often used interchangeably, although from the standpoint of information architecture and risk management they have different content.

In this paper, the term HR system is used in a narrower and more applied sense, corresponding to individual functional digital solutions aimed at supporting specific HR processes, such as recruiting (ATS), personnel accounting (HRIS), payroll systems or learning management (LMS). In contrast, the term HR platform in a broader interpretation encompasses integrated digital ecosystems that combine multiple HR systems, provide centralized data management and include complex integration mechanisms with external services. This distinction is fundamentally important in the context of compliance and cybersecurity, since digital HR risks can manifest themselves both at the level of individual modules and at the level of the entire platform as a whole.

In view of the above, the research results are structured around the concept of digital HR systems as functional components of the digital HR environment, which allows for a more accurate assessment of risks, threats and management mechanisms according to the layered compliance model. Thus, further analysis focuses on a systemic approach to managing risks of digital HR systems, which ensures methodological consistency and increases the practical relevance of the results obtained.

Digitalization of HR management is one of the key directions of modern organizational transformation, as digital HR systems are increasingly used for recruiting, talent management, personnel analytics, productivity monitoring and remote work support. However, along with the increase in the efficiency of such platforms, the level of risks associated with the processing of large amounts of personal data of employees, the use of artificial intelligence algorithms, cyber threats and ethical challenges is also significantly increasing. That is why digital HR systems require not only technological implementation, but also proper regulatory and normative support [22].

The HR sector is characterized by the fact that it handles information that is highly sensitive: personal data, health information, assessment results, personnel decisions, financial indicators and internal communications. In the digital environment, this data becomes a potential target for cyberattacks, leaks or misuse. In addition, the globalization of business and the spread of virtual teams create additional challenges of cross-border data transfers and the need to comply with different jurisdictions.

In this regard, the regulatory field of digital HR systems is formed at the intersection of several areas: personal data protection, cybersecurity, labor law, regulation of electronic document flow, ethical use of artificial intelligence and compliance when engaging external HR providers. To systematize these requirements, it is advisable to apply a classification approach that allows structuring regulatory acts by objects of regulation and their practical purpose in HRM.

Table 1 is given below summarizes key regulations that can be applied to digital HR systems in different legal environments: national (Ukraine), European and British, North American (USA and Canada), as well as international. This approach allows us to consider digital HR not only as an internal HR tool, but as an element of the global digital infrastructure of the enterprise, which must meet multi-level regulatory requirements.

Table 1
Classification of regulatory acts applicable to digital HR systems in the context of risk management and compliance

Object of regulation	Ukraine	EU / United Kingdom	USA / Canada	International standards
1. Privacy data protection	Law of Ukraine "On Protection of Personal Data" [5]	EU / United Kingdom •(EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [23] •UK GDPR / Data Protection Act 2018 [24]	USA / Canada •(USA) CCPA (California Consumer Privacy Act – of 2018 [25] •(Canada) Personal Information Protection and Electronic Documents Act PIPEDA [26]	Council of Europe. Convention 108 and Protocols [27] •Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [28]
2. Cybersecurity, information protection in information and telecommunications systems (ITS), incidents	Law of Ukraine "On Information Protection in Information and Communication Systems" [29] •Regulatory and legal framework. List of laws of Ukraine and resolutions of the Cabinet of Ministers of Ukraine [30] •Law of Ukraine "About the basic principles of ensuring cyber security of Ukraine" [31]	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) [32]	•(USA) 45 CFR Part 164 – security and privacy. HIPAA Security / Privacy for Health Plans / Providers [33] •(Canada) (Personal Information Protection and Electronic Documents Act PIPEDA cyber practices adapted to provincial regimes [26]	•Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System (Policies / Rules / Guidelines) [34]
3. Electronic document management, e-signature,	•Labor Code of Ukraine (as a basic framework for labor relations;	•Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on	•(Canada) (Personal Information Protection and Electronic	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification

eID, trust services (HR documents / HR processes online)	applies to personnel procedures, including digital ones) [35]	electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [37]	Documents Act PIPEDA contains elements on electronic means/commerce, but the key focus is privacy [26]	and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC eID/e-sign practices are widely harmonized through the eIDAS approach as a "de facto" model in many jurisdictions [37]
4. AI/HR analytics: algorithmic solutions, profiling, transparenc y and rights of subjects	•Law of Ukraine «On Protection of Personal Data ». At the level of «hard law» – through norms on personal data + labor law (depends on the specific situation) [5]	•Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations EU AI Act [38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). GDPR (Art. on profiling/automated decisions) [23]	•(USA) CCPA (California Consumer Privacy Act – of 2018 (USA) approach is mostly fragmented: privacy (e.g. CCPA) + anti-discrimination regulations + local regulations (states/cities) [25] (Canada) (Personal Information Protection and Electronic Documents Act PIPEDA cyber practices adapted to provincial regimes [26]	Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (principles that often form the basis of automated processing and risk management requirements) [28]
5. Employee monitoring & workplace privacy	Labor Code of Ukraine (general framework for employment relations and workplace control mechanisms) [35] Law of Ukraine "On Protection of Personal Data" (lawful	Regulation (EU) 2016/679 (GDPR) – lawful basis, proportionality, employee monitoring rules [23] UK GDPR and Data Protection Act 2018 [24]	Electronic Communications Privacy Act [39]	ILO Code of Practice: Protection of Workers' Personal Data (international guidance for monitoring) [40]

	processing, transparency, proportionality) [5] Law of Ukraine "On Information Protection in Information and Communication Systems" [29]			
6. Regional privacy regimes for internationa l companies	Law of Ukraine "On Protection of Personal Data" (single national framework) [5]	GDPR + national employment- specific rules of Member States [23] Data Protection Act 2018 (UK) [24]	Québec: Act Respecting the Protection of Personal Information in the Private Sector (P-39.1) [41] Federal: Personal Information Protection and Electronic Documents Act (PIPEDA) [26]	OECD Privacy Guidelines (common baseline for multinational compliance) [28] Convention 108+ (Council of Europe Data Protection Convention) [27]
7. Background checks / candidate checks, references, third parties (recruitment screening & outsourcing)	Labor Code of Ukraine (general framework of labor relations; applies to hiring procedures and personnel checks within the framework of labor law) [35] Law of Ukraine “On Protection of Personal Data” (legal grounds for processing, data minimization, rights of the subject, conditions of transfer to third parties) [5]	GDPR (controller/processor, minimization, purpose limitation, contracts with contractors, DPIA as needed) [23] UK GDPR / Data Protection Act 2018 (similar logic for screening & third-party checks) [24]	Fair Credit Reporting Act (FCRA) – the key framework for background checks through “consumer reports”, notice/consent and adverse action [42] PIPEDA (conditions of consent, notice, responsibility for transfer to third parties within the framework of the “accountability principle”) [26]	International benchmarks / best practices OECD Privacy Guidelines (accuracy, minimization, purpose limitation, security of processing) [28]
8. Whistleblow ing / ethics	Possible national rules / practices	Directive (EU) 2019/1937 on the protection of persons	•(USA and Canada) regulations	Supported by the principles of worker protection and privacy in

reports, compliance channels, whistleblower protection (whistleblowing & ethics hotlines)	(depends on the organization and sector); in international companies it is often implemented as a corporate compliance process. Law of Ukraine "On Prevention of Corruption" (legal principles of whistleblower protection, reporting channels, guarantees) [43] Law of Ukraine "On Protection of Personal Data" (confidentiality of messages, processing of personal data of message participants / investigation) [5]	who report breaches of Union law (Whistleblower Directive) [44] GDPR (legal basis, data minimization, whistleblower identity protection, access) / retention) [23] UK: Public Interest Disclosure Act (PIDA) 1998 (protection of whistleblowers in employment relationships) [24]	depend on the sector and jurisdiction; often implemented through corporate compliance policies + regulatory requirements (especially in financial / public companies) Whistleblower protections (fragmentary, depending on the sector): SEC Whistleblower Program (for financial violations) [45]. Depends on jurisdiction / sector; for the federal public sector: Public Servants Disclosure Protection Act [46]	international guidelines (ILO guidance) (International Labour Organization) ILO guidance on worker protection and due process (as a soft-law guideline in employment relations) [40]

The summary presented in Table 1 demonstrates that the regulation of digital HR systems is complex and multidimensional. No single regulation can fully cover all the risks of digital HR, as HR platforms simultaneously address employee privacy, cybersecurity of corporate systems, ethical aspects of automated decisions, and legal enforcement of electronic interactions. The practical value of the proposed grouping of regulations is that it allows building a logical bridge between the regulatory framework and the real threats that arise in digital HR systems. Each type of risk (personal data leaks, insider threats, AI bias, employee monitoring, provider interaction risks, cross-border information transfers) can be directly correlated with the corresponding classification feature. This provides a clear justification for which regulatory requirements define the boundaries of acceptable practices in the field of digital HR.

Thus, the proposed classification of regulatory acts is not only a reference tool, but also a methodological basis for further analysis of the risks of digital HR systems and the development of practical mechanisms for their management. This approach proves that digital HR in the context of modern transformation should develop on the basis of technological efficiency, cyber resilience, legal compliance and ethical responsibility to employees. To ensure regulatory compliance of digital HR systems, it is advisable to apply a multi-layered approach to compliance, which reflects a gradual layering of requirements: from basic personal data protection to artificial intelligence risk management, employee monitoring and interaction with external providers. Since different types of HR systems (ATS, HRIS, Payroll, LMS) operate with different categories of data and create

specific risks, compliance should be built systematically and integratedly. To clearly present such an approach, the Layered Compliance Framework for Digital HR Systems (Figure 1) is proposed.

Figure 1: Layered Compliance Framework for Digital HR Systems.

The presented Layered Compliance Framework for Digital HR Systems demonstrates that regulatory compliance of digital HR systems cannot be limited only to compliance with requirements for the confidentiality of personal data. Effective compliance involves the integration of cybersecurity standards, legal support for electronic document management, ethical management of algorithmic solutions, regulation of monitoring practices and control of risks associated with the involvement of third parties. Thus, this architecture can serve as a universal basis for building a risk management system in the digital HR environment and be used as an analytical tool in research and practice of corporate personnel management.

This approach involves further formalization with the creation of a hierarchical index model "Compliance Maturity / Coverage" (Multi-Criteria Decision Analysis (MCDA) / Analytic Hierarchy Process (AHP)). The idea of which is to construct a compliance index for each type of HR system (ATS, HRIS, Payroll, LMS). This is a mathematical approach used when you need to evaluate an object based on many criteria at the same time. These criteria are six layers of compliance: Privacy, Security, eID/e-sign, AI governance, Monitoring, Third parties.

$$s \in \{ATS, HRIS, Payroll, LMS\}$$

and each layer

$$l \in \{1...6\}.$$

MCDA allows you to calculate the integral index *CIs*. AHP is a method that allows you to determine the weights of criteria αl, build a hierarchy of controls, and assess which layer of compliance is more important. For example, Security may be more important than eID/e-sign in a Payroll system. AHP does this through pairwise comparison of criteria. Formalization of the model:

Let

s – digital HR system (ATS, HRIS, Payroll, LMS),

l – compliance layer (privacy, security, eID/e-sign, AI governance, monitoring, third parties),

k – specific control within the layer.

The implementation level of control k for system s on layer l is denoted as $c_{s,l,k}$, where the value can be measured on a normalized scale from 0 to 1.

The compliance coverage of layer l for system s is calculated as a weighted aggregation of control scores:

$$M_{s,l} = \frac{\sum_{k=1}^{K_l} \omega_{l,k} \cdot c_{s,l,k}}{\sum_{k=1}^{K_l} \omega_{l,k}}, \quad (1)$$

and the overall system compliance index :

$$CI_s = \sum_{l=1}^{L=6} \alpha_l M_{s,l}, \quad (2)$$

where $\omega_{l,k}$ are the weights of the controls,

L – total number of layers in the model,

α_l – layer weights (determined by AHP / expert or from data).

This model allows for comparisons between systems (ATS vs HRIS, etc.); create a compliance "heat map" by layer; work in the case of a small number of incidents. It is best to determine the layer weights α_l using the AHP (Analytic Hierarchy Process) or Best–Worst Method, and then check the sensitivity using the sensitivity analysis method.

The proposed model for assessing the maturity of compliance of digital HR systems involves the use of a set of empirical data that reflect both the technical state of the system and organizational risk management mechanisms. Such data include checklists of implemented controls, results of internal and external audits, corporate security and privacy policies, event and access logs, Service Level Agreement (SLA), the presence of formalized incident response procedures, personnel training programs, as well as appropriate technical settings of digital HR platforms. For quantitative analysis, the results of self-assessment of controls for individual layers of compliance on a scale of (0–5), actual incidents over the past 12–24 months (personal data leaks, phishing attacks, access management errors), as well as cyber hygiene metrics, in particular, the level of Multi-Factor Authentication (MFA) coverage, compliance with requirements for updates and fixes within the agreed time according to the SLA (patch SLA), as well as the phishing click rate can be used. Additionally important are the vendor risk score in cases of using cloud HR solutions Software as a Service (SaaS HR), data on the use of Artificial Intelligence (AI) in HR processes (where exactly AI is used, whether an algorithmic bias audit is conducted, whether the human-in-the-loop principle is maintained). A separate category is employee monitoring policies and the number of complaints or incidents related to privacy violations, which can act as indirect indicators (proxy) of the effectiveness of governance mechanisms. The set of such data provides the possibility of practical application of the model for calculating the compliance index and assessing the level of risks of digital HR systems based on real corporate indicators.

In smart industry environments, digital HR systems are closely connected with enterprise operational infrastructure. In modern smart factories, workforce management systems interact with industrial digital platforms, including identity management systems, training platforms, and contractor access systems. A typical workflow of HR-related access in a smart manufacturing enterprise may include the following stages:

1. Recruitment and onboarding. Candidates apply through an ATS platform, where their personal data and qualifications are processed.
2. Identity creation and access provisioning. After hiring, the employee receives a digital identity linked to corporate identity management systems that control access to enterprise IT systems and sometimes industrial operational technology (OT) environments.
3. Industrial training and certification. Employees complete mandatory training programs through Learning Management Systems (LMS), including safety training, machine operation certification, and cybersecurity awareness programs.
4. Operational access to industrial systems. Based on HR records and training status, employees receive role-based access rights to production management systems, digital twins, industrial control systems, or engineering software.
5. Monitoring and compliance control. Digital systems track access logs, training completion, and compliance with safety procedures.
6. Contractor and third-party management. External contractors working in smart factories often receive temporary digital identities managed through HR or vendor management platforms.

This integration means that vulnerabilities in HR systems (for example compromised credentials or incorrect role assignments) may lead to unauthorized access not only to corporate data but also to industrial infrastructure. Therefore, the governance of HR digital platforms becomes an important element of cybersecurity management in smart industrial ecosystems.

Maturity Index (MCDA/AHP), a Compliance Heat Map has been generated, allowing for a comparison of regulatory control coverage across various types of digital HR systems for each of the six functional layers (Figure 2).

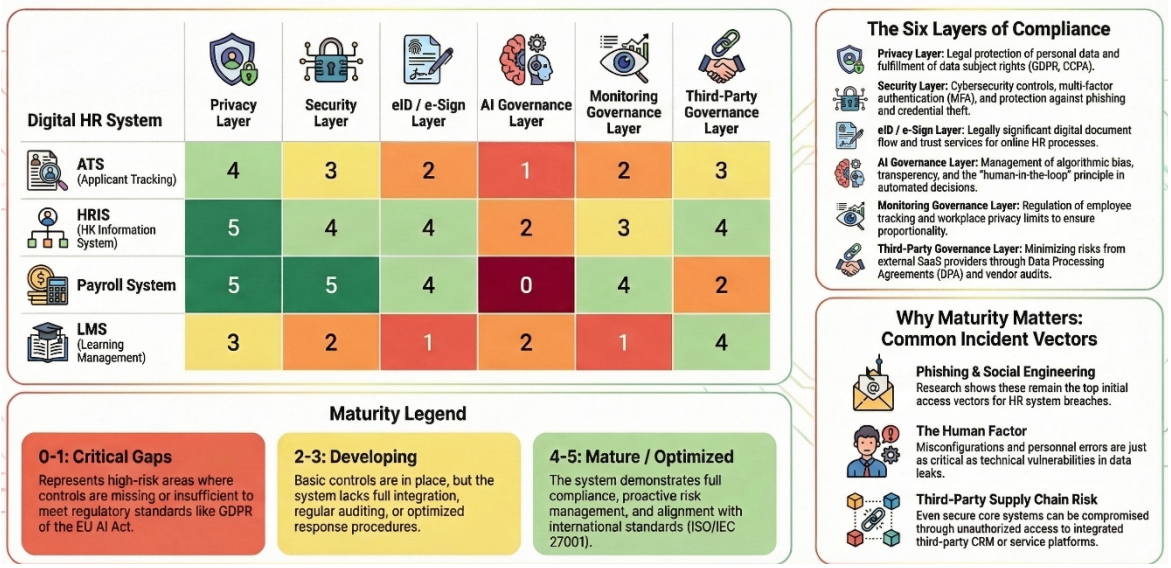

Figure 2: Compliance Heat Map for Digital HR Systems: a Layered Maturity Framework

This heat map provides a quantitative visualization of the Compliance Maturity/Coverage Index for key digital HR systems, such as ATS, HRIS, Payroll, and LMS. The map is organized according to the Layered Compliance Framework, which structures regulatory and ethical requirements into six critical dimensions: Privacy, Security, eID/e-sign, AI Governance, Monitoring Governance, and Third-Party Governance.

Each cell in the visualization represents the implementation level of specific controls, calculated using Multi-Criteria Decision Analysis (MCDA) and the Analytic Hierarchy Process (AHP). By applying a color-coded maturity scale (0–5), the map allows organizations to:

- Identify critical vulnerabilities across different functional modules.
- Assess the maturity of HR platforms in meeting international standards like GDPR, ISO/IEC 27001, and the EU AI Act.

- Prioritize risk management efforts by highlighting layers where compliance coverage is insufficient, such as third-party risks or algorithmic bias in AI.

Enhance cyber resilience by integrating technical, legal, and ethical indicators into a single analytical view.

The results of the analysis of incidents related to the leakage of personal data in digital HR systems demonstrate that key security breaches in this area are predominantly not purely technical, but socio-technical in nature. In particular, empirical observations and industry reports confirm that the main reasons for the compromise of HR environments remain phishing, misuse of credentials, weak authentication mechanisms and personnel errors. Such conclusions are consistent with both IBM analytical data on typical initial access vectors and Workday practical cases, where social engineering and compromise of third-party services have become the main triggers of incidents [47, 48].

IBM's data breach risk reports highlight that phishing remains one of the most common mechanisms for initial intrusion into corporate systems, including HR environments. HR systems are particularly attractive targets because they contain highly sensitive employee data (identification data, contact data, candidate documents, medical data, financial data, performance evaluation, recruitment data, training data, disciplinary data, HR analytics), and have a wide range of users, which increases the attack surface. Within the Layered Compliance Framework, this directly applies to the Security layer, where control variables $c_{s,security,k}$ can include the level of multi-factor authentication implementation, resistance to phishing attacks, access control procedures, and user training.

Notably, IBM also identifies human factors as one of the main causes of breaches, alongside malicious attacks and technical failures. This means that compliance effectiveness in digital HR systems is determined not only by the presence of technological barriers, but also by the organizational maturity of processes that reduce the likelihood of staff errors. In the compliance maturity model, this can be formalized through the indicators $c_{s,l,k}$, which reflect the frequency of cyber hygiene training, the level of employee awareness of social engineering, and the compliance of policies with privacy-by-design principles.

The Workday case further demonstrates the importance of the Third Parties Governance layer. In particular, the incident report related to unauthorized access to a third-party CRM platform through social engineering confirms that even if the core HR system is secure, risks can be implemented through external integrated services. In this context, the control parameters cs,third,k should cover vendor due diligence, the presence of data processing agreements, supply chain auditing, and monitoring of third-party system access.

A separate area of risk is the compromise of HR accounts in the payroll environment, where phishing or credential theft gives attackers the ability to change payment details. Such incidents highlight the need to strengthen controls not only at the Security layer, but also at the Monitoring Governance layer, which involves detecting anomalous changes in personnel or financial records. In model terms, this means that cs,monitoring,k can include implementing critical transaction logging, automated alerts on payroll data changes, transaction confirmation procedures, and regular access checks.

From an ethical perspective, an important element of post-mortem management is the quality of the post-mortem analysis. An ethically correct post-mortem in HR should ensure transparency about the nature of the breach, timely notification of victims, implementation of preventive measures and avoidance of a "blame-the-worker" culture. Workday in its public materials emphasizes the threats of social engineering and the need to increase user awareness, which is a positive element of ethical communication. However, a full assessment of the post-mortem is limited by the level of available information, since detailed internal reports on root causes and corrective actions are usually not disclosed in the public domain. Thus, the results of the IBM and Workday analysis confirm that security breaches of digital HR systems mainly arise from a combination of phishing, compromised credentials, human error and risks of interaction with third parties. This justifies the need to apply the Layered Compliance Framework as a multi-level risk

management model, where each layer is formalized through control indicators $c_{s,l,k}$. This approach allows you to quantitatively assess the maturity of compliance of HR systems, identify critical areas of vulnerability and form empirically based mechanisms for increasing the cyber resilience of the digital HR environment.

Post-mortem analysis is an integral part of cyber incident response in digital HR systems, as it allows an organization to not only document a security breach, but also to deeply analyze its causes, consequences, and gaps in risk management. Unlike purely technical remediation of an incident, a post-mortem approach aims to build organizational learning, increase system resilience, and prevent similar situations from recurring in the future. This is especially important in HR, where data leaks can have not only financial, but also significant social and reputational consequences for employees.

Ethical post-mortem analysis of HR incidents is a critical component of responsible digital risk management, as such incidents directly affect the sensitive data of employees and candidates. An ethically correct post-mortem should provide transparency regarding the nature of the breach, the categories of data affected, and the time frame of the incident, as well as minimize harm through timely notification of victims and recommendations for preventing secondary attacks, including phishing. An important principle is accountability without creating a “blame culture”, i.e. focusing on systemic causes, improving procedures, and training staff rather than individual blame. An ethical post-mortem should also include specific corrective and preventive measures, while maintaining a balance between sufficient disclosure to assess risks and respect for privacy so as not to create additional opportunities for attackers.

4. Conclusion

Research confirms that digital HR systems have become critical important components of modern organizations, as they provide automation of HR processes, but at the same time concentrate large amounts of confidential information about personnel. This creates an increased level of cyber risks and ethical threats in the digital HR environment. One of the key results of the work is the developed classification of regulatory acts applicable to digital HR systems in the context of risk management and compliance. It is shown that the regulatory support for digital HR is formed at the intersection of personal data protection regimes, cybersecurity, labor law, regulation of electronic document flow, management of AI solutions and cross-border data transfers. This confirms the multidimensionality of compliance, which cannot be reduced only to the fulfillment of individual privacy requirements.

The study proposes a Layered Compliance Framework for Digital HR Systems, which formalizes compliance as a multi-layered risk management architecture. The content of each layer is defined: privacy provides legal protection of personal data; security covers cyber protection and access management; eID/e-sign is responsible for legally significant digital document flow; AI governance controls the ethics and transparency of algorithmic HR solutions; monitoring governance regulates the permissible limits of employee monitoring; third parties governance minimizes external risks of HR systems. The grounded hierarchical model Compliance Maturity/Coverage Index (MCDA/AHP) allows for a quantitative assessment of the compliance maturity of digital HR systems based on empirical indicators (audits, incidents, cyber hygiene metrics, and vendor ratings). A practical manifestation of this model is the "Compliance Heat Map," which provides a visual diagnostic of regulatory coverage across different HR modules (ATS, HRIS, Payroll, LMS), allowing management to identify and prioritize critical vulnerability gaps. Overall, the study results confirm the need for an integrated approach that combines legal, technical, and ethical mechanisms to ensure a secure digital HRM transformation.

In the context of smart industrial environments, the governance of these systems becomes a vital component of broader cyber resilience, as HR-related vulnerabilities can directly impact industrial operational technology and safety-critical infrastructure.

Based on two case studies from IBM and Workday, it is demonstrated that the main causes of data leakage incidents in HR systems remain phishing, compromised credentials, human factors, and third-party interaction vulnerabilities. The results highlight the sociotechnical nature of threats, where organizational errors and insufficient cyber hygiene are no less critical than technical vulnerabilities. An important result is also the interpretation of ethical post-mortem analysis as a necessary element of the mechanism in risk management, which ensures transparency, minimizes harm, and prevents repeated incidents in the HR environment.

Declaration on Generative AI

The authors used GPT-4 (OpenAI) for grammar, spelling checking and minor language editing.

References

[1] Society for Human Resource Management (SHRM), "HR Data Security and Privacy," SHRM, 2025. URL: https://www.shrm.org/.

[2] Organisation for Economic Co-operation and Development (OECD), "Digital Security Risk Management," OECD, 2025. URL: https://www.oecd.org/en/topics/digital.html.

[3] D. L. Stone and J. H. Dulebohn, "The only constant in human resources management today is 'change'," in The Only Constant in HRM Today is Change, Emerald Publishing, 2019, pp. xx–xx. doi:10.1108/978-1-64113-613-620251002.

[4] S. Alkoud and L. Qatamin, "Global trends and future directions of virtual teams in the workplace: A bibliometric analysis," Proceedings of the Institution of Civil Engineers – Management, Procurement and Law, ahead-of-print, 2025. doi:10.1680/jmapl.24.00073.

[5] Verkhovna Rada of Ukraine, Law of Ukraine "On Protection of Personal Data", 2010. URL: https://zakon.rada.gov.ua/laws/show/en/2297-17.

[6] European Union, "General Data Protection Regulation (GDPR)," Official text, 2016. URL: https://gdpr.eu.

[7] European Commission, "Data protection: principles and rights," 2025. URL: https://commission.europa.eu/law/law-topic/data-protection_en.

[8] European Union Agency for Cybersecurity (ENISA), "Data Protection and Privacy," ENISA, 2025. URL: https://www.enisa.europa.eu/topics/data-protection.

[9] P. M. Leonardi, "The social media revolution: Sharing and learning in the age of digital collaboration," Information and Organization, vol. 27, no. 1, pp. 47–59, 2017.

[10] Stockholm International Peace Research Institute (SIPRI), SIPRI Yearbook 2025: Summary (Ukrainian edition), Razumkov Centre, 2025. URL: https://razumkov.org.ua/images/sipri/SIPRI_2025_summary_ukr.pdf.

[11] Razumkov Centre, "Security and defence analytics (SIPRI materials)," 2025. URL: https://razumkov.org.ua.

[12] ENISA, "Cybersecurity guidelines and publications," 2025. URL: https://www.enisa.europa.eu/publications.

[13] V. Yu. Zubok and V. V. Mokhor, Cybersecurity of Internet Topology: Monograph, Kyiv: Pukhov Institute for Modelling in Energy Engineering, 2022. URL: https://ipme.kiev.ua/wp-content/uploads/2022/07/Zubok_Mokhor_Kiberbezpeka_Topologii_Internet.pdf.

[14] C. B. Gibson and J. L. Gibbs, "Unpacking the concept of virtuality," Administrative Science Quarterly, vol. 51, no. 3, pp. 451–495, 2006.

[15] Use of Digital Technologies in Criminalistics and Forensic Expertise: Proceedings of the International Scientific Round Table, Kharkiv, Ukraine, 2024. URL: https://cutt.ly/PtcUjPgG.

[16]International Organization for Standardization, “ISO 30414: Human resource management – Human capital reporting,” ISO, 2025. URL: https://www.iso.org/standard/30414.
[17]International Organization for Standardization, “ISO/IEC 27001:2022 – Information security management systems,” ISO, 2022. URL: https://www.iso.org/standard/82875.html.
[18]International Organization for Standardization, “ISO/IEC 27000:2018 – Overview and vocabulary,” ISO, 2018. URL: https://www.iso.org/standard/73906.html.
[19]L. V. Maznyk and Z. P. Dvulit, “Management of cybersecurity specialists under full-scale invasion,” Management and Entrepreneurship in Ukraine, vol. 5, no. 2, Lviv Polytechnic, 2023.
[20]N. Shpak et al., “Influence of digital technologies on the labor market of HR specialists,” CEUR Workshop Proceedings, vol. 3171, pp. 1475–1487, 2022.
[21]N. Shpak et al., “Intelligent systems for assessment and development of personnel,” CEUR Workshop Proceedings, vol. 3171, pp. 1488–1498, 2022.
[22]L. Maznyk et al., “Applying data mining techniques in people analytics,” Lecture Notes on Data Engineering and Communications Technologies, vol. 181, pp. 106–115, 2023.
[23]European Union, “Regulation (EU) 2016/679 (GDPR),” Official Journal of the EU, 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[24]UK Parliament, Data Protection Act 2018, 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents.
[25]State of California, California Consumer Privacy Act (CCPA), 2018. URL: https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf.
[26]Government of Canada, Personal Information Protection and Electronic Documents Act (PIPEDA), 2000. URL: https://www.laws-lois.justice.gc.ca/eng/acts/P-8.6.
[27]Council of Europe, “Convention 108+ on Data Protection,” 2018. URL: https://www.coe.int/en/web/data-protection/convention108-and-protocol.
[28]OECD, “Guidelines Governing the Protection of Privacy and Transborder Flows,” 2013. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
[29]Verkhovna Rada of Ukraine, Law of Ukraine “On Information Protection in Information and Communication Systems”, 1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
[30]CSIRT Ukraine, “Regulatory and legal framework,” 2025. URL: https://csirt.csi.cip.gov.ua/en/pages/regulatory-and-legal-framework.
[31]Verkhovna Rada of Ukraine, Law of Ukraine “On the Basic Principles of Cybersecurity”, 2017. URL: https://cis-legislation.com/document.fwx?rgn=101792.
[32]European Union, “Directive (EU) 2022/2555 (NIS2 Directive),” 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.
[33]U.S. Government, “45 CFR Part 164 – HIPAA Security and Privacy,” 2025. URL: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164.
[34]Asia-Pacific Economic Cooperation (APEC), “Cross-Border Privacy Rules System,” 2025. URL: https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf.
[35]International Labour Organization, Labor Code of Ukraine, ILO NATLEX, 2025. URL: https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/46087/UKR-46087%20%28EN%29.pdf.
[36]Central Certification Authority of Ukraine, “Normative acts on electronic trust services,” 2025. URL: https://czo.gov.ua/en/normative-documentation.
[37]European Union, “Regulation (EU) No 910/2014 (eIDAS),” 2014. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng.

[38]European Union, “Regulation (EU) 2024/1689 (EU AI Act),” 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[39]Legal Information Institute, “Electronic Communications Privacy Act (ECPA),” Cornell Law School, 2025. URL: https://www.law.cornell.edu/wex/electronic_communications_privacy_act.
[40]International Labour Organization, “Protection of workers’ personal data: Guidance,” ILO, 2025. URL: https://www.ilo.org/global/publications.
[41]Government of Québec, Act Respecting the Protection of Personal Information in the Private Sector (P-39.1), 2025. URL: https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1.
[42]Legal Information Institute, “Fair Credit Reporting Act (FCRA),” Cornell Law School, 2025. URL: https://www.law.cornell.edu/wex/fair_credit_reporting_act.
[43]Verkhovna Rada of Ukraine, Law of Ukraine “On Prevention of Corruption”, 2014. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text.
[44]European Union, “Directive (EU) 2019/1937 on whistleblower protection,” 2019. URL: https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng.
[45]U.S. Securities and Exchange Commission, “Whistleblower Program,” SEC, 2025. URL: https://www.sec.gov/whistleblower.
[46]Government of Canada, Personal Information Protection and Electronic Documents Act (PSDPA), 2025. URL: https://laws-lois.justice.gc.ca/eng/acts/P-31.9/.
[47]Workday Inc., “Security and Trust Whitepaper,” Workday, 2025. URL: https://www.workday.com/en-us/company/trust/security.html.
[48]IBM Corporation, “HR Data Breach Risks and Security Insights,” IBM Security, 2025. URL: https://www.ibm.com/security/data-breach.