e-ISSN 2733-2039 print-ISSN 2733-2144

DEVELOPMENT OF DIGITAL COMPETENCIES IN RISK MANAGEMENT PROFESSIONALS

Oksana Motuzenko[1]

[1]*Ph.D. (Management), Chief Risk Manager, Fozzie Group, PJSC "Insurance Company "INGO", Financial Research Analyst, Rating Agency "MIRA", Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-3434-9553*

Citation:
Motuzenko, O. (2025). DEVELOPMENT OF DIGITAL COMPETENCIES IN RISK MANAGEMENT PROFESSIONALS. *Pedagogy and Education Management Review*, (3(21), 17–28. https://doi.org/10.36690/2733-2039-2025-3-17-28

Received: August 27, 2025
Approved: September 29, 2025
Published: September 30, 2025

Abstract. *The study explores the transformation of professional competencies in risk management under the influence of digitalization and artificial intelligence (AI). In today's rapidly changing technological environment, traditional risk management approaches—based on manual analysis and static control mechanisms—are becoming insufficient. The aim of the article is to analyze the essence, structure, and development directions of digital competencies among risk management professionals, identifying key skills required to operate effectively in digital ecosystems. The research applies a qualitative methodology, combining comparative analysis, synthesis, and content interpretation of international frameworks such as ISO 31000:2018, ISO/IEC 23894:2023, ISO/IEC 42001:2023, and NIST AI RMF (2023), alongside policy documents like DigComp 2.2, OECD Skills for a Digital World, and the World Economic Forum's Future of Jobs Report (2023). The study also reviews educational and corporate models, including professional certification programs (FRM, CRISC, ISO 31000, AI Governance & Ethics), to identify best practices in cultivating digital literacy, cyber resilience, and ethical AI governance. The findings reveal a global shift from procedural compliance to governed, data-driven, and ethically grounded practice. The proposed Integrated Competency Model identifies four interconnected pillars: analytical-technological (data analytics, AI/ML), cyber and information security (zero-trust, monitoring, resilience), ethical and regulatory (AI governance, bias mitigation, transparency), and communicative-leadership (data storytelling, collaboration, decision-making under uncertainty). Educational programs and corporate academies increasingly align with this model, combining problem-based learning, simulation labs, and continuous upskilling. The study concludes that digital competence is no longer a supplementary asset but a core component of professional excellence in risk management. A unified Digital Competence Framework for Risk Managers, harmonized across DigComp, ISO, and NIST, is proposed to ensure standardized, measurable, and adaptive professional development in the age of intelligent automation.*

Keywords: *digital competencies; risk management; artificial intelligence; ISO 31000; cybersecurity resilience; digital literacy; financial literacy; digital transformation; corporate training; DigComp framework; OECD; World Economic Forum; integrated competency model; professional upskilling; digital risk management.*

JEL Classification: G32, M15, O33, J24, D83

Formulas: 0; fig. 0; tabl. 7; bibl. 15

e-ISSN 2733-2039 print-ISSN 2733-2144

Introduction. Risk management is one of the key functions of modern corporate governance, ensuring business resilience, asset protection, and corporate reputation. Traditionally, risk management activities were based on methods of identifying, assessing, and mitigating risks that relied on analytical models, expert judgments, and internal regulations. However, in the era of digital transformation - when the speed of decision-making and data volume grow exponentially - classical approaches to risk management lose efficiency.

The modern business environment is characterized by a high level of technological uncertainty, cybersecurity threats, geopolitical instability, and information turbulence. This necessitates rethinking the role of the risk manager - from controller to analyst and strategic business partner. The digitalization of risk management processes and the implementation of artificial intelligence (AI), machine learning (ML), big data, and automated controls require a qualitatively new level of professional competence.

Today's risk management professionals must not only possess traditional risk analysis skills but also understand the principles of digital platforms, predictive algorithms, cybersecurity systems, and data governance. They must be capable of integrating technological innovations into decision-making while maintaining compliance with ethical, legal, and regulatory standards. Thus, developing digital competencies becomes not merely a competitive advantage but a precondition for the effectiveness of risk management in a dynamic environment.

The issue of developing digital competencies among risk managers covers multiple aspects - from adapting academic curricula and professional standards to corporate learning, certification, and cross-disciplinary collaboration between finance, IT, audit, and data analytics professionals. Within this context, particular attention should be given to identifying key digital skills required for effective risk management and determining mechanisms for their development in organizations across various economic sectors.

Literature Review. The professional activity of risk managers continues to be grounded in international risk management standards. ISO 31000:2018 codifies the principles, process, and integration of risk management into corporate governance, emphasizing adaptability and scalability across different organizational contexts (ISO, 2018). Against the backdrop of digitalization, a new cluster of documents focused on AI risks has emerged: ISO/IEC 23894:2023 offers AI risk management guidance aligned with ISO 31000, while ISO/IEC 42001:2023 introduces an AI Management System (AIMS), emphasizing transparency, accountability, and bias as objects of control (ISO/IEC, 2023a; ISO/IEC, 2023b). In parallel, in the United States, NIST AI RMF 1.0 provides a voluntary yet authoritative framework for trustworthy AI across the entire lifecycle, and NIST CSF 2.0 (2024) updates approaches to cybersecurity and supply-chain risks in digital ecosystems (NIST, 2023; NIST, 2024). Taken together, these sources shift the professional focus from procedural "compliance" toward the governed, evidence-based integration of digital and AI controls into the ERM process.

e-ISSN 2733-2039 print-ISSN 2733-2144

Table 1. Comparison of Risk Manager Competencies Before and After Digitalization

Dimension	Before Digitalization	After Digitalization / AI Integration
Data	Manual sampling, Excel-based analysis	Streaming data, API, lakehouse architecture
Analytics	Descriptive/expert-based	Predictive/prescriptive, AutoML models
Controls	Periodic, manual	Event-based, orchestrated, automated
Governance	Reactive compliance	AI-/privacy-by-design, Model Risk Management
Communication	Reports → committees	Dashboards, "what-if" scenarios, risk SLOs

Source: systematized by the author

Several international frameworks are relevant for operationalizing "digital competencies" within professional roles. DigComp 2.2 (JRC of the European Commission) proposes an integrated structure of five domains (information literacy, communication and collaboration, content creation, safety, and problem-solving) and 250+ examples of knowledge/skills/attitudes, including AI-related aspects (Vuorikari, Kluzer, & Punie, 2022). OECD publications distinguish technological, cognitive, and social components of digital skills and emphasize the link between digital and data literacy and labor productivity (OECD, 2016; Grundke et al., 2018). In the WEF Future of Jobs Report 2023, data analytics and risk management are listed among the top future competency areas, underscoring the need for upskilling/reskilling over a 3–5-year horizon (World Economic Forum, 2023). For risk managers, this implies that digital competencies should encompass data literacy, cyber resilience, ethics/AI and data governance, and data communication.

Reviews of ML/AI applications in the financial sector demonstrate systematic accuracy gains in tasks of credit risk and internet finance, describing the trade-off between accuracy and explainability (Tian et al., 2024). Cross-industry syntheses show that contemporary approaches complement traditional "probability × impact" matrices with predictive/prescriptive analytics as well as simulations and digital twins (Yazdi, 2024). At the intersection with cybersecurity, the updated NIST CSF 2.0 introduces clearer guidance for managing supply-chain risks and integrating them with corporate risk management processes (NIST, 2024).

Empirical and conceptual works confirm the effectiveness of ecosystem models of training (university–business–government) and internal corporate academies that combine incident simulations, risk labs, mentoring, and microlearning (Quttainah, 2024). Across industries, data literacy emerges as a "core" managerial competence directly correlated with decision quality and the maturity of a data culture (MIT Sloan, 2024; Gartner, 2024). Educational studies additionally stress that professional upskilling should cover not only technical aspects (Python/SQL, BI/ML tools) but also XAI, MLOps, and AI governance policies (Ramachandran et al., 2024).

ISO/IEC 23894 and ISO/IEC 42001 detail requirements for a governed model lifecycle (registry, validation, monitoring, explainability, and documentation of limitations), while NIST AI RMF 1.0 specifies attributes of trustworthy AI (validity, safety, security/resilience, accountability, explainability) and processes for operationalizing risk controls (NIST, 2023; ISO/IEC, 2023a; ISO/IEC, 2023b). Separate profiles/guides are emerging for generative AI, describing additional risks

e-ISSN 2733-2039 print-ISSN 2733-2144

(content authenticity, training data, adversarial scenarios) and approaches to their management (NIST, 2024b). For the professional profile, this implies incorporating competencies in MRM (Model Risk Management), privacy-/AI-by-design, and integrating logging/traceability into GRC processes.

The literature cautions that growing predictive power without adequate explainability and drift monitoring leads to operational and ethical failures (Yazdi, 2024). System-level deficits in digital and financial literacy are also documented, constraining effective data- and AI-driven decision-making (OECD, 2016; World Economic Forum, 2023). For its part, CSF 2.0 emphasizes the need to align cyber and business risks and to expand supply-chain risk management (NIST, 2024).

Research on digital competencies in risk management is growing, but is still fragmented and empirically underdeveloped. There is a lack of longitudinal evidence on how improving the skills of risk managers impacts firm-level risk and value in the face of regulatory change. Metrics and skill levels are not standardized across risk roles, and common frameworks require sector-specific KPIs (e.g. MTTD/MTTR, AUC, SLA for retraining). Explanation, reliability, and resilience metrics are rarely embedded in risk appetite and ERM reporting, while AI security lacks a unified threat taxonomy and robust testing practices outside of finance. Finally, there is no proven method for aligning ISO/IEC 23894/42001, NIST AI RMF, NIST CSF 2.0, and industry regulations into a single, low-friction GRC system, indicating the need for integrated, multidisciplinary approaches.

Aims. The purpose of this article is to analyze the essence, structure, and directions of developing digital competencies among risk management professionals under conditions of business digitalization. This involves a review of theoretical approaches, practical tools, and educational models that enhance the efficiency of risk management in the digital age.

Methodology. The research applied a qualitative design combining comparative analysis, synthesis, and content interpretation to explore how digital competencies evolve within the profession of risk management. The methodology was grounded in a systemic approach that united normative, educational, and managerial perspectives, ensuring that both theoretical frameworks and practical applications were considered. The study drew upon international standards such as ISO, IEC, and NIST, European frameworks including DigComp and the Digital Finance Package, and strategic reports by the OECD and World Economic Forum on digital skills and the future of work. Additionally, peer-reviewed studies, professional certification programs, and corporate training models were analyzed to capture the diversity of practices shaping the digitalization of risk management.

The research process unfolded in three interconnected stages. First, an analytical review of global standards and frameworks identified the core digital competence domains relevant to risk management. Second, a comparative synthesis of academic, regulatory, and corporate approaches to digital upskilling revealed alignment patterns and integration challenges. Finally, a conceptual modeling stage produced an integrated competency framework linking analytical, technological, cyber, ethical, and communicative dimensions.

e-ISSN 2733-2039 print-ISSN 2733-2144

To ensure coherence and validity, the data were interpreted through thematic coding and cross-framework mapping, which made it possible to align insights from policy documents, educational structures, and industry practices. This combination of qualitative methods provided a comprehensive foundation for developing a competency roadmap that reflects the realities of the digital economy and promotes responsible governance within contemporary risk management.

Results. The European Commission defines digital competence as the confident, critical, and responsible use of digital technologies for learning, work, and civic participation. Building on this, DigComp 2.2 structures competence into five domains - information literacy, communication and collaboration, digital content creation, safety, and problem-solving - which, in the risk-management context, map directly onto data literacy and cyber-risk awareness. The EU's 2023 Digital Finance Package extends this logic from individual skills to organizational practice, requiring risk professionals to embed digital risk-assessment tools - big data, analytical models, and automated controls - into strategic planning. Together, these initiatives mark a shift in the European approach from ad hoc use of IT tools to the governed management of end-to-end digital processes and the risks generated by digitalization.

Table 2. Global Frameworks for Digital Competence Development

Framework / Organization	Core Competence	Implications for Risk Managers	Example Metrics / Artifacts
DigComp 2.2 (EU)	Information literacy, security, problem-solving	Data literacy, cyber risk awareness	Data lineage map, password security policy
Digital Finance Package (EU)	Integration of digital tools in strategy	Using big data, automated controls	Digital control plan in ERM
ISO 31000 / ISO/IEC 23894	Integrated risk management; AI risk	Model lifecycle, validation, ethics	Model registry, XAI report
ISO/IEC 42001	AI management system	AI governance-by-design	AI policy, decision logs
NIST AI RMF / CSF 2.0	Trustworthy AI, cybersecurity resilience	Model testing, monitoring, supply chain risk	CSF control matrix
OECD Skills for a Digital World	Technological, cognitive, social skills	Analytics + collaboration + ethics	Team competence matrix
WEF Future of Jobs	Data analytics, risk management	Priority skills of the future	12-month upskilling plan

Source: systematized by the author

ISO and NIST provide the backbone for standardizing digital competencies in risk management. ISO 31000:2018 establishes principles and embeds risk management within governance, while ISO/IEC 23894:2023 extends this foundation to AI-specific risks by requiring fluency in model lifecycles, validation, and ethical oversight. Building on these, ISO/IEC 42001:2023 operationalizes an AI Management System that prioritizes transparency, accountability, bias mitigation, and responsible data use; for practitioners, this elevates AI governance, cybersecurity resilience, and model risk management from desirable skills to core capabilities. In parallel, NIST's AI Risk Management Framework (2023) and Cybersecurity Framework 2.0 (2024) translate these requirements into concrete analytical and operational practices for managing risks across digital ecosystems, including data and AI supply chains. Collectively, these

e-ISSN 2733-2039 print-ISSN 2733-2144

standards shift the competence profile from basic tool familiarity to governed, auditable practice.

Complementing this standards-based view, OECD and the World Economic Forum define the broader capability mix needed for the digital economy and responsible leadership. OECD's "Skills for a Digital World" distinguishes technological, cognitive, and social layers of competence, highlighting the decisive role of cognitive skills - data interpretation and evidence-based judgment - for risk professionals. The WEF's Future of Jobs 2023 further positions risk management and data analysis among the top in-demand skills and underscores "soft digital" strengths such as hybrid communication, data-driven collaboration, systems thinking, and information resilience. Together, these perspectives extend digital competence beyond technical literacy to include ethical judgment, emotional intelligence, and leadership under uncertainty.

Synthesizing the above yields an integrated competency model for risk managers comprising four interlocking pillars: an analytical–technological pillar (data literacy, ML/AI proficiency, model validation, and lifecycle stewardship); a cyber and information-security pillar (zero-trust practices, incident monitoring and response, and supply-chain assurance); an ethical and regulatory pillar (AI governance per ISO/IEC 42001, ISO/NIST compliance mapping, bias mitigation, and traceability); and a communicative–leadership pillar (data storytelling, cross-functional facilitation, and timely decision-making under uncertainty). Aligned with ISO and NIST standards and consistent with OECD/WEF priorities, this model defines a coherent, auditable capability set for risk managers operating in digital ecosystems.

The integrated model of digital competencies for risk managers serves as a conceptual framework that combines the requirements of international standards with the practical demands of modern digital ecosystems. It emphasizes that effective risk management in the digital age requires a balanced fusion of technical, analytical, ethical, and communicative skills. Each competence area functions not in isolation but as part of an interconnected system that supports decision-making and organizational resilience.

At its core, the model identifies four interdependent pillars. The analytical–technological pillar includes data literacy, mastery of AI and machine learning tools, and the ability to build and validate predictive models. The cyber and information security pillar focuses on safeguarding digital assets through zero-trust approaches, continuous monitoring, and incident response coordination. The ethical and regulatory pillar ensures that risk professionals operate within frameworks of transparency, fairness, and accountability, integrating standards such as ISO/IEC 42001 and NIST AI RMF into everyday practice. Finally, the communicative–leadership pillar highlights the capacity to translate complex analytical findings into actionable insights, foster cross-functional collaboration, and guide teams through uncertainty.

By linking these four domains, the model illustrates how digital competencies evolve from technical proficiency to strategic influence. It demonstrates that risk managers must not only understand how to deploy technologies but also how to govern, explain, and ethically justify their use. As summarized in Table 3, this integrated model

forms a practical roadmap for aligning professional development with international standards while embedding digital intelligence and responsible leadership at the heart of risk management practice.

Table 3. Integrated Model of Digital Competencies for Risk Managers

Competence Block	Description	Expected Behavior	Maturity Indicators
Analytical & Technological	Big Data, ML/AI, digital twins	Build scenarios, validate models	Model accuracy, retraining frequency
Cyber & Information Security	Zero-trust, monitoring, incidents	Implement controls, coordinate response	MTTR, number of critical incidents
Ethical & Regulatory	AI governance, compliance	Conduct DPIA/ALTA, maintain model register	XAI reports, audit success rate
Communicative & Leadership	Data storytelling, facilitation	Translate risk into business terms	Stakeholder satisfaction, decision time

Source: systematized by the author

Development of digital competencies begins in academia, where interdisciplinary programs blend finance, IT, cybersecurity, and data analytics. Leading universities—including the University of Leeds, the Vienna University of Economics, and ESCP Business School—now offer Master's tracks in Digital Risk Management that fuse ERM principles with Big Data, Blockchain, and AI. Practical training anchors this curriculum in real tools and contexts: students work with GRC platforms, build analyses in Power BI, Tableau, and Python, and run simulation models for risk forecasting. Pedagogically, problem-based learning and case studies strengthen applied digital literacy and critical thinking by connecting theory to live organizational challenges. Beyond degree programs, professional certifications consolidate and signal competence across key domains: FRM validates financial and analytical risk assessment; CRISC targets IT and digital risk control; ISO 31000 Risk Manager formalizes integrated risk management practices; and AI Governance & Ethics certificates (e.g., WEF, NIST, Coursera) cover ethical and regulatory stewardship of AI. Taken together, these pathways create a coherent pipeline from foundational knowledge to verifiable professional capability, with outcomes summarized in Table 4 (Educational Pathways and Learning Outcomes).

Table 4. Educational Pathways and Learning Outcomes

Education Level	Core Modules	Key Skills	Measurement of Results
Master's (ERM + Digital)	Data literacy, Python/SQL, GRC, XAI	Analytical modeling, XAI reporting	Case exam, model project
Postgraduate Certifications	FRM, CRISC, ISO 31000, AI Governance	Financial, IT risk, AI compliance	Practical exam, portfolio
Corporate Academies	Risk labs, cyber simulations	Incident response, SOAR playbooks	MTTR in simulations
Microlearning	e-learning, mentoring	Lifelong learning	Skill badges, quarterly updates

Source: systematized by the author

Corporate education is pivotal to building digital competencies at scale. Many leading firms - Deloitte, PwC, Siemens, Allianz, and IBM among them - have launched Digital Risk Academies that upskill employees in cyber risk, AI model governance,

e-ISSN 2733-2039 print-ISSN 2733-2144

data management, regulatory compliance, and crisis response. This learning ecosystem typically blends e-learning platforms (e.g., LinkedIn Learning, Coursera for Enterprise) with risk simulation labs that rehearse cyber incidents, data-literacy programs that strengthen analytical thinking, and cross-functional projects that unite risk, IT, audit, and finance teams around shared digital initiatives. To reinforce adoption and retention, organizations increasingly rely on gamification, microlearning, and mentoring, cultivating a culture of continuous improvement and risk-aware collaboration that embeds new skills directly into day-to-day workflows.

Table 5. Competence Matrix in a Multidisciplinary Risk Team

Role	Core Digital Competencies	Additional Skills	Level (1–4)
Risk Lead	Data storytelling, GRC, AI governance	SQL/Python basics, XAI	☐1 ☐2 ☐3 ☐4
Data Scientist	ML/AutoML, XAI, MLOps	Privacy engineering	☐1 ☐2 ☐3 ☐4
DevSecOps	SIEM, SOAR, zero-trust	Threat modeling for AI	☐1 ☐2 ☐3 ☐4
Compliance Officer	ISO/NIST mapping, DPIA/ALTA	Model risk policy	☐1 ☐2 ☐3 ☐4
Internal Auditor	Control testing, traceability	Adversarial testing	☐1 ☐2 ☐3 ☐4

Source: systematized by the author

The development of digital competencies in risk management is inseparable from the effective use of technological tools that automate, visualize, and enhance decision-making processes. In contemporary organizations, these tools form an integrated digital ecosystem that supports every stage of the risk management cycle - from identification to governance.

At the identification and assessment stages, GRC platforms such as MetricStream, SAP GRC, and IBM OpenPages enable centralized risk registries, control mapping, and workflow automation. These systems streamline compliance reporting and ensure traceability of decisions, creating a structured environment for managing operational and regulatory risks. Complementing them, analytical environments like Power BI, Tableau, and Python-based solutions allow risk professionals to perform scenario modeling, predictive analytics, and interactive data visualization. The ability to translate raw data into clear insights through such tools represents a core element of digital literacy for risk managers.

At the monitoring and response stages, cybersecurity and automation technologies play a decisive role. Security Information and Event Management (SIEM) systems - such as Splunk, QRadar, or Rapid7 - facilitate continuous monitoring of incidents and automate alerts, while Security Orchestration, Automation, and Response (SOAR) platforms help standardize reaction protocols and reduce Mean Time to Respond (MTTR). Simultaneously, Robotic Process Automation (RPA) tools support repetitive compliance tasks, allowing experts to focus on strategic risk analysis.

Finally, governance and audit assurance are strengthened through model management systems and Explainable AI (XAI) tools that document model lifecycles, ensure transparency, and align with standards such as ISO/IEC 23894 and NIST AI RMF. These instruments not only enhance operational efficiency but also institutionalize accountability and ethical oversight.

e-ISSN 2733-2039 print-ISSN 2733-2144

In sum, digital tools transform risk management from a static compliance function into a dynamic, data-driven process (Table 6). Mastery of these platforms becomes a defining indicator of professional competence, demonstrating a practitioner's ability to integrate analytical insight, technological agility, and governance discipline into organizational resilience.

Table 6. Digital Tools Supporting Risk Management Competencies

Process Stage	Platform / Tool	Function	Operational KPI
Identification	GRC (MetricStream, SAP GRC)	Risk registry, control mapping	% of coverage by controls
Assessment	Python / AutoML / Tableau	Scenario modeling, visualization	MAE/AUC, confidence intervals
Monitoring	SIEM (QRadar, Splunk)	Real-time event detection	MTTD, alert frequency
Response	SOAR/RPA, playbooks	Semi-automated responses	MTTR, % auto-closures
Governance	Model registry, XAI reports	Explainability, audit trail	Validation frequency, compliance ratio

Source: systematized by the author

An ecosystem approach to training risk professionals is increasingly taking shape through triple-helix partnerships that connect universities, industry, and public institutions. Networks such as RiskNet Europe and GARP co-design joint courses that blend academic rigor with corporate practice in digital transformation, AI ethics, cyber-risk modeling, and ESG risk assessment. This integration creates institutional learning pathways that move beyond isolated courses to include stackable certifications, internship pipelines, and participation in international professional communities. In doing so, it aligns curricular content with real organizational needs, accelerates time-to-competence, and embeds graduates and practitioners into living networks where skills are continuously refreshed.

Table 7. Competence Development Roadmap (6–12 Months)

Period	Key Actions	Expected Outcome	Success Metrics
Months 1–2	Skill audit; data/privacy basics	Competency baseline matrix	90% profiles completed
Months 3–4	Workshops on XAI/MLOps; model registry	AI governance policy	100% critical models registered
Months 5–6	Pilot SOAR/RPA automation	Automated playbooks	−30% MTTR improvement
Months 7–9	Drift monitoring; stress tests	Stable model performance	95% retraining SLA met
Months 10–12	Certification; GRC integration	Operational maturity	Audit passed without critical findings

Source: systematized by the author

Table 7 operationalizes the triple-helix approach into a time-boxed plan that organizations can apply to teams or individual practitioners. Each phase specifies actions (e.g., skill audits, XAI/MLOps workshops, SOAR/RPA pilots), expected outcomes (e.g., AI governance policy, automated playbooks), and success metrics (e.g., % models registered, MTTR reduction, retraining SLA adherence, audit pass rates). Managers can use the table as a program board: start with a baseline skills assessment, prioritize high-impact controls, monitor KPI movement quarter-over-quarter, and iterate the roadmap to institutionalize continuous upskilling.

e-ISSN 2733-2039 print-ISSN 2733-2144

Despite momentum, four structural barriers remain. First, there is no unified digital training standard tailored to risk roles, which fragments curriculum design and assessment. Second, a persistent academia–industry expectation gap limits the direct transfer of skills into practice. Third, programs still lack sufficient interdisciplinarity, slowing integration of finance, data science, cybersecurity, and governance. Fourth, ethical and legal dimensions are often under-integrated into technical courses, weakening accountability and trust. Addressing these issues requires a Digital Competence Framework for Risk Managers harmonized with DigComp, ISO, and NIST, plus AI-driven assessment systems that personalize learning trajectories, track proficiency against operational KPIs, and support continuous reskilling in fast-evolving digital environments.

Discussion. The findings confirm that digitalization is transforming the risk management profession from a reactive, compliance-oriented function into a strategic, data-driven discipline. As organizations adopt AI, automation, and data-centric decision systems, risk managers must evolve into analytical leaders capable of interpreting, validating, and governing digital processes.

ISO and NIST frameworks redefine professional competence through governed practice rather than tool familiarity. The integration of ISO/IEC 23894, ISO/IEC 42001, and NIST AI RMF emphasizes transparency, model validation, and AI ethics, creating a new paradigm of trustworthy digital risk governance. These standards establish a foundation for measurable competence, shifting training goals toward model stewardship, explainability, and lifecycle accountability.

Meanwhile, the OECD and WEF frameworks introduce the human dimension - linking digital literacy with social and cognitive resilience. They underline that digital competence must extend beyond technical proficiency to encompass ethical reasoning, cross-functional communication, and adaptive leadership. This convergence of technological and behavioral skills defines the "hybrid professional," capable of managing uncertainty while maintaining compliance, innovation, and trust.

Educational and corporate systems are already moving in this direction. Universities are offering interdisciplinary master's programs in Digital Risk Management, while corporations such as Deloitte, PwC, and Allianz have launched Digital Risk Academies to institutionalize lifelong learning. These initiatives confirm that digital competence must be continuously cultivated through ecosystem partnerships - the "triple helix" model connecting academia, industry, and regulators.

However, the research also reveals significant barriers: fragmentation of standards, lack of empirical metrics for digital proficiency, and weak integration of ethical and legal elements in technical education. Bridging these gaps requires the creation of a Digital Competence Framework for Risk Managers, harmonized across DigComp, ISO, and NIST, and supported by AI-driven assessment systems that monitor skills development over time.

Conclusion. Digital transformation has reshaped the landscape of risk management, demanding a new generation of professionals equipped with technical agility, ethical awareness, and strategic foresight. The study demonstrates that digital

competencies - spanning data analytics, cybersecurity, AI governance, and communication - are now fundamental to effective risk management.

The proposed integrated competency model offers a structured approach for aligning education, certification, and corporate training with international standards. It highlights four core pillars - analytical-technological, cyber and information security, ethical-regulatory, and communicative-leadership - each contributing to organizational resilience and responsible innovation.

Future research should focus on developing quantitative tools for assessing digital competence maturity and measuring its impact on corporate risk performance. Establishing such evaluation systems will enable continuous improvement and benchmarking across industries, ensuring that risk management remains both technologically advanced and ethically grounded in the era of intelligent automation.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Gartner. (2024). *Data literacy: A guide to building a data-literate organization*. https://www.gartner.com
2. Grundke, R., et al. (2018). Which skills for the digital era? *OECD iLibrary*. https://doi.org/10.1787/9a9479b5-en
3. ISO. (2018). *ISO 31000:2018 — Risk management: Guidelines*. International Organization for Standardization. https://www.iso.org
4. ISO/IEC. (2023a). *ISO/IEC 23894:2023 — Artificial intelligence: Guidance on risk management*. International Organization for Standardization. https://www.iso.org/standard/77304.html
5. ISO/IEC. (2023b). *ISO/IEC 42001:2023 — Artificial intelligence management systems (AIMS)*. International Organization for Standardization. https://www.iso.org/standard/42001
6. MIT Sloan. (2024, August 14). *Data literacy: The key to cracking the data culture code*. https://mitsloan.mit.edu/ideas-made-to-matter/data-literacy-key-to-cracking-data-culture-code
7. NIST. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
8. NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
9. NIST. (2024b). *AI Risk Management Framework: Generative AI Profile* (NIST AI 600-1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
10. OECD. (2016). *Skills for a digital world* (OECD Digital Economy Papers, No. 250). https://www.oecd.org/en/publications/skills-for-a-digital-world_5jlwz83z3wnw-en.html
11. Ramachandran, S., et al. (2024). Digital competencies and training approaches to support inter- and transdisciplinary collaboration: A rapid review. *Digital Health, 10*, Article 20552076241252108. https://doi.org/10.1177/20552076241252108
12. Tian, X., et al. (2024). Machine learning in internet financial risk management: A systematic literature review. *PLOS ONE, 19*(7), e0300195. https://doi.org/10.1371/journal.pone.0300195
13. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens* (EUR 31006 EN). Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC128415

14. World Economic Forum. (2023). *The Future of Jobs Report 2023*. https://www.weforum.org/publications/the-future-of-jobs-report-2023
15. Yazdi, M. (2024). Navigating the power of artificial intelligence in risk management. *Safety, 10*(2), 42. https://doi.org/10.3390/safety10020042