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

Digital Competences of Professionals in Security and Fraud Prevention

Igor Korzhevskyi[1]

[1]*Ph.D. (Management), Director, LTD «Risk-Control», Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-3012-0735*

Citation:
Korzhevskyi, I. (2026). Digital Competences of Professionals in Security and Fraud Prevention. *Pedagogy and Education Management Review*, (1 (23), 22–32. https://doi.org/10.36690/2733-2039-2026-1-22-32

Received: February 27, 2026
Approved: March 30, 2026
Published: March 31, 2026

Abstract. *This article examines the content, structure, and practical significance of digital competences of professionals working in security and fraud prevention. The relevance of the topic is determined by the digital transformation of organizations, the growing complexity of cyber-enabled fraud, the expansion of social engineering, and the increasing role of data, digital platforms, and automated systems in detecting suspicious activity and managing security risks. The article proceeds from the assumption that a modern security or anti-fraud professional must combine general digital competence, analytical skills, the ability to work with digital evidence, cybersecurity awareness, and legal, ethical, communication, and lifelong-learning capacities. The aim of the article is to provide a theoretical substantiation of the system of digital competences required in security and fraud prevention and to determine their place in professional training and practice. The methodological basis of the study includes an interdisciplinary approach, logical analysis, systematization, comparison, and generalization of contemporary academic, policy, and analytical sources. As a result, a structural model of digital competences is proposed, covering informational-analytical, cybersecurity, anti-fraud, legal-ethical, and communication-organizational blocks. The study argues that the effectiveness of security and anti-fraud professionals increasingly depends not only on narrow professional expertise but also on the ability to operate in digital environments, interpret risk signals, identify anomalies, critically assess digital information, and act under conditions of rapidly evolving threats. The practical significance of the research lies in the possibility of using the proposed model to update higher education curricula, professional development programs, and organizational personnel development systems.*

Keywords: *digital competences, cybersecurity, fraud prevention, anti-fraud, security professionals, digital literacy, cyber resilience, professional training.*
JEL Classification: M15, M53, D83, G53
Formulas: 0; fig.: 0; tabl.: 3; bibl.: 11

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

Introduction. Digital transformation has fundamentally changed the professional environment in the fields of security and fraud prevention. Whereas earlier security and fraud-control functions relied primarily on document-based verification, physical access control, internal inspections, and traditional financial analysis, current practice increasingly depends on digital traces, monitoring platforms, data analytics, incident-management systems, digital counterparty verification, cyber hygiene, and early-warning mechanisms. In the European context, DigComp 2.2 defines digital competence as the confident, critical, and safe use of digital technologies for learning, work, and participation in society, while also emphasizing interaction with emerging technologies, including AI-related systems. This already indicates that digital competence has moved far beyond instrumental computer literacy and now includes safety, judgment, and responsible action in digital environments (Vuorikari et al., 2022).

At the same time, the profile of fraud itself is changing. The 2024 ACFE global report was based on 1,921 real occupational fraud cases from 138 countries and territories, with aggregate losses in the analyzed cases exceeding USD 3.1 billion. These figures demonstrate not only the scale of fraud as a global organizational problem but also the need for a new type of professional preparation in which the anti-fraud specialist must also function as a data user, digital analyst, and interpreter of technology-enabled risk (ACFE, 2024).

A broader labor-market perspective reinforces this conclusion. The World Economic Forum identifies AI and big data, networks and cybersecurity, and technological literacy among the fastest-growing skills by 2030. This means that professionals in security and fraud prevention are already operating in an occupational environment where digital capability is not optional but central to professional relevance and long-term employability (World Economic Forum, 2025).

Under such conditions, research interest should move beyond the general recognition that digital skills matter. A more precise question emerges: which digital competences are critical for professionals in security and fraud prevention, how are they connected to real professional roles, and how should they be embedded in professional education and continuing development?

Literature Review. In contemporary scholarship and policy discourse, digital competences are increasingly interpreted not as purely technical abilities but as multidimensional combinations of knowledge, skills, attitudes, and responsible behavioral patterns. One of the most influential general models is DigComp 2.2, which structures digital competence through five domains: information and data literacy, communication and collaboration, digital content creation, safety, and problem solving. For the present topic, the most relevant domains are information and data literacy, safety, and problem solving in digital environments, because professionals

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

in security and fraud prevention must work with large volumes of information, distinguish trustworthy and untrustworthy signals, and act securely under conditions of uncertainty (Vuorikari et al., 2022).

However, general digital competence frameworks are insufficient for professions directly linked to security risks and cyber-enabled fraud. In this regard, the European Cybersecurity Skills Framework developed by ENISA is particularly important. ENISA states that the ECSF aims to create a common understanding of the relevant roles, competences, skills, and knowledge required in cybersecurity, to facilitate recognition of cybersecurity skills, and to support the design of training programmes. The framework summarizes cybersecurity-related work into 12 representative role profiles, thereby moving from abstract competence discourse to occupationally meaningful structures (ENISA, 2022).

A similar logic underlies the NICE Workforce Framework for Cybersecurity by NIST. NIST describes the NICE Framework as a common, consistent lexicon that categorizes and describes cybersecurity work and improves communication about how to identify, recruit, develop, and retain cybersecurity talent. Importantly, the framework emphasizes agility and flexibility, acknowledging that organizations must adapt to a constantly evolving cybersecurity ecosystem and that there is no one-size-fits-all competence solution (NIST, 2020).

For fraud prevention, professional and law-enforcement sources indicate that the digital component of risk is continuously intensifying. Europol treats online fraud schemes as a distinct area of criminal threat and links them to payment fraud, stolen data, malware, impersonation, and social engineering. This confirms that contemporary anti-fraud work increasingly unfolds in digital channels and requires the capacity to interpret not only financial irregularities but also technology-enabled behavioral and transactional patterns (Europol, 2025).

In addition, policy-level documents on digital skills emphasize that digital capability is now closely tied to employability, trustworthy information use, social participation, and institutional resilience. This means that in professional domains involving risk, control, and prevention, digital competence should be understood as a structural requirement rather than a secondary enhancement (European Commission, 2025).

At the same time, the existing literature leaves several important gaps. First, much of the literature addresses either general digital competence or cybersecurity workforce development, while relatively few studies focus specifically on digital competences at the intersection of security management and fraud prevention. Second, many existing models are fragmented by professional field: DigComp addresses digital citizenship, ENISA and NIST focus on cybersecurity roles, while fraud-related reports document practical schemes and losses but do not fully theorize competence structures. Third, the literature insufficiently elaborates the organizational

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

dimension of digital competence. Individual skills are widely described, but their role inside governance, compliance, incident response, audit, and internal control systems is much less systematically discussed. Fourth, there is still limited analytical attention to the dynamic character of digital competence in security-related professions, despite the fact that technologies, attack vectors, and fraud scenarios evolve rapidly. These gaps justify the need for a synthetic model that conceptualizes digital competences of professionals in security and fraud prevention as an integrated professional resource.

To make these gaps more explicit, they can be summarized as follows (Table 1).

Table 1. Key research gaps in the study of digital competences of professionals in security and fraud prevention

Research gap	What is insufficiently covered in the literature	Why it matters
Fragmentation of competence approaches	Existing studies usually focus either on general digital competence, cybersecurity workforce models, or fraud practice separately	Security and anti-fraud professionals work at the intersection of these domains and require an integrated model
Limited focus on anti-fraud professional roles	General digital frameworks do not fully reflect fraud analytics, digital evidence handling, anomaly detection, and fraud-risk interpretation	Fraud prevention demands competences that go beyond broad digital literacy
Underdeveloped organizational perspective	Many studies describe individual skills but pay less attention to how competences function inside governance, compliance, audit, and incident-response systems	In practice, digital competence affects both individual performance and organizational resilience
Limited attention to dynamic updating	The literature does not sufficiently emphasize the speed at which competences become outdated under new fraud schemes, cyber threats, and AI-enabled risks	This supports treating digital competence as a continuously updated professional capacity rather than a static skill set

Source: developed by the author based on Vuorikari et al. (2022), ENISA (2022), NIST (2020), ACFE (2024), Europol (2025), World Economic Forum (2025)

The gaps summarized in Table 1 indicate that the current literature does not yet provide a sufficiently integrated model of digital competences for professionals who work simultaneously with security risks, cyber threats, compliance requirements, and fraud prevention tasks. This creates the theoretical basis for the present study.

Aims. The aim of this article is to provide a theoretical substantiation of the system of digital competences required for professionals in security and fraud prevention and to determine their place in professional activity, training, and continuing education.

To achieve this aim, the article addresses the following objectives: to clarify the meaning of digital competences in the context of security- and anti-fraud-related professions; to analyze international frameworks and approaches relevant to defining professional digital competences; to

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

systematize the key groups of digital competences required for professionals in security and fraud prevention; to propose a structural model of digital competences for further use in educational programs and systems of professional development.

Methodology. The study is theoretical and analytical in nature and is based on an interdisciplinary approach combining concepts from digital education, cybersecurity, fraud prevention, risk management, and professional workforce development. The article uses logical analysis to clarify the conceptual apparatus and identify the structural elements of digital competences. Comparison is applied to examine the relationship between general digital competence frameworks and profession-specific cybersecurity and fraud-related models. Systematization is used to group digital competences into functional blocks. Generalization supports the development of an authorial structural model of digital competences for professionals in security and fraud prevention.

The empirical basis of the article is not original fieldwork but published international frameworks, analytical reports, and official materials produced by authoritative organizations, including the European Commission, ENISA, NIST, Europol, ACFE, and the World Economic Forum. Therefore, the conclusions are interpretive and conceptual in nature and are intended to provide a foundation for future empirical and applied studies.

Results. The analysis conducted in this study suggests that digital competences of professionals in security and fraud prevention should not be viewed as an auxiliary technical addition to professional training. Rather, they constitute one of its core structural elements. In today's digital environment, risks, threats, fraudulent practices, and mechanisms for their detection increasingly arise, develop, and leave traces within digital channels. As a result, the effectiveness of professionals in this field depends not only on knowledge of security procedures, control mechanisms, and fraud typologies but also on their ability to work with digital traces, analyze data, interpret risk signals, use digital verification tools, and maintain information and cybersecurity resilience.

The content of digital competences in this field is therefore integrative by nature. Contrary to simplified understandings that reduce digital competence to the use of software or routine applications, in security and anti-fraud work it includes the capacity to operate under uncertainty, identify digital anomalies, connect technological signals with behavioral indicators of risk, assess the legal permissibility of digital actions, and make decisions in an environment of rapidly changing tools, attack vectors, and fraud scenarios. In this sense, digital competence becomes a form of professional adaptability to a new architecture of risks.

The comparative review of international frameworks also shows that no single model fully captures the professional needs of security and anti-fraud specialists. General competence frameworks provide the basis for safe and

critical digital participation, but they do not sufficiently specify occupational security functions. Profession-specific cybersecurity frameworks offer more detailed role-based descriptions, yet they do not always fully integrate anti-fraud analytics, investigative reasoning, digital evidence handling, and communication across organizational functions. This creates the need for a synthetic model.

To clarify the logic of this synthesis, the main international frameworks and sources relevant to digital competences in security and fraud prevention can be summarized as follows.

Table 2. International frameworks and sources relevant to defining digital competences of professionals in security and fraud prevention

Framework / source	Main focus	Relevance for security and anti-fraud professionals
DigComp 2.2	General digital competence for citizens	Provides the foundation for safe, critical, and responsible use of digital technologies
ENISA ECSF	Professional roles, knowledge, and skills in cybersecurity	Offers a profession-oriented model of competences for security functions
NIST NICE Framework	Work roles, tasks, knowledge, and skills in cybersecurity	Connects competences with concrete labor functions and workforce development
ACFE Report to the Nations	Occupational fraud practice and detection	Identifies current fraud risks, losses, and anti-fraud capability needs
Europol online fraud materials	Current online fraud schemes	Reflects real digital fraud scenarios and channels of attack
WEF Future of Jobs Report 2025	Dynamics of emerging skills	Confirms the growing importance of cybersecurity, AI, and technology-related skills

Source: developed by the author based on Vuorikari et al. (2022), ENISA (2022), NIST (2020), ACFE (2024), Europol (2025), World Economic Forum (2025)

The evidence summarized in Table 2 demonstrates that digital competences in this field emerge at the intersection of at least three domains. The first is general digital literacy, which involves safe, critical, and responsible use of digital technologies. The second is profession-specific cybersecurity preparedness, including knowledge of digital threats, system protection logic, access control, incident management, and interaction with IT infrastructure. The third is the anti-fraud dimension, where the key competences concern identifying fraud patterns, interpreting transactional and behavioral anomalies, handling digital evidence, and evaluating risk across organizational functions.

On the basis of this synthesis, it becomes possible to propose a five-block structural model of digital competences of professionals in security and fraud prevention.

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

Table 3. Structural model of digital competences of professionals in security and fraud prevention

Competence block	Content	Example of professional manifestation
Informational-analytical	Searching, verifying, interpreting, visualizing, and critically analyzing digital data	Analysis of suspicious transactions, OSINT-based counterparty verification, detection of anomalies
Cybersecurity	Cyber hygiene, access control, system protection, understanding digital vulnerabilities	Incident handling, access management, account protection, secure data handling
Anti-fraud	Recognition of digital fraud schemes, fraud patterns, and risk triggers	Detection of phishing, fake accounts, collusion, digital document manipulation
Legal-ethical	Compliance with legality, confidentiality, procedures, and digital ethics	Proper handling of evidence, personal data protection, incident documentation
Communication-organizational	Cross-functional interaction, reporting, crisis communication, staff training	Anti-fraud training, communication of risks to management, coordination with IT and compliance

Source: developed by the author

Table 3 shows that digital competences in security and fraud prevention form a coherent professional system rather than a loose set of isolated skills. The informational-analytical block is essential for working with digital traces, electronic documents, transaction data, open sources, and internal information flows. It allows professionals not merely to collect digital information but to verify, compare, and interpret it critically.

The cybersecurity block reflects the fact that professionals in this field operate in environments where information processes are constantly exposed to risks such as unauthorized access, credential compromise, data leakage, and loss of system integrity. This block is important not only for technical protection but also for understanding the logic of organizational digital vulnerability.

The anti-fraud block concentrates specifically on the competences needed to identify fraud in digital environments. It includes the ability to detect fraud scenarios, work with risk profiles, notice atypical behavioral or transactional deviations, analyze social engineering signals, and assess how digital tools are used to bypass controls or conceal misconduct.

The legal-ethical block is equally important. In security and fraud prevention, digital actions cannot be effective if they are not aligned with legality, confidentiality, procedural correctness, and ethical permissibility. Work with digital evidence, personal data, internal monitoring systems, and investigative materials requires not only technical but also legal literacy.

The communication-organizational block reflects the fact that professionals in this field rarely act in isolation. They must interact with IT units, compliance, internal audit, HR, management, and sometimes external actors. Therefore, digital competences also include the ability to translate digital findings into understandable managerial conclusions, recommendations, and preventive actions.

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

Taken together, the proposed five-block model demonstrates that digital competences in security and fraud prevention are multilevel, interdependent, and functionally integrated. Deficiency in any one block weakens overall professional effectiveness. Thus, the results make it possible to formulate a generalized logic of professional action in this field: digital literacy and safe technology use → analytical processing of digital data → identification of anomalies and risk patterns → interpretation of fraud or security threats → evidence-based decision-making → coordination, prevention, and organizational learning.

Discussion. The results obtained in this study allow for broader theoretical reflection on the role of digital competences in the professional activity of specialists in security and fraud prevention. First, digital competences can no longer be seen as a peripheral addition to professional training. Their function has changed substantially. If digital tools were once treated mainly as instruments supporting core work, today the digital environment itself has become the main space in which risks emerge, evolve, are concealed, and are detected. In this context, digital competences turn into one of the main determinants of professional capability and of the ability to act effectively, lawfully, and analytically under conditions of uncertainty.

A particularly important conclusion of the study concerns the integrated character of digital competences. Professional effectiveness in security and fraud prevention is not ensured by isolated digital skills. Rather, it is formed at the intersection of several mutually reinforcing dimensions: digital literacy, cybersecurity readiness, analytical capacity, anti-fraud reasoning, legal culture, and communication-based coordination. This interdependence defines the contemporary professional profile. The ability to use analytical tools is insufficient if a specialist cannot interpret suspicious signals in light of organizational context, behavioral indicators, risk patterns, and legal limitations. Likewise, knowledge of cyber threats alone remains insufficient without the capacity to communicate those risks to management and embed them into preventive governance mechanisms.

This makes it possible to argue that digital competences in this field should be treated not merely as a set of skills but as a form of professional readiness for operating in digitally mediated uncertainty. Such readiness includes the ability to work with incomplete information, recognize weak signals of risk, correlate heterogeneous digital data, assess their credibility critically, and make decisions in contexts where threats and tools evolve continuously.

The analysis also clarifies the place of international frameworks in shaping the competence profile of such professionals. General models such as DigComp 2.2 are highly valuable as a foundation for safe, critical, and responsible digital behavior. Profession-specific frameworks such as ENISA ECSF and NIST NICE offer a more detailed account of roles, knowledge, and tasks in cybersecurity. Yet none of these frameworks on its own fully

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

incorporates the behavioral, investigative, financial-analytical, and compliance dimensions of fraud prevention. The synthetic model proposed in this article is therefore important not only as a theoretical construction but also as an attempt to overcome the fragmentation of existing approaches.

Another important issue concerns the relationship between digital competences and organizational resilience. In practical terms, insufficient or fragmented digital competence among personnel is not simply an educational weakness. It is a direct risk factor. An employee who cannot identify phishing signals, does not understand the logic of digital control circumvention, fails to verify the reliability of digital sources, or mishandles sensitive data may effectively become a weak link in the organization's security architecture. Therefore, digital competences should be interpreted not only as an individual professional resource but also as a component of organizational risk management, compliance, and resilience.

From this perspective, the preparation of professionals in security and fraud prevention must change not only quantitatively but qualitatively. It is not enough to add several technology-related courses to existing training programs. Rather, the very logic of professional education needs to be reconsidered. Digital competences should be embedded across all key components of professional preparation, including risk analysis, investigation, internal control, compliance, incident management, information security, communication, and ethical decision-making.

The issue of continuous updating is particularly significant. Unlike some traditional areas of professional knowledge that remain stable over time, digital competences in security and fraud prevention are subject to rapid obsolescence because both technologies and fraud schemes evolve quickly. This means that digital competence should not be understood as a fixed educational outcome but as a dynamic professional capacity for adaptation, upskilling, and relearning. Consequently, simulation-based training, case analysis, incident-based exercises, and modular continuing education become especially important in competence development.

In practical terms, the model proposed in this article may be used in several directions. It can serve as a basis for updating higher education programs that prepare specialists in economic security, cybersecurity, compliance, internal audit, and risk management. It can be adapted for organizational staff-assessment systems in which digital competences become one of the indicators of professional maturity and readiness to handle incidents. It can also support professional-development programs that aim not only at technical training but also at integrating analytical, ethical, and communication dimensions of digital professional work.

At the same time, the study has limitations. The conclusions are conceptual and analytical and are based on the systematization of international frameworks, reports, and scholarly sources. They have not yet been empirically validated on samples of professionals working in security

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

and fraud prevention. In addition, different sectors may require different configurations of digital competences depending on regulation, digital maturity, dominant risks, and internal control models. Future research should therefore focus on empirical validation of the proposed structure, development of indicators for assessing each competence block, and comparative testing of their relevance across sectors and professional roles.

Overall, the discussion confirms that digital competences of professionals in security and fraud prevention are not merely a sign of modernization but a foundational condition of effective professional activity. They combine technical, analytical, behavioral, legal, and organizational dimensions and thereby shape a new standard of professional capability under conditions of digitally transformed risks.

Conclusion. The article has demonstrated that digital competences of professionals in security and fraud prevention constitute a multidimensional professional characteristic that includes not only technical skills but also analytical, cybersecurity-related, legal, ethical, and communication components.

It has been argued that, under contemporary conditions, the effectiveness of professionals in this field increasingly depends on their ability to work with digital data, recognize digital fraud patterns, maintain secure digital environments, critically assess information, and coordinate actions under conditions of risk. The proposed five-block structural model allows the requirements for such professionals to be systematized and may be used to modernize educational programs, professional standards, and internal organizational personnel-development systems.

Future research should focus on empirical validation of the proposed model, development of tools for assessing the level of digital competences of security and anti-fraud professionals, and adaptation of the model to different sectors, including finance, public administration, education, and corporate governance.

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.

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

References:

1. Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf
2. ENISA. (2022). *European Cybersecurity Skills Framework (ECSF)*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf
3. ENISA. (2022). *European Cybersecurity Skills Framework role profiles*. European Union Agency for Cybersecurity. https://shorturl.at/fjFxt
4. ENISA. (2022). *European Cybersecurity Skills Framework user manual*. European Union Agency for Cybersecurity. https://shorturl.at/eV0v3
5. European Commission. (2025). *Digital skills*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/digital-skills
6. European Commission. (2025). *Digital skills initiatives*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives
7. Europol. (2025). *Online fraud schemes*. Europol. https://www.europol.europa.eu/crime-areas/online-fraud-schemes
8. National Institute of Standards and Technology. (2020). *Workforce Framework for Cybersecurity (NICE Framework)* (NIST SP 800-181 Rev. 1). NIST. https://doi.org/10.6028/NIST.SP.800-181r1
9. National Institute of Standards and Technology. (2025). *NICE Framework current versions*. NIST. https://shorturl.at/SfWNc
10. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. Publications Office of the European Union. https://doi.org/10.2760/115376
11. World Economic Forum. (2025). *The Future of Jobs Report 2025*. World Economic Forum. https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf