Funded by the European Union

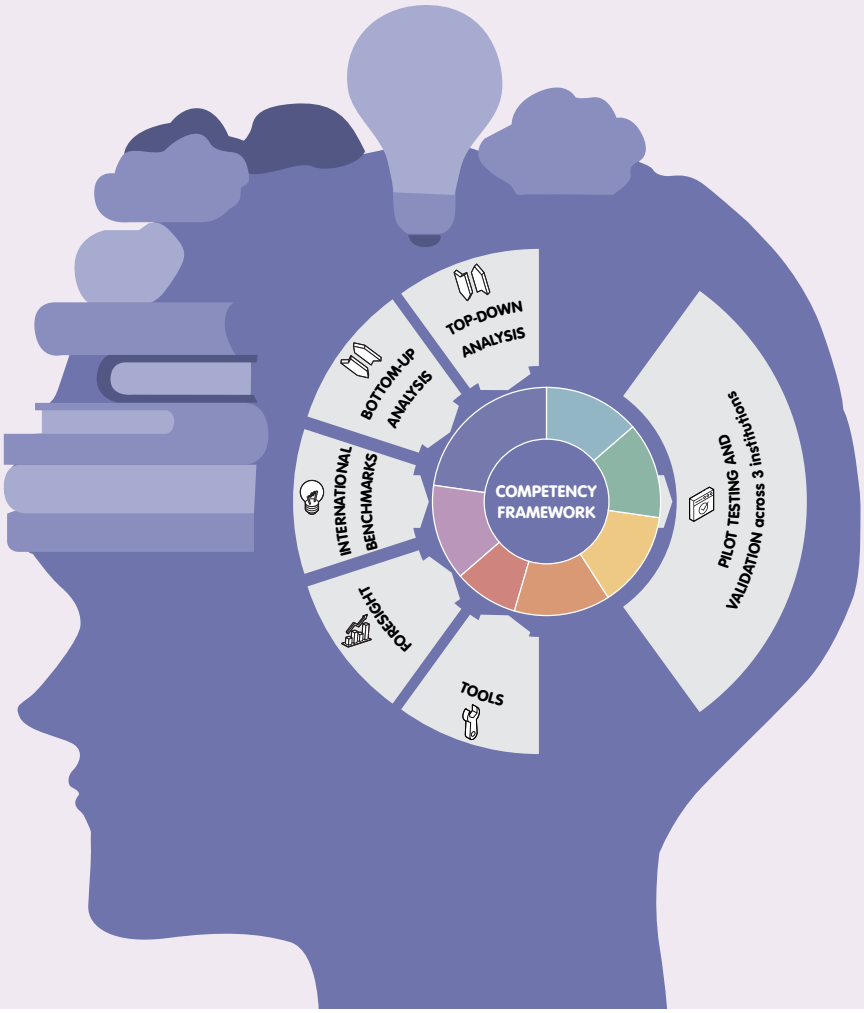
Agenția Națională a Funcționarilor Publici

Autoritatea pentru Digitalizarea României

Activity 5
Event and report on lessons learned for other member states

OUTPUT 5

THE DIGITAL COMPETENCY FRAMEWORK FOR THE PUBLIC ADMINISTRATION - DISTILLED VERSION AND LESSONS LEARNED FROM THE DESIGN PROCESS IN ROMANIA



WORLD BANK GROUP

DISCLAIMER

This document was produced with the financial assistance of the European Union. Its content is the sole responsibility of the authors. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

This project is carried out with funding by the European Union via the Technical Support Instrument (TSI) managed by the European Commission's Reform and Investments Task Force (SG REFORM) and implemented by the World Bank with the support and the partnership of SG REFORM.

This work is a product of the staff of the World Bank. The findings, interpretation and conclusions expressed in this paper do not necessarily reflect the views of the Executive Directors of the World Bank, the European Commission or the Government. The World Bank does not guarantee the accuracy of the data included in this work.

COPYRIGHT STATEMENT

1818 H Street NW, Washington DC 20433

Telephone: 202-473-1000; Internet: www.worldbank.org

ACKNOWLEDGEMENTS

The report was prepared under the Technical Support Instrument (TSI) component *"Romania: Developing a General Digital Competence Framework for Civil Servants"*, led by Anca Butnaru (Senior Public Sector Expert), Dimitrie Mihes (Senior Public Sector Specialist) and Fanny Weiner (Senior Public Sector Specialist).

This report was developed by Anca Butnaru (Senior Public Sector Expert) and Cristina Zamfir (Senior Public Sector Expert). Key inputs were also provided by: Riina Vuorikari (Senior International Digital Competence Expert), Cezar Haj (Public Sector Expert), Marius Merluşcă (Senior HRM Expert), Magdalena Popescu (Senior Communication Expert and HRM Expert) and Sorana Gheorghiade (Governance Analyst).

Riina Vuorikari led the technical design process, with key inputs provided by Cezar Haj, Marius Merlusca, Anca Butnaru and Cristina Zamfir. Inputs were also provided by Mogens Andersen (Senior Digitalization Expert) and Ramona Moldovan (Senior Public Sector Expert).

The report also benefited from technical inputs from Judith Cosgrove (Scientific Officer, European Commission - Joint Research Centre), Sven Schade (Scientific Project Leader, European Commission - Joint Research Centre) and Simon Vrecar (External Consultant, European Commission - Joint Research Centre).

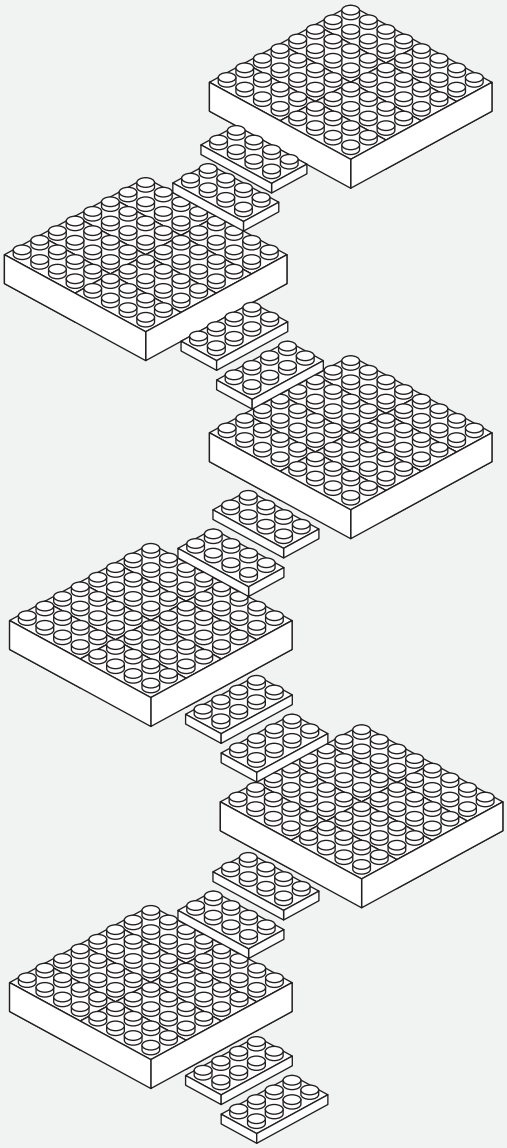
Anita Sobjak (Senior Public Sector Specialist), Kai-Alexander Kaiser (Senior Governance and Public Sector Specialist) and Fanny Weiner (Senior Public Sector Specialist) provided valuable insights as peer reviewers.

The team would like to thank Fabian Seiderer (Practice Manager, Governance Global Practice, Europe and Central Asia), Yasser El-Gammal (Country Manager for Romania), and the Romania Portfolio Team for their overall advice, guidance, and support throughout the development of this report.

The graphic design of this report was done by Razvan Zamfira (Senior Graphic Editor), in coordination with Magdalena Popescu.

The team would like to express its gratitude to the counterparts in SG REFORM, in particular to Johannes Boermann (Head of Sector), in the National Agency for Civil Servants, in particular to Lavinia Niculescu (Director) and Cristina Panțîru (Public Manager), in the National Institute for Administration, in particular to Ioana Melenciuc-Ioan (President), Alina Blei (Director) and Alina Sandu (Head of Service) and in the Authority for the Digitalization of Romania, in particular to Alina Paraiala (Head of Service), Cristina Catai (e-Government Expert) and Sabin Dragoman (e-Government Expert) for their constructive collaboration, as well as to other government agencies and private sector entities who actively participated in consultations and interviews.

This report has been delivered in January 2026, under the EC Contract No. REFORM/IM2024/005 (under TF074110). It has been delivered as part of the project "Romania: Developing a General Digital Competence Framework for Civil Servants" (Donor code 24RO12).



Index of figures

Index of tables

Index of boxes

Executive Summary

Project context

Digital transformation has fundamentally reshaped what public administrations do and how civil servants must perform their roles. Technologies such as artificial intelligence, data analytics, automation, cloud infrastructures and digital platforms have moved from peripheral tools to core mechanisms through which governments design policies, deliver services, manage risks and uphold democratic accountability. Public administration employees are now expected not only to operate digital systems but also to understand their implications, safeguard public data, cooperate across institutions, and adapt to rapidly evolving regulatory and technological environments. In this context, digital competence has become a universal capability rather than a specialist function, inseparable from the effective exercise of public authority.

The European Union (EU) has progressively established a strategic and legal architecture that elevates digital competence to a core capability for modern public administration. The Digital Decade Policy Programme 2030, the European Declaration on Digital Rights and Principles, the European Skills Agenda and the Pact for Skills articulate an ambitious vision of digitally mature administrations. EU legislation such as the Open Data Directive, the Data Governance Act, the Data Act, the Interoperable Europe Act, and the Single Digital Gateway Regulation require civil servants to work with data in interoperable, secure, and reusable formats and to communicate digitally in an accessible and citizen-centric manner. At the same time, the AI Act, GDPR, NIS2, eIDAS 2.0, impose concrete obligations for AI literacy, human oversight, data protection, and cybersecurity across public administrations[1]. These requirements make clear that digital capability is now essential for public administration performance, institutional resilience and trust.

As the scope and ambition of digital and AI-driven reforms in public administration continue to expand, the need for a clear and shared understanding of the digital competencies required from public administration employees has become increasingly important. DigComp[2] offers a structured baseline for individuals' digital empowerment, but its orientation does not reflect institutional mandates or the accountability of public office. The e-Competence Framework defines competencies for ICT professionals[3] but does not cover the broader population of public officials who increasingly make decisions shaped by technological, data and cybersecurity considerations. Several Member States have already developed adaptations of digital competency frameworks for the public administration, confirming both the usefulness of these instruments and the need for a framework tailored to administrative realities.

Methodological approach

In this context, the World Bank, in partnership of the European Commission, supported the Government of Romania (GoR) to develop a General Digital Competence Framework for Public Administration through the Technical Support Instrument (TSI) *"Romania: Developing a General Digital Competence Framework for Civil Servants"*. The overarching goal of the TSI project[4] is to strengthen the digital capabilities of Romanian civil servants so that they can contribute more effectively to public service delivery and advance the country's digital transformation. The effort directly supports several national priorities, including improved human resource management, enhanced administrative capacity and alignment with European digitalisation objectives. The beneficiary institutions are the National Agency for Civil Servants

1. A full mapping of relevant EU legislation that underpinned the design process for the proposed digital competency framework is included in Output 1 developed under the TSI project Developing a General Digital Competency Framework for Civil Servants in Romania: World Bank (2025), Report on the assessment of the digital competencies needed in the Romanian public administration.
2. COSGROVE, J. and CACHIA, R., DigComp 3.0: European Digital Competence Framework - Fifth Edition, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/0001149.
3. ICT specialists are defined as "*workers who have the ability to develop, operate and maintain ICT systems, and for whom ICT constitutes the main part of their job*", in line with Eurostat definition. Glossary: ICT specialists - Statistics Explained - Eurostat
4. This project is carried out with funding by the European Union via the Technical Support Instrument (TSI) managed by the European Commission's Reform and Investments Task Force (SG REFORM) and implemented by the World Bank with the support and the partnership of SG REFORM.

(NACS)[5], the Authority for the Digitalization of Romania (ADR)[6], and the National Institute for Administration (INA)[7], the key institutions responsible for HRM policies, digital transformation and public administration training.

The project's methodological approach was designed to translate broad reference models into a digital competence framework suitable for the organisational structures, mandates and HRM systems of public administration in Romania. The development of the framework followed a structured assessment and design process comprising: (i) analysis of the policy and regulatory environment; (ii) large-scale job analysis; (iii) international benchmarking; (iv) foresight on future digital roles; (v) extensive consultation and co-design with institutions; (vi) pilot testing and validation; (vii) construction of a descriptor bank grounded in international evidence; and (viii) formulation of recommended operationalisation pathways for embedding the framework across HRM and capability-building systems.

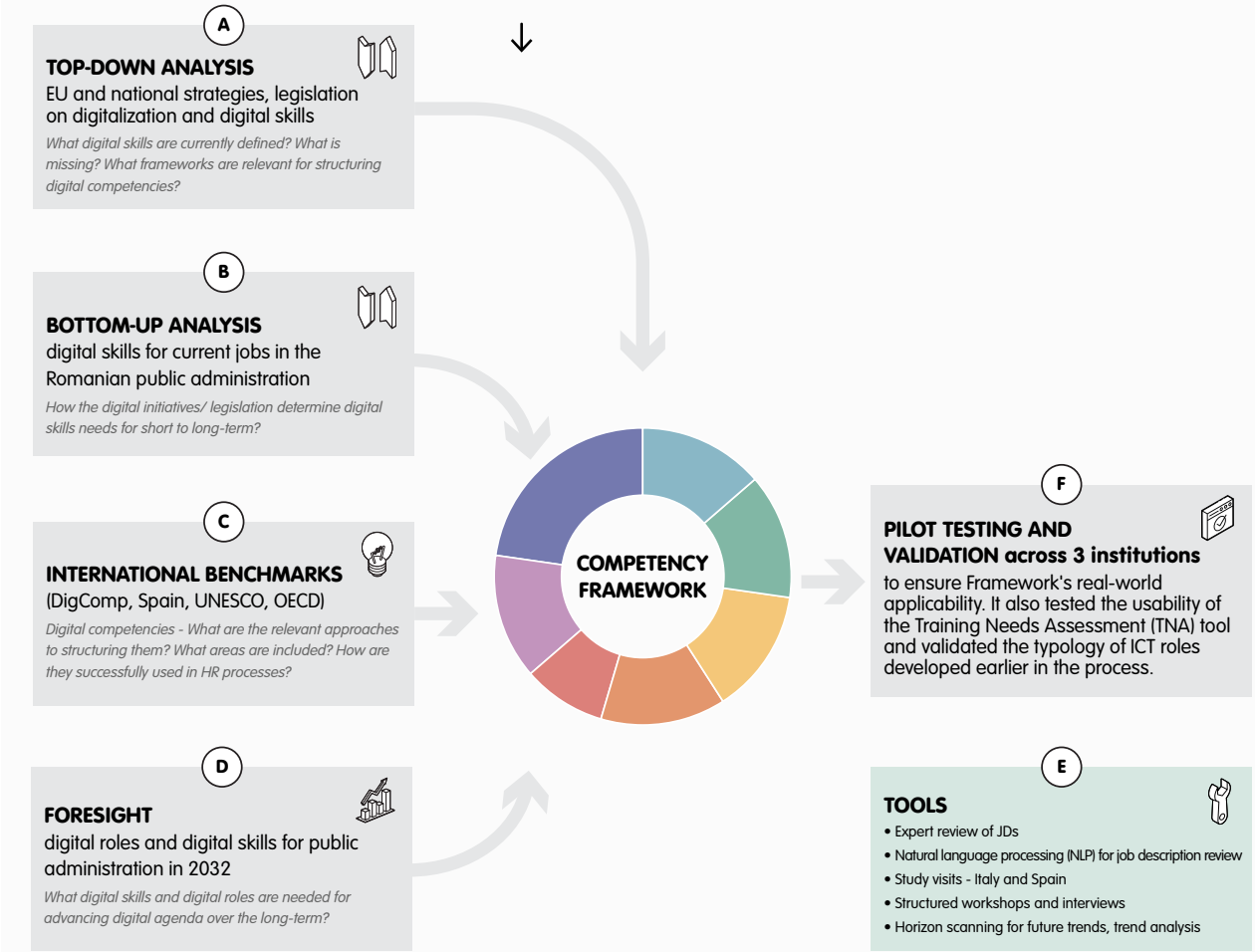
These various workstreams under the TSI project were reflected in previous outputs, as follows:

- **Output 1[8] ensures the analytical foundations** mentioned in points (i) – (iv) above, covering an in-depth assessment of the digital competencies needed in the public administration. This assessment targeted the Romanian civil service, but also the European level strategic and regulatory framework and relevant international experience;
- **Output 2 proposes a Digital Competency Framework Model for the Public Administration in Romania** and presents the design process, consultations and pilot results, covering also points (v) – (vii) above;
- **Outputs 3 and 4 focus on operationalization in the Romanian context** (point viii above): Output 3 addressed the legal and procedural integration of the framework into key HR processes, while Output 4 focused on the training system, proposing an updated digital training needs assessment methodology, reviewing international digital skills assessment platforms, and outlining curriculum elements.
- **Output 5 - the current report, presents the reference digital competency framework proposed for public administrations beyond the Romanian specific context**, summarizes the Romanian design process to inform similar reforms elsewhere, and distils key lessons learned.

The project began by examining the policy and regulatory environment shaping digital transformation and HR development in Romania. This analysis revealed fragmented mandates, gaps in capability-development systems and the absence of a unifying digital skills strategy for the civil service. The work then moved to the institutional level through an examination of 2,380 job descriptions, complemented by workshops, interviews, focus groups and AI-assisted text analysis. This revealed inconsistent and incomplete representations of digital capability in job documentation and highlighted the lack of structured pathways for ICT roles. These insights confirmed the need for a competency model that would clarify expectations across institutions while accommodating functional diversity.

5. NACS is the central public institution with the mandate to design and implement the ambitious HRM reforms of the Romanian public administration.
6. ADR's main role is to oversee and drive the digital transformation of the country.
7. INA is the primary institution responsible for civil service training.
8. World Bank, Output 1- *Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service: Taking Into Account Relevant Policies at the National and European Union Levels (English)*. http://documents.worldbank.org/curated/en/099071725093059745.

FIGURE 1: Design process rooted in national and European-level assessments



Source: Authors' elaboration

International benchmarking strengthened the conceptual foundation and ensured alignment with emerging European standards. The project reviewed a broad range of frameworks, including DigComp 2.2 and 3.0, national public-administration adaptations from Spain[9] and Italy[10], UNESCO and ITU models related to AI and digital transformation[11], Apolitical's AI-readiness Check for Civil Servants[12], the European e-Competence Framework[13], the European Cybersecurity Skills Framework[14] and the Skills Framework for the Information Age. For example, the Apolitical AI Readiness Check was used as an input to validate the inclusion of transversal AI literacy elements, particularly ethical awareness, risk understanding, and responsible use expectations for non-technical staff.

9. INAP, "Marco de Competencias Digitales," Spain, 2023. https://www.inap.es/es/aprendizaje/ecosistema-competencial/marco-de-competencias-digitales
10. Italy, Syllabus for Digital Skills for the public administration.
11. UNESCO, Broadband Commission ITU, "Artificial intelligence and digital transformation: competencies for civil servants - UNESCO Digital Library," 2022. https://unesdoc.unesco.org/ark:/48223/pf0000383325
12. Apolitical, AI Readiness Check: https://apolitical.co/en/pages/arc.
13. https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf.
14. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

Foresight analysis ensured that the framework would not only address current needs but anticipate future digital roles, capabilities and organisational models. The exercise, conducted jointly with experts from the EC's Joint Research Centre and the Prospectiva Foresight Institute, explored how digital transformation is likely to reshape administrative functions over the next decade. It identified a continuum of roles - ICT-intensive, ICT-enhanced and ICT-dependent - and highlighted the rise of hybrid profiles such as AI governance specialists, data stewards, digital transformation leaders and service orchestrators. This forward-looking lens ensured that the framework would remain relevant as technologies evolve and as public institutions adopt more predictive, data-driven and collaborative models of governance.

Extensive consultation and co-design with Romanian institutions grounded the framework in administrative practice and ensured its operational feasibility. More than twenty institutions participated in a structured HR technical working group, jointly convened with the National Agency for Civil Servants (NACS). The HR Working Group included HR experts from the central public administration. The Group was involved in refining competency definitions, shaped the proficiency scale, clarified terminology and validated the framework's overall structure. Consultations also revealed broader system needs, including credible mechanisms for certification, stronger integration with HRM processes and the importance of plain administrative language.

The formulation of recommended operationalization pathways was integral to the methodological design. This component translated the framework into actionable processes for job analysis, recruitment, learning and development, performance management and career progression, and sequencing strategies tailored to different levels of HRM maturity. It also proposed digital-platform requirements for training needs assessment (TNA) and training curriculum for public administration. As a result, the framework was conceived not only as a conceptual model but as a fully implementable system embedded in public-administration capability development.

Pilot testing and validation confirmed the framework's usability and informed refinements to descriptors, proficiency levels and associated tools. Institutions tested the applicability of descriptors across different job families and validated associated methodologies. The pilots confirmed that the framework was sufficiently clear, flexible and comprehensive to support real-world applications.

To support transferability beyond Romania, a non–Romania-specific version of the digital competency framework was prepared and is proposed in this report, removing country-specific institutional and policy references while preserving its full conceptual structure and level of rigor. The framework builds on established international references, notably DigComp and translates them into a coherent model tailored to public administration needs. Its transferability lies in its modular design and maturity-sensitive implementation logic, which allow other administrations to adopt the framework in full or apply it selectively depending on their institutional capacity, reform priorities, and stage of digital transformation.

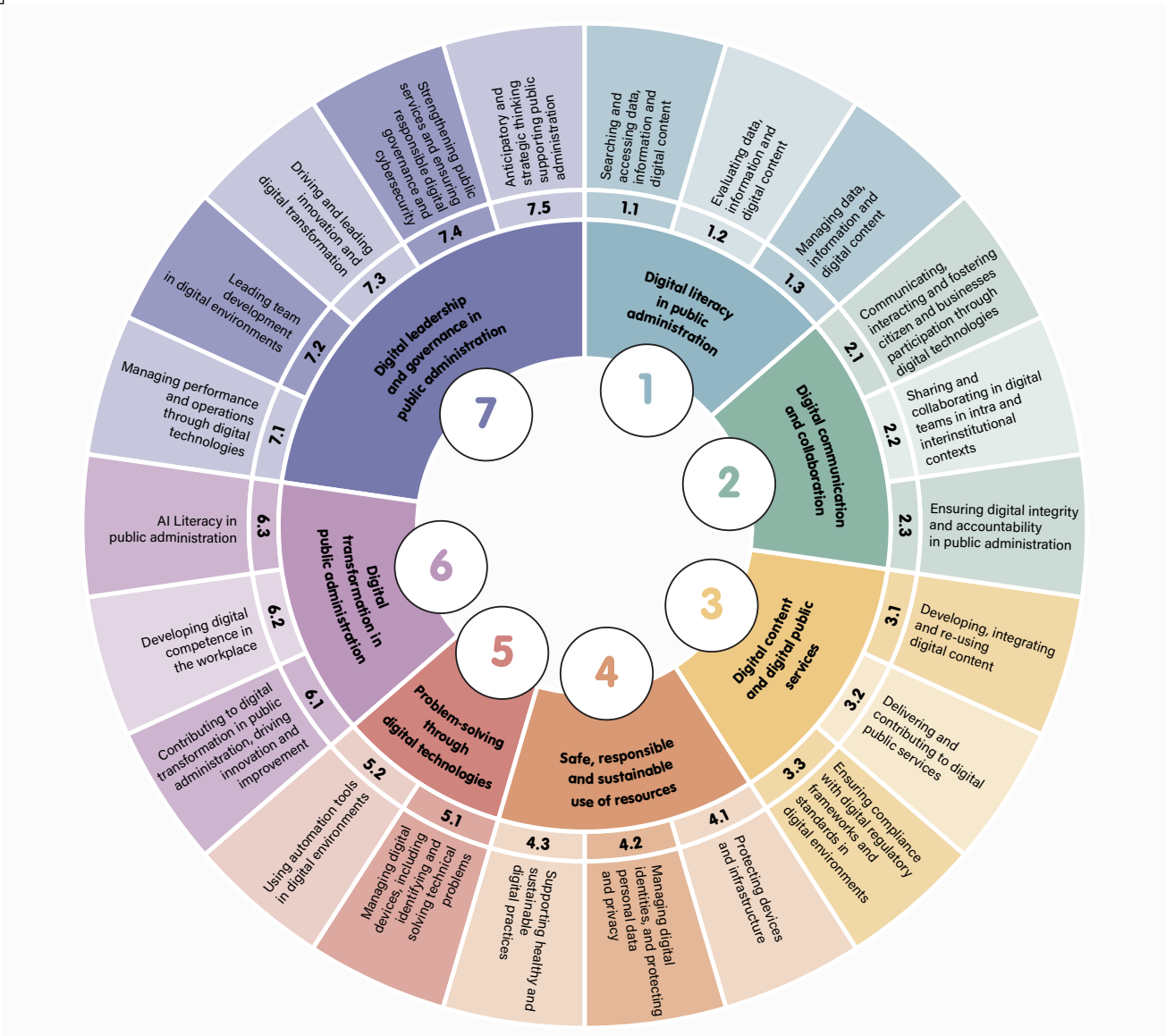
Result 1: The Digital Competence Framework for the Public Administration

The project resulted in a comprehensive framework, grounded in European and international standards and tailored to public administration mandates. The design proposed in Output 2 (which also includes specific references for Romania) and that is reflected also in this report as a generic model draws closely on DigComp for conceptual structure and progression, on the European e-Competence Framework for distinctions between generalist and specialist ICT roles, and on public administration models from the OECD, World Bank and UNESCO that emphasize digital collaboration, responsible data use, cybersecurity awareness and digital leadership. These sources shaped a definition of "general digital competence" that reflects public administration's dual responsibility: delivering services efficiently while upholding legality, fairness, security and trust. The resulting definition emphasizes confident, critical, ethical and effective use of digital technologies and data for public value creation.

"General digital competence in the public administration is the confident, critical, responsible, and effective use of digital technologies, data, and information systems to deliver, innovate, and improve public services, in ways that are secure, ethical, inclusive, and aligned with national and European digital transformation objectives. It encompasses an integrated set of knowledge, skills, and attitudes required to access, evaluate, create, and manage digital resources; collaborate and communicate effectively in digital environments; ensure data protection, cybersecurity, and ethical AI use; leverage data and digital infrastructures for evidence-based policymaking, citizen engagement, and organizational transformation; and adapt to emerging technologies and evolving societal needs."

The framework is organized into seven competency areas, comprising 22 competencies described across three proficiency levels. It brings together two structural dimensions: (i) three competency types - fundamental competencies for all staff, digital-transformation competencies for specialized non-IT functions, and managerial competencies for leadership roles; and (ii) seven thematic areas grouping related competencies. Each competency is articulated through descriptors of knowledge, skills and attitudes at Levels A (basic), B (intermediate) and C (advanced), enabling self-assessment, structured evaluation and curriculum design. The modular structure mirrors international best practice and supports both horizontal comparability and vertical progression across roles and seniority levels.

FIGURE 2: Digital Competency Framework for Public Administration



Source: Authors' elaboration

Alignment with DigComp ensures EU coherence, traceability and future adaptability. Areas 1–5 build directly on DigComp's logic for digital literacy, but have been tailored to reflect public administration realities, such as working with institutional systems, ensuring interoperability, safeguarding data, and applying responsible AI practices. Areas 6 and 7 introduce competencies specific to digital transformation and digital leadership, which are addressed only in a generic manner in DigComp, primarily from the perspective of individual proficiency, and required further extension and development to reflect the organisational, governance, and leadership functions essential to modern public administration. The framework was subsequently updated to integrate DigComp 3.0, incorporating a stronger focus on AI and safety, allowing mapping to granular learning outcomes. This ensures conceptual consistency with core EU initiatives, including the Digital Decade and the Union of Skills agenda.

The proposed model responds to the strategic direction set at EU level, where artificial intelligence has been identified as a major opportunity for improving public administration, while recognising that adoption across Member States remains uneven and at an early stage in many policy areas[15]. EU-level analyses have consistently highlighted that the main constraints to effective AI uptake are not technological availability, but gaps in skills, organisational capacity, governance arrangements, and regulatory preparedness[16]. Against this backdrop, the model introduces a dedicated competency on AI literacy to establish a shared baseline for civil servants across Member States, while also embedding AI-related descriptors across multiple competency areas. This dual approach reflects the European understanding that AI is not a standalone technical subject, but a cross-cutting capability with implications for service delivery, management practices, procurement, and public-sector governance. As the European Commission has progressively mobilised significant investment through programmes such as Horizon Europe, Digital Europe, and NextGenerationEU to support AI experimentation, scaling, and reuse in the public sector, the framework equips public officials to understand AI concepts and use cases, engage meaningfully with technical experts and suppliers, and anticipate key risks related to transparency, data protection, bias, and accountability. In doing so, it supports preparedness for the implementation of the EU AI Act and aligns with the EU's long-standing objective of promoting trustworthy, human-centric AI grounded in European values. By integrating AI considerations across both operational and strategic competencies, the model provides a forward-looking foundation for building administrative capacity ahead of wider AI uptake in the European public sector, in line with the policy trajectory and investment priorities defined at EU level.

To complement general competencies, the project developed a structured framework for specialised ICT roles essential to digital government. Digital transformation requires not only transversal digital capability but also professional ICT roles responsible for architecture, cybersecurity, development, operations, data, service design and product management. The project mapped ICT functions in Romanian institutions against the European e-Competence Framework and the European Cybersecurity Skills Framework, producing a set of 24 ICT roles organised into six job families. This approach distinguishes between roles (what work needs to be done) and jobs (how posts are classified in HRM systems), enabling governments to diagnose capability gaps, reduce over-reliance on outsourcing and build structured digital career paths.

15. EC, 2024, *Adopt AI study*, available at https://digital-strategy.ec.europa.eu/en/library/eu-study-calls-strategic-ai-adoption-transform-public-sector-services.
16. Communication from the Commission, Artificial Intelligence for Europe. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

TABLE 1: Proposed ICT roles and jobs[16]

Public ICT function/job	Predominant associated ICT roles from the 24 proposed
ICT Manager	Business Information Manager, CIO, Digital Transformation Leader, ICT Operations Manager, Product Manager
ICT Architect	Enterprise Architect, Systems Architect, Solution Designer
Cybersecurity specialist	Information Security Manager, Information Security Specialist
ICT Service Delivery and Support specialist	Network Specialist, Service Support, Systems Administrator, Technical Specialist, Test Specialist
ICT Service Management specialist	Business Analyst, ICT Specialist, Service Designer, Systems Analyst
ICT Development and Data Specialist	Database Administrator, Data Scientist, Data Specialist, Developer, User Researcher

In the scope of the TSI project, digital skills are treated as foundational enablers of digital transformation, rather than as outcomes in themselves. Adequate digital competencies are necessary for public servants to effectively use digital systems, redesign processes, manage and share data, and embed new ways of working. Experience from Romania and other EU administrations shows that where digital skills do not keep pace with technological investments, digital reforms tend to remain superficial, with limited uptake, parallel manual processes, and weak institutionalization. Empirical analyses across EU member states also find that higher levels of digital skills at the national level are associated with stronger overall digital transformation performance[18], Country experience from digital leaders such as Estonia, indicates that sustained public-sector digitalization depends as much on workforce capabilities as on technology itself[19].

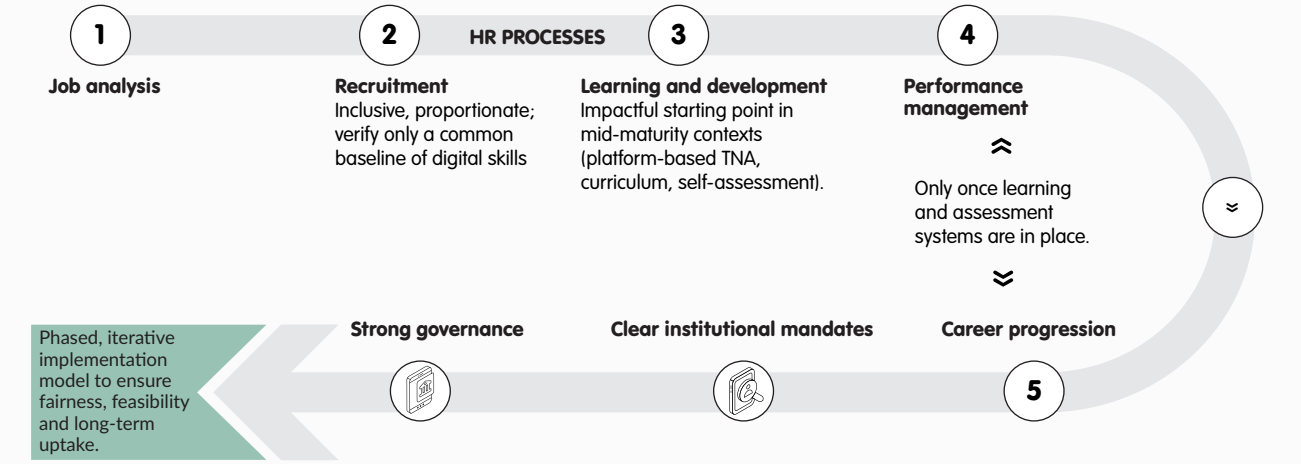
Result 2: Recommended pathways for operationalising the Framework across HRM and capability-building systems

A key contribution of this project is the development of a maturity-sensitive pathway for putting the framework into practice across public-administration HRM processes. While the framework provides a clear definition of the digital capabilities required of today's civil service, its value depends on how effectively it is embedded into recruitment, development, performance management and career progression. Because EU Member States vary considerably in HRM maturity, digital readiness, and institutional capacity, the operationalization model distinguishes between feasible pathways for different starting points. The recommendations presented in this report are thus calibrated to a mid-range maturity context, informed by the experience of piloting the framework in one Member State (i.e. Romania) whose HRM system is undergoing reform and where workforce digital skills remain uneven.

The operationalization approach begins from the recognition that a framework must be integrated into existing HR systems, but in a sequence that matches institutional capacity. In administrations with limited or inconsistent competency-based HRM practices, digital competencies cannot be introduced across all HR processes at once. Doing so risks overburdening HR units, reducing fairness in recruitment, or generating compliance-oriented implementation rather than genuine capability building. For these systems, digital competencies are best introduced first through lower-stakes, design-oriented processes - most importantly job analysis and learning and development - allowing institutions to build familiarity and capacity before applying digital evidence in other HR decisions.

17. As reflected in the Connected Report on the proposed ICT roles and ICT jobs classification for the Romanian public administration, report accompanying Output 2 under the TSI project.
18. Sofrankova, B., Sira, E., Horvathova, J., & Mokrisova, M. (2025). Digital Skills and Digital Transformation Performance in the EU-27: A DESI-Based Nonparametric and Panel Data Study. Economies, 13(11), 315. https://doi.org/10.3390/economies13110315.
19. Based on information available at: https://e-estonia.com/, https://ega.ee/

FIGURE 3: Entry points for operationalization into HRM processes



Source: Authors' elaboration

Job analysis thus becomes important for correctly calibrating the applicability of the framework across various roles. Public administrations already rely on job analysis to articulate job purpose, tasks and competency expectations. Embedding digital competencies within this familiar process enables institutions to clarify digital requirements consistently and proportionately, replacing generic formulations ("good computer skills") with structured expectations aligned to the actual digital tasks of each role.

Recruitment should apply the framework in a proportionate and inclusive manner, verifying only a common baseline of digital skills for all candidates. Early implementation contexts are not well-positioned to assess the full breadth of the framework at entry. Instead, a small subset of foundational competencies, typically aligned to DigComp areas 1–5, can be assessed to ensure minimum digital readiness without narrowing recruitment pools or introducing disproportionate burdens on candidates. More advanced digital skills should be developed after entry or assessed through job-specific tools once institutions have the appropriate assessment infrastructure.

Learning and development is therefore the most practical and impactful starting point for operationalization. The framework enables administrations to redesign, update and identify gaps in training catalogues, group digital learning into thematic clusters, and create modular pathways suited to different levels of responsibility. Foundational competencies become universal learning priorities, while more advanced modules support analysts, managers, ICT specialists and digital transformation roles. Piloting confirmed that this differentiated, role-aware approach helps institutions allocate resources effectively and address digital skills gaps without overwhelming staff.

Performance management and career progression should incorporate digital competencies only once learning and assessment systems are in place. Using digital proficiency prematurely in ratings or promotion criteria risks unfairness and may weaken trust in the system. Instead, digital competencies should initially support forward-looking development dialogues, helping managers and staff identify capability gaps and plan learning actions. Only when assessment tools, training pathways and recognition systems are fully operational, and accessible to all staff, should digital evidence inform decisions related to progression or mobility.

A strategic, platform-based training needs assessment (TNA) process is central to this approach. Traditional TNA mechanisms (e.g., paper forms, perception-based reporting, or appraisal-linked checklists) cannot generate reliable, comparable or role-specific insights into digital capability. A digital TNA platform enables hybrid assessment methods (self-assessment, knowledge checks, scenario-based tasks),

automated learning recommendations, and dashboards for institutional and system-level planning. This transforms TNA from an administrative routine into a strategic diagnostic tool that guides investment, supports targeted upskilling and provides evidence for workforce planning. Successful international practice shows that platform-enabled TNA becomes the backbone of continuous digital capability development.

Effective operationalization also requires clear institutional mandates and governance. A sustainable model designates a national training institution to own and operate the TNA platform, a central HR authority to ensure alignment with competency-based HRM, and a digital agency to update skills priorities and oversee specialized ICT roles. Joint governance maintains coherence, ensures stable resource allocation and provides mechanisms for updating expected proficiency levels as technologies and EU regulatory requirements evolve.

Therefore, the sequencing of the digital skills implementation in various HR processes needs to reflect differences in institutional capacity and HRM maturity. The appropriate scope and sequencing of implementation therefore depend on country context. In most administrations, particularly those with lower-maturity HR systems, training and development represent the most accessible and pragmatic entry point for applying the digital competency framework, as these functions are generally in place and allow for early, visible results. For Romania the framework is intended to be implemented for the entire public administration but in a phased manner in line with the recommendations in Output 2. For countries with lower HRM maturity or more limited resources, the framework can be adapted through phased and selective application, including targeting priority groups of civil service jobs (e.g. policy-making or service-delivery roles). Training programs could target relevant clusters of related competencies, allowing administrations to tailor the framework to reform priorities and available capacity.

A phased, iterative implementation model ensures fairness, feasibility and long-term uptake. Pilot testing across diverse institutional types allows administrations to refine tools, calibrate proficiency expectations and simplify user journeys. Local focal points support adoption and act as intermediaries between institutions and central authorities. A monitoring framework tracks participation, equity and progress in priority areas such as cybersecurity, data literacy and AI readiness. Over time, as digital skills improve and HRM systems mature, administrations can expand the use of digital competencies across recruitment, performance and career development, and align national systems with emerging EU-level certification and training initiatives.

Lessons learned

FIGURE 4: Key lessons learned from the Romanian assessment and design process

Lesson 1:
A core set of general digital competencies can be justified as common across EU public administrations

Lesson 2:
DigComp provides the necessary European reference standard, but should be adaptatively tailored for the public administration, using a co-design process

Lesson 3:
DigComp is the foundation, while digital transformation and digital leadership competencies should be seen as system requirements, not optional add-ons

Lesson 4:
Proficiency differentiation is essential to fairness and feasibility

Lesson 5:
AI competency needs to be embedded in digital competency frameworks, but managed as an adaptive layer responding to rapid technological and regulatory change

Lesson 6:
Framework impact depends on HR integration, not only on technical design

Lesson 7:
Learning systems should lead reform sequencing

Lesson 8:
General digital upskilling cannot substitute professional ICT capacity

Lesson 9:
System reform benefits from phased, adaptive governance

Source: Authors' elaboration

The project confirms that a core set of general digital competencies is now a common requirement across EU public administrations. Large-scale job analysis and structured consultations showed that digital tasks have become embedded in virtually all categories of administrative work - policy design, service delivery, case management, inspection, and support services alike. What varies is not whether digital competence is needed, but the level at which particular digital competences are needed to perform tasks in various roles. This finding validates the premise that a single transversal framework can credibly cover the entire civil service, provided it allows for differentiated proficiency expectations across roles and functions, rather than imposing uniform thresholds.

DigComp provides a robust European backbone, however, as it is a generic framework, it must be carefully adapted to public-administration realities through a co-design process. Anchoring the framework in DigComp 3.0 ensures coherence with EU digital-skills policy, mutual recognition efforts, and emerging certification schemes, but the project demonstrated that direct transfer of citizen-centred descriptors is insufficient to describe the full range of public administration digital competences. Also, public administrations operate under a specific institutional logic, compliance obligations, accountability requirements and structured HR systems. These conditions were analysed to determine what competency levels are necessary and sufficient for public administration staff to contribute to organisational digital objectives. This also implied the need for adaptation in language and emphasis. Systematic adaptation - distinguishing between competencies that are only "adapted," more deeply "modified," and those that are entirely "new" - was necessary to reflect institutional data governance, interoperability, regulated workflows, procurement and audit constraints, and AI governance. A structured co-design process with practitioners was essential to translate these standards into administratively usable descriptors that civil servants recognise as relevant to their daily work.

Digital transformation and digital leadership competencies should be treated as system requirements, not optional add-ons. The experience confirms that DigComp-aligned foundational areas (digital literacy, communication, content and services, safety, problem-solving) are necessary but not sufficient for modern public administrations. Dedicated competency areas for digital transformation and digital leadership capture the capabilities required to redesign processes, scale digital initiatives, govern data and AI, and steer organisational change. These are not niche ICT skills; they are core responsibilities for managers and coordinators who must plan, prioritise, and oversee digital projects, rather than delegate all digital accountability to technical teams. Without explicitly defining and developing these competencies, administrations risk building digital infrastructure without the leadership and governance capacity needed to use it responsibly and effectively.

Differentiating proficiency levels is essential for fairness, feasibility, and credible implementation. The decision to adopt a simple three-level proficiency structure was informed by international benchmarking and validated through practical application. In particular, the Spanish digital competency framework for public administration provided a strong reference, demonstrating that a limited number of clearly differentiated proficiency levels can support both assessment and workforce development at scale. This approach was further confirmed during the pilot implementation in Romania's central public administration, where institutions found the three-level structure intuitive, easy to apply, and sufficiently granular to capture meaningful differences in digital capability across roles and functions. A streamlined three-level model (A–B–C) proved both operational and intuitive, but its value lies in how it is applied. In the foundational areas, progression largely reflects growing technical depth and autonomy of use; in the leadership area, it reflects qualitatively different governance responsibilities, from contributing to local improvements to steering system-wide digital change. Lessons from the work show that system-wide baselines can and should be set at a realistic level for recruitment, while higher proficiency levels are best pursued through learning pathways and career development rather than used as rigid entry filters. This protects equity and mobility, avoids unnecessary barriers to recruitment, and ensures that digital capability growth is driven by real job needs.

Framework impact ultimately depends on integration into HRM systems and shared understanding and buy-in on the part of all stakeholders not on technical design alone. The project repeatedly confirmed that even the most sophisticated competency model remains a paper exercise if it is not embedded in HR processes such as job analysis, recruitment, learning and development, performance dialogues, and career progression. Effective integration requires more than a legal act: it needs standardised templates, guidance for HR units and managers, quality-assurance mechanisms, and digital infrastructure to store and use competency data. Where these elements are absent or underdeveloped, the risk is that digital competencies become another "box-ticking" requirement, with limited influence on workforce development or organisational behaviour.

Learning systems, and in particular strategic, platform-enabled TNA, should lead the sequencing of reform. One of the strongest lessons is that digital competencies should first power training and development, supported by a modern TNA platform, before they inform high-stakes HR decisions. A DigComp-coherent digital TNA system can diagnose gaps, map staff to role-appropriate learning pathways, and generate data for institutional and system-level planning. International experience, echoed by this project, shows that frameworks achieve most impact when they are used to structure learning ecosystems (e.g., curricula, catalogues, micro-credentials) rather than when they are immediately tied to appraisal scores or promotion rules. Starting with learning builds trust, improves capability, and creates the conditions under which later integration into recruitment, performance, and progression can be both fair and effective.

General digital upskilling is necessary but cannot substitute for professional ICT capacity. The work clearly distinguished between transversal competencies required across the civil service and the deep specialist expertise needed to design, secure, and maintain complex digital systems. Even at advanced proficiency, general digital competencies cannot replace roles such as enterprise architects, cybersecurity specialists, developers, testers, data scientists, or service designers. The development of a parallel ICT professional roles framework, aligned with e-CF and European Cybersecurity Skills Framework (ECSF), was therefore a necessary complement, ensuring that administrations address both broad workforce readiness and specialist capacity. The key lesson is that digital workforce strategies must couple general upskilling with explicit ICT professionalisation pathways, rather than trying to stretch a general competency framework to cover highly technical functions. For the current public administration workforce this means combining broad digital training with targeted pathways for ICT professionalisation and, where necessary, external recruitment to fill critical gaps, as proved by the pilot process.

Digital competency reform is best approached as a phased, adaptive human-centred system-building process. The experience reinforces that implementation must be tailored to national HRM maturity, digital readiness, and legal traditions. Phased pathways, supported by joint governance arrangements, allow administrations to sequence change: starting with learning and development, piloting in diverse institutional contexts, gradually extending the use of digital competencies across HR processes, and periodically recalibrating proficiency expectations. Successful deployment depends less on the speed of formal adoption and more on sustained governance capacity to refine tools, adjust thresholds, and respond to new EU regulations, technologies and organisational realities over time.

The primary challenge identified through the design process is less about aligning the framework with existing international references, public administration needs, or future-oriented digital skills, and more about conceptualizing and managing the roll-out and implementation effort, which must be carefully calibrated to different roles and administrative contexts. Accordingly, for countries with lower HRM maturity or more limited institutional capacity, the report emphasizes phased and selective implementation pathways, focusing on applying relevant parts of the framework to priority groups or functions (e.g. managers, policy-making roles, or digital transformation–related functions), rather than pursuing an immediate, bureaucracy-wide roll-out. This approach supports pragmatism, ownership, and sustainability while preserving alignment with international good practice.

Opportunities for future integration

The pilot process of the proposed framework in the Romanian public administration demonstrated that the framework is not only conceptually sound but practically deployable in real administrative settings. It validated the structural compatibility with EU reference models while confirming that national adaptation is both feasible and necessary. Building on this success, further piloting in other Member States would be highly relevant to ensure that country-specific contexts - such as institutional mandates, HR systems, and legal frameworks - are properly reflected.

The framework offers concrete opportunities to strengthen alignment with the EU digital-skills ecosystem while preserving national specificity. By design, the general digital competency framework for public administration is structurally compatible with DigComp 3.0 for transversal skills and with e-CF/ECSF for professional ICT roles. This dual anchoring situates the model within the broader European skills architecture underpinning ESCO updates, EU cybersecurity initiatives, and emerging certification schemes. It demonstrates that it is possible to build a public-administration-specific model that is fully interoperable with European reference frameworks, enabling future mutual recognition, shared assessment solutions and participation in EU-level digital academies.

This compatibility creates scope for substantial economies of scale in learning content, assessment tools, and certification. When Member States base their public administration frameworks on shared European taxonomies but adapt them to administrative realities, they can pool investments in curricula, item banks, simulation exercises, micro-credentials and digital leadership programmes. Localisation efforts can then focus on institutional examples, legal nuances and language, rather than on reinventing core competency models. The proposed framework illustrates how national descriptors can remain close enough to EU structures to allow re-use of content and tools across borders, while still reflecting domestic mandates and HRM systems.

For example, as the framework aligns with emerging AI competency models and governance standards, the model provides a foundation for further integrating AI-specific profiles - such as machine learning engineers, AI ethics officers, and data governance specialists - without fragmenting the skills architecture. This compatibility ensures that AI roles can be mapped to existing European taxonomies and that administrations can leverage shared EU resources for AI training, certification, and risk management while tailoring implementation to national contexts.

Shared frameworks also support the emergence of cross-national communities of practice and the development of digital public service profiles (such as the ones needed for interoperability). Common skill vocabularies make it easier for public servants, trainers and HR professionals to compare roles, understand proficiency levels, and participate in joint learning initiatives. For individual administrations, this opens avenues for peer exchange, joint programmes and blended cohorts with other Member States. For the EU as a whole, it contributes to a gradual consolidation of a recognisable digital public service profile, strengthening cooperation on interoperability, data governance and AI implementation.

More broadly, the experience shows that European standardisation and national customisation are not competing objectives but mutually reinforcing ones. By using DigComp, e-CF and related EU instruments as structural backbones while adapting descriptors, examples and implementation pathways to national contexts, Member States can reduce fragmentation, improve the effectiveness of EU-funded training investments, and ensure that digital transformation strategies are matched by coherent, evidence-based investments in public administration human capital. The framework and methodology developed in this project thus offer both a national reference model and a transferable template for translating European digital-skills architectures into concrete, administratively meaningful reforms.

I. Project context and methodological approach

1.1 Why a digital competency framework for the public administration?

1. **Digital transformation has fundamentally altered the nature of administrative work and the expectations placed on governments.** Artificial intelligence, data analytics, platform-based service delivery, automation and cloud infrastructures are no longer peripheral technical instruments but core mechanisms through which services are designed, policies are implemented and public value is created. Citizens now expect public services to be accessible, transparent, personalised and secure. At the same time, administrations must safeguard data, ensure resilient and interoperable systems, and maintain the legitimacy and trust that underpin democratic governance. Digital competence, therefore, has shifted from being a specialist IT attribute to a universal capability required across the civil service.

2. **Public administration employees are increasingly expected not only to use digital tools, but also to understand their implications, contribute to service co-design, manage public data, navigate cybersecurity vulnerabilities, and cooperate across institutional and even national boundaries.** Digital administration is no longer an auxiliary support to government: it is integral to regulatory oversight, service delivery, risk management and policy formation. The ability to interpret digital obligations, apply them responsibly and act in technologically mediated environments has become inseparable from the responsibility to serve the public interest.

3. **The European Union (EU) has reinforced this transition through a strategic and legal architecture that places new expectations on state capacity.** The Digital Decade Policy Programme 2030[20], the European Declaration on Digital Rights and Principles[21], the European Skills Agenda[22] and the Pact for Skills[23] collectively articulate a vision of digitally mature public administrations. Parallel legislative measures on data, artificial intelligence, cybersecurity, digital markets, services, interoperability and accessibility have elevated digital competence from an aspirational reform goal to a compliance-linked requirement. They reshape how public services must be designed and safeguarded, how information must be governed, how risks must be anticipated, and how citizens' rights must be protected in digital environments.

4. **Despite this clarity of direction, no EU-level framework currently defines what digital competence means specifically for public administration employees.** Existing instruments provide partial orientations but do not capture the full administrative mandate. The European Digital Competence Framework (DigComp) for individuals[24], offers a transversal, general framework, which needs to be adapted to capture public administration digital competences, institutional duties and accountability. The European e-Competence Framework (e-CF)[25] outlines the capabilities of ICT professionals, but it is not designed for non-specialist officials who must nonetheless make informed decisions regarding technology, data and digital service delivery. Adaptations undertaken in several Member States demonstrate the relevance of these reference points but also confirm the need for a model tailored to the administrative sphere.

5. **A digital competence framework designed specifically for public administration is therefore relevant and useful, and the framework developed in this study builds on and adapts existing**

20. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030.
21. Joint Declaration of the European Parliament, the Council and the European Commission, European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01
22. European Skills Agenda.
23. European Commission: Pact for Skills.
24. The European Digital Competence Framework (DigComp) for Citizens was developed by the Joint Research Centre (JRC).
25. The European e-Competence Framework (e-CF) classifies 40 competences for the Information and Communication Technology (ICT) professionals. It establishes a common language for competences, skills and proficiency levels across Europe.

frameworks to capture the realities of the work of public administrations. Government operates through defined authority structures, legal mandates and HR systems that require clarity regarding what digital proficiency means at entry, at managerial level and in leadership positions; which competencies differentiate ICT specialists from generalist officials; and how digital capability should evolve alongside career progression, mobility and responsibility. Moreover, public administration carries obligations that are distinct from the private sector and from the popuation at large: safeguarding data in the public interest, ensuring accessibility and interoperability of services, managing algorithmic decision-making transparently, and sustaining trust in state institutions.

6. **International perspectives reinforce this need and also highlight the characteristics such a framework should incorporate.** OECD[26] research points to competencies in collaboration, user-centred design, responsible data use and digital leadership. The World Bank[27] emphasises the importance of combining foundational digital literacy with advanced capabilities in data-driven policymaking, cybersecurity, communication and organisational change. UNESCO[28] adds a focus on digital attitudes such as adaptability, creativity, critical thinking and trust. These perspectives show that successful digital transformation depends not only on technical skills but also on behavioural, strategic and organisational competencies that support the modernisation of public administration.

7. **At the same time, such a framework would need to be anchored in broader lifelong learning policies.** Digital competence should be understood as a lifelong learning capability, rather than as a static attribute acquired at a single point in time or as a generational characteristic. DigComp 3.0 explicitly frames digital competence as a lifelong learning construct.[29] Effective digital transformation therefore depends not only on initial digital competence of new entrants to the public administration, and existing levels of competence of current staff, but on the capacity of public administrations to enable continuous upskilling, reskilling, and learning agility as technologies, legal obligations, and service delivery models evolve. In the EU context, this logic is reflected in the adoption of DigComp framework, which is subsequently translated into sector-specific competency frameworks (for example in education), including for public administration, ensuring coherence between lifelong learning policies and the evolving competency demands placed on the civil service.

1.2 Project objectives

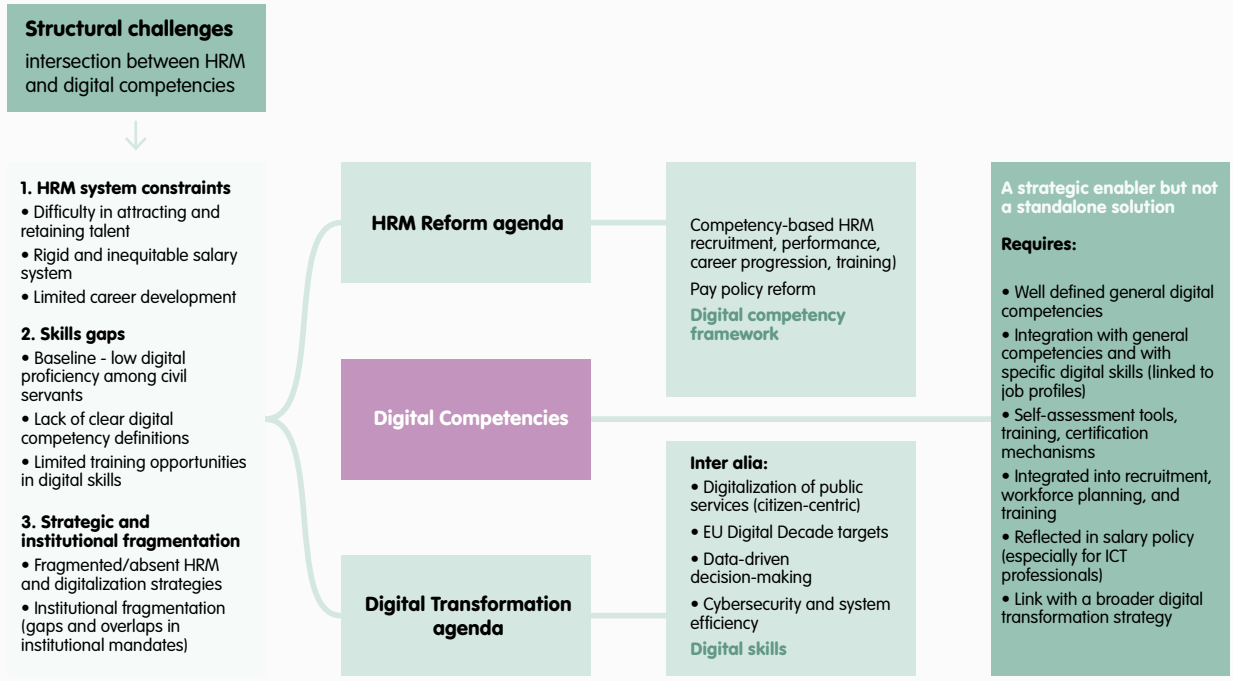
8. **In this context, the World Bank, in partnership with the European Commission, supported the Government of Romania (GoR) to develop a General Digital Competence Framework for Public Administration through the Technical Support Instrument (TSI) *"Romania: Developing a General Digital Competence Framework for Civil Servants"*.** The overarching goal of the TSI project[30] is to strengthen the digital capabilities of Romanian civil servants so that they can contribute more effectively to public service delivery and advance the country's digital transformation. The effort directly supports several national priorities, including improved human resource management, enhanced administrative capacity and alignment with European digitalisation objectives. The beneficiary institutions are the National Agency for Civil Servants (NACS)[31], the Authority for the Digitalization of Romania (ADR)[32],

26. OECD (2021), OECD Working Paper no. 45, The OECD Framework for digital talent and skills in the public sector.
27. World Bank (2024). Digital Progress and Trends Report 2023.
28. UNESCO's Broadband Commission for Sustainable Development (2022), *Artificial Intelligence and Digital Transformation Competencies for Civil Servants*.
29. Cosgrove, J. and Cachia, R., DigComp 3.0: European Digital Competence Framework - Fifth Edition, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121.
30. This project is carried out with funding by the European Union via the Technical Support Instrument (TSI) managed by the European Commission's Reform and Investments Task Force (SG REFORM) and implemented by the World Bank with the support and the partnership of SG REFORM.
31. NACS is the central public institution with the mandate to design and implement the ambitious HRM reforms of the Romanian public administration.
32. ADR's main role is to oversee and drive the digital transformation of the country.

and the National Institute for Administration (INA)[33], the key institutions responsible for HRM policies, digital transformation and public administration training.

9. **The project is grounded in a theory of change that links competency development to stronger public administration performance.**[34] The approach assumes that Romania can build a digitally capable public workforce by: (i) identifying the digital competency needs that matter in the national and broader EU context, (ii) defining general digital competencies in a structured format with clear descriptors and proficiency levels, and (iii) integrating these competencies into core HRM processes such as recruitment, training and career development. Strengthening digital competencies in this way enables Romania to develop a critical component of its digital public administration ecosystem: a workforce equipped to implement digital policies, adopt new tools and deliver modern, citizen-centred services.

FIGURE 5: Context for developing the general digital competency framework: intersection between HRM and digital transformation



Source: Authors' elaboration under Output 1

10. **The work has been firmly anchored in the realities of Romania's public administration, while aiming to produce a model with relevance beyond the national level.** Romania's ongoing HRM reforms, the introduction of a new general competency framework[35] and the varied levels of digital maturity across public institutions shaped the project's analytical approach and design choices. These contextual factors required a framework that is robust yet adaptable, capable of supporting both national needs and alignment with EU trends. Beyond defining competencies, the framework is intended to strengthen the foundations for broader HRM reforms, including capacity-building initiatives, strategic workforce planning and targeted adjustments to recruitment and wage policies that help attract and retain digital talent. As such, the resulting model and methodology offer not only

33. INA is the primary institution responsible for civil service training.
34. World Bank, Output 1- Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service : Taking into Account Relevant Policies at the National and European Union Levels, 2025. Available at: https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745.
35. A general competency framework is in place and serves as the foundation for the national recruitment competition system for civil servants. This framework is gradually being extended to other HR processes and to other categories of personnel beyond the core civil service, aligning with the reform objectives outlined in Romania's National Recovery and Resilience Plan (NRRP).

a national solution but also a potential reference for other Member States seeking to modernise their HRM systems and enhance digital capability across their administrations. As this report and previous deliverables developed under the TSI project document in detail the underlying approach, governance arrangements and co-design methodology, this can enable other Member State actors to understand, use and adapt the work to their own institutional, legal and administrative contexts.

1.3 Project activities

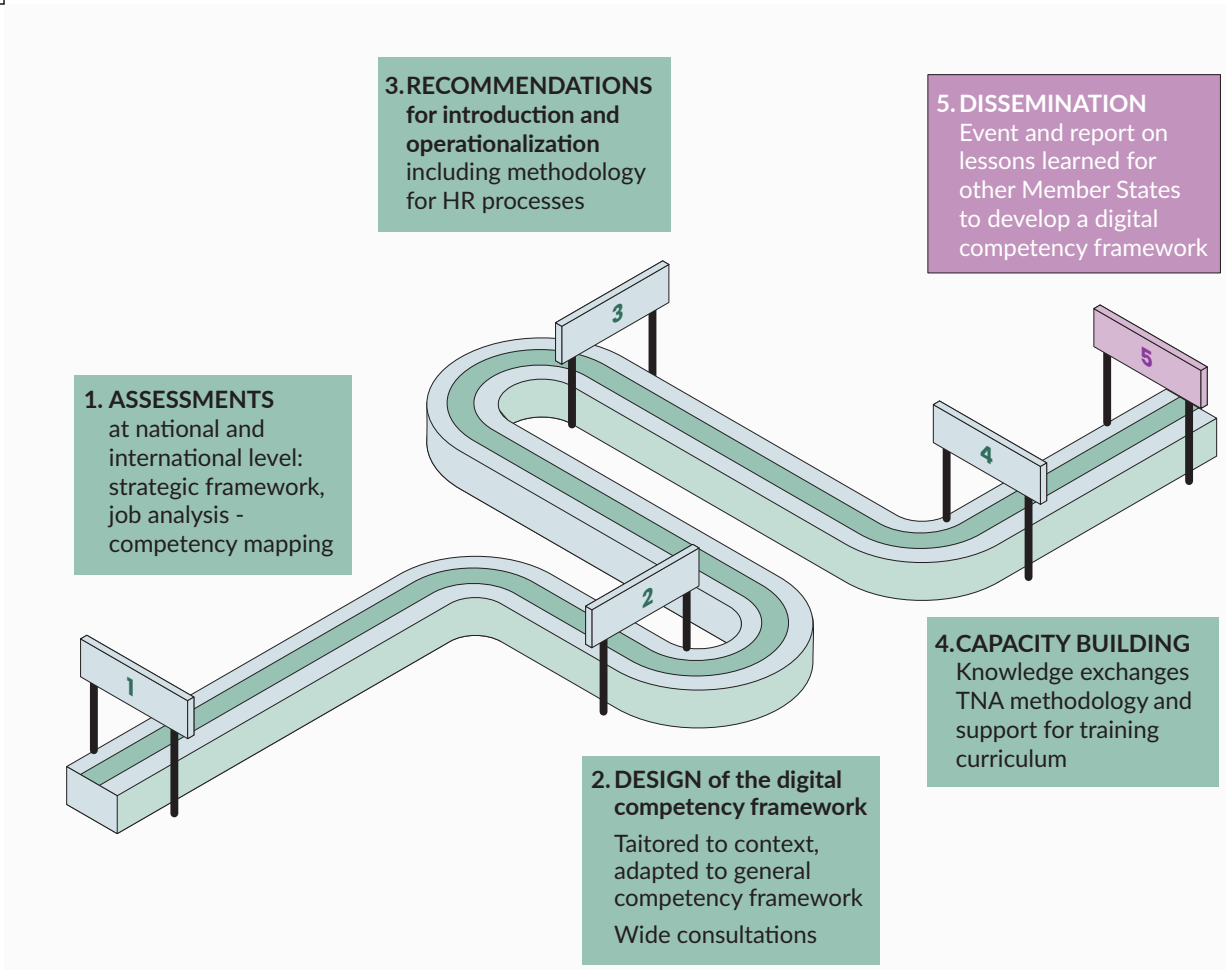
11. **The project was organised around five complementary activities that supported the design, operationalisation and dissemination of Romania's digital competency model.** Activities 1 to 4 covered the analytical groundwork, framework design, integration into HRM processes and capacity-building support. Activity 5, under which this report is produced, focuses on consolidating lessons learned and facilitating knowledge sharing within Romania and across the European Union.

- **Activity 1 Assessment of digital competency needs:** established the analytical foundation through a review of EU and national policies, a job analysis of civil service roles, and foresight exercises to anticipate future skill requirements.
- **Activity 2 Design of the digital competency framework:** defined the structure of digital competency areas, including knowledge, skills, and attitudes,[36] and developed proficiency levels. This phase also included pilot testing and stakeholder consultations to validate and refine the framework.
- **Activity 3 Integration into HRM processes:** focused on developing recommendations and methodologies for embedding the digital competency framework into Romania's HR systems and legal context. This includes identifying operational mechanisms for applying digital competencies in key HR processes such as recruitment, performance management, and training.
- **Activity 4 Capacity building and implementation support:** provided tools and learning opportunities to support the application of the framework, including study visits, updates to training needs assessment methodologies, and the development of curriculum elements.
- **Activity 5 Knowledge sharing and dissemination:** synthesizes lessons learned and facilitates exchange with other EU Member States to inform similar reform efforts. Activity 5 also includes a learning and dissemination event bringing together national stakeholders and EU experts to discuss the Romanian experience and its relevance for the wider European context.

12. **This report constitutes Output 5 under Activity 5 and documents the lessons learned from Romania's experience in developing a General Digital Competence Framework for Civil Servants.** Figure 6 below illustrates Activity 5 in the broader intervention logic of the TSI project. The report summarises the project's key findings, highlights the approaches that proved most effective and identifies the conditions that facilitated progress. It also presents considerations for Member States that may wish to adapt or build similar frameworks, drawing on the evidence, consultations and comparative research undertaken across Activities 1 to 4. While the report reflects the Romanian context, its scope is intentionally broader, offering insights that can inform digital skills strategies for public administrations across the EU.

36. The structuring of competencies around knowledge, skills and attitudes (KSA) is aligned with the DigComp framework, which itself builds on the 2018 Council Recommendation on Key Competences for Lifelong Learning. At the same time, the KSA approach is also applied across a range of international and national competency frameworks reviewed during the project and was retained to ensure coherence and comparability.

FIGURE 6: TSI project intervention logic: Report corresponds to Activity 5

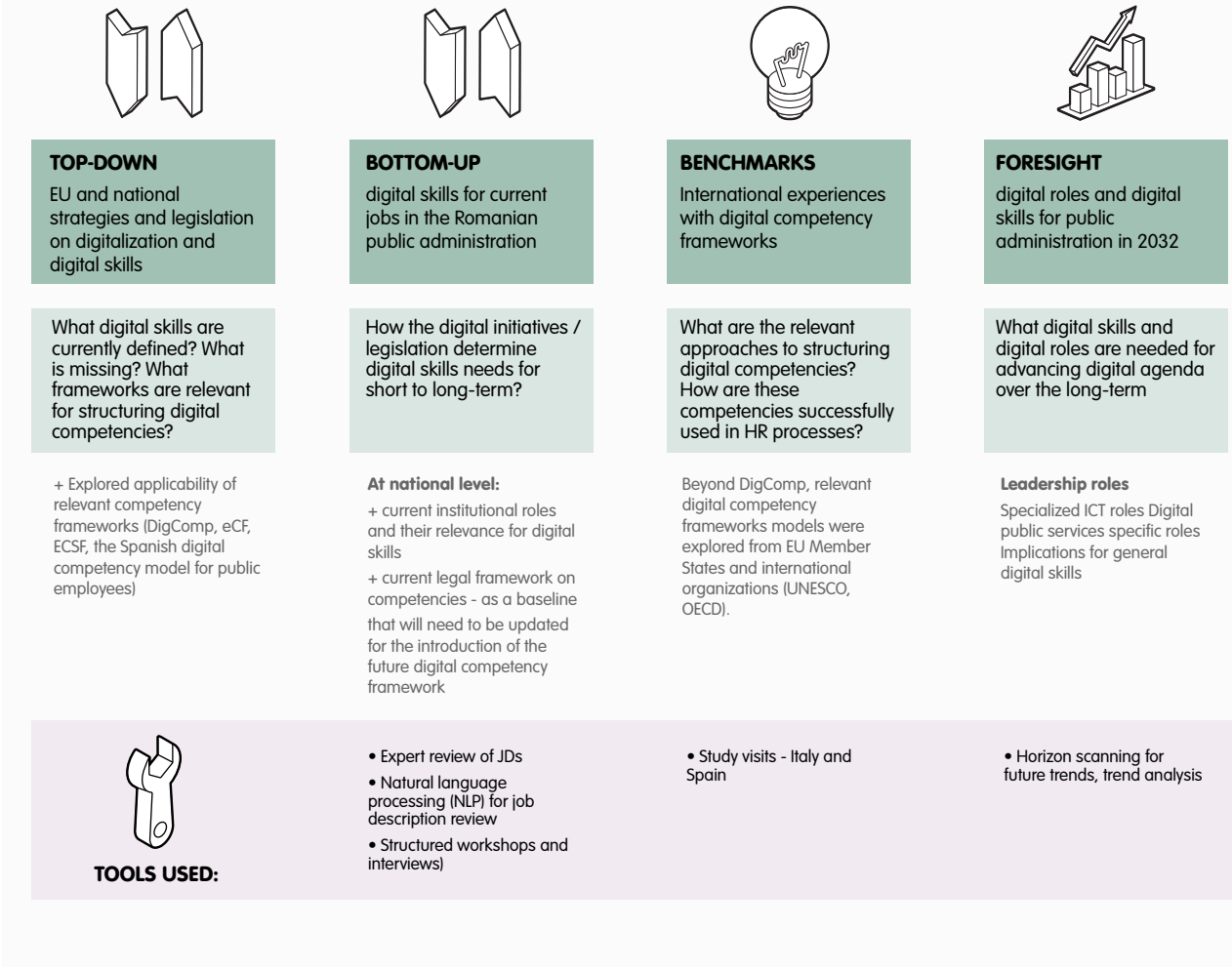


Source: Authors' elaboration under previous project outputs.

1.4 Methodological approach and conceptual link with the European reference models

13. **The development of Romania's Digital Competency Framework for Civil Servants followed a structured, evidence-based process designed to ensure both national relevance and full coherence with European reference models.** The methodology combined four complementary analytical components: a top-down policy and regulatory review, a bottom-up job role analysis, an international benchmarking exercise and a foresight assessment. Each component contributed distinct insights, while collectively ensuring that the resulting framework is coherent, future-oriented and consistent with European standards for digital competence development.

FIGURE 7: Multi-layer analytical approach for the development of the framework



Top-down analysis: grounding the framework in EU and national policy requirements

14. **The first analytical component focused on the policy and regulatory landscape governing digital transformation and human resources development in Romania.** This phase established the strategic foundation for the framework, ensuring that it would align with national commitments and respond to the evolving European regulatory environment.

15. **Despite the extensive policy architecture, the analysis highlighted a fragmented landscape in terms of HRM and capability development.** Romania's HRM legal framework lacks a unified system for defining and operationalising digital competences. The existing general competency framework, established under the Administrative Code, does not yet integrate digital competencies in a structured way across recruitment, training, or performance evaluation. Moreover, institutional mandates related to digital skills are dispersed. The National Agency for Civil Servants oversees HRM modernisation but lacks authority over digital skills policy; the Authority for Digitalization of Romania is responsible for the national digital transformation agenda, yet its strategy remains pending formal adoption; and the National Institute of Administration provides training under resource constraints. The absence of a national digital skills plan for the public administration has left capacity-building efforts reliant on fragmented, project-based initiatives, such as the NRRP-funded training programme for 30,000 civil servants. These initiatives, though valuable, are not yet embedded in a coherent national strategy.

Bottom-up analysis: capturing real institutional needs and job requirements

16. **A second analytical strand addressed institutional realities through a bottom-up assessment of job roles, capturing how digital competencies are reflected in practice across the civil service.** This analysis provided a grounded understanding of the digital skills already required within public institutions and those likely to be needed in the near future. The World Bank team conducted an extensive review of 2,380 job descriptions from 20 central public institutions. These data were complemented with focus groups, interviews, and workshops involving HR specialists, institutional leaders, and technical experts. Advanced Natural Language Processing and AI-assisted techniques were used to extract and cluster references to digital competencies, offering a data-driven profile of current patterns and emerging gaps. Findings were reviewed in collaboration with the HR Working Group, consisting of HR experts from the central public administration.

17. **The results revealed widespread inconsistency in the way digital competencies are described and applied across institutions.** While nearly three-quarters of job descriptions mention basic office tools such as Microsoft Office, references to more advanced competencies like cybersecurity, data analytics, or digital service design were sporadic. A significant proportion, around fifteen percent, contained no reference to digital skills at all. Many of the competencies identified were implicit, linked to tasks involving digital tools but not explicitly recognised in the job documentation. This situation has made it difficult to integrate digital skills systematically into HR processes.

18. **The analysis also exposed structural weaknesses in how ICT roles are managed within the civil service.** Career pathways for technical staff remain poorly defined, salary structures are not competitive, and training investments are inconsistent. These conditions contribute to high turnover among IT specialists, outdated systems, and growing operational risks. Advanced digital skills are rarely associated with structured training, certification, or professional development opportunities. These findings confirmed that Romania's public administration needs a clearer model for defining and developing digital competencies across all job categories.

International Benchmarking

19. **A third analytical component examined international experience, ensuring that the Romanian framework would reflect European and global best practice.** The benchmarking review covered a range of models, including DigComp 2.2, DigComp 3.0 (under development at the time of review), Spain's and Italy's public administration adaptations of DigComp, UNESCO's framework on AI and digital transformation, Apolitical's AI Readiness Check for Civil Servants, the European e-Competence Framework, the European Cybersecurity Skills Framework, and the Skills Framework for the Information Age. The comparative analysis revealed that only a few EU Member States, including Spain, Italy, Denmark, Finland, as well as the United Kingdom, have developed structured frameworks for the public sector. Spain and Italy stand out for their integrated approaches that link frameworks with national training platforms and certification systems. Their models combine a clear competency taxonomy with digital learning environments such as Spain's AgeDigital and BAIT systems or Italy's Syllabus platform, ensuring that digital competence development is directly connected to learning opportunities and recognition mechanisms.

BOX 1: Overview of key country examples analysed under Output 1[34]

Relevant digital competency framework models were analysed during the assessment phase and reflected in Output 1.

Models from six European countries were analysed: Spain, Italy, Latvia, Denmark, Finland and UK. Countries like Italy and Spain have implemented structured digital competency frameworks, covering "traditional" types of foundational digital skills, but also emerging technologies, such as AI. Such frameworks are regularly updated to remain relevant. The UK, on the other hand, focuses only on a framework for specialized IT job profiles, describing the technical skills necessary for digital transformation. Finland and Denmark offer broader strategic approaches, prioritizing organizational transformation and leadership development.

The digital competency models primarily target general digital competencies, with specific initiatives focusing on specialized ICT skills for public administration.

Countries like Italy, Spain (and the Basque Country), and Finland emphasize defining digital skills and competencies needed for policy development roles (ICT-enhanced tasks) in the public administration. Beyond individual competencies, Denmark's model highlights the need for broader capacity of organizations to navigate and lead digital transformation efforts. This model reinforces the knowledge, skills, and attitudes necessary to manage change and lead digital transformation in the public administration. Frameworks like SFIA and the UK's Government Digital and Data Profession Capability Framework provide structured guidance on advanced-level digital skills for IT professionals, defining the competencies required for ICT-intensive tasks in public administration.

Training needs assessment platforms and digital skills certification were identified as essential for the upskilling agenda.

Spain's AgeDigital project and the Basque Country's BAIT certification model provide valuable lessons in assessing and attesting digital skills. These models highlight the importance of a clear certification system to validate digital competencies and support career development. They offer insights into developing self-assessment tools that enable civil servants to evaluate their digital competencies and receive official certification upon completing structured training programs.

Foresight-based alignment with emerging technologies and digital transformation goals.

20. **A foresight exercise complemented this analytical work, ensuring that the Romanian framework would not only address current needs but also anticipate future ones.** The exercise also involved experts from the EC's Joint Research Centre and the Prospectiva Foresight Institute from Romania in mapping emerging roles and skill profiles likely to shape public administration through 2032. The foresight identified three broad categories of roles that illustrate the spectrum of digital engagement in government. ICT-intensive roles, such as cybersecurity analysts, cloud engineers, and AI governance specialists, require advanced technical knowledge. ICT-enhanced roles, including digital transformation officers and smart city managers, combine domain expertise with digital innovation. ICT-dependent roles, such as service designers, user experience specialists, and data analysts, rely on digital proficiency to perform non-technical functions more effectively. The analysis showed that these categories will coexist and expand within the Romanian civil service, demanding a framework that differentiates competencies according to both function and depth. The foresight also underscored the growing importance of strategic roles - Digital Transformation Leaders, for example - that blend policy insight, change management, and technical understanding to steer reform in complex digital environments.

37. World Bank, Output 1- *Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service: Taking Into Account Relevant Policies at the National and European Union Levels (English)*. http://documents.worldbank.org/curated/en/099071725093059745.

FIGURE 8: Foresight exercise: future digital roles for predictive governance (2032)

Specialized IT roles (technical expertise in AI, blockchain, data, and infrastructure	Strategic and policy roles (leading and overseeing governance, compliance, and long-term digital transformation)	Service delivery & citizen-focused roles (bridging digital systems with public needs)
• AI & NLP engineer - develops and optimizes AI-driven virtual assistants and predictive analytics models. • Chief data officer - Manages data governance, interoperability, and AI-driven analytics across public administration. • Cloud & edge computing specialist- manages cloud infrastructure and decentralized computing systems. • Cybersecurity & data protection specialist- ensures the security of digital systems, blockchain networks, and AI- powered services. • IoT & sensor network engineer- develops and maintains IoT-enabled smart infrastructure for predictive governance. • Blockchain architect - designs secure blockchain-based verification systems for public records and procurement. • Geospatial data scientist & GIS analyst- develops digital twins and AI-driven geospatial analytics for urban planning. • Health data system architect- designs and maintains the Romanian health data space (RHDS) and ensures interoperability. • Smart contract developer- builds automated digital contracts for procurement, taxation, and benefits distribution. • Digital identity & security specialist - Develops and secures eID, decentralized digital identity (DID) systems, and authentication mechanisms.	• Digital transformation manager- leads the modernization of government services and infrastructure. • AI policy & strategy lead - develops national AI policies and ensures ethical AI deployment in public services. • Cybersecurity & data governance officer - oversees regulatory compliance, risk management, and GDPR enforcement. • Smart city program manager- guides the implementation of predictive governance and digital infrastructure. • Blockchain policy & compliance officer- ensures blockchain systems align with legal frameworks and data protection regulations. • Public sector digital transformation manager-aligns digital innovation with government priorities and strategic objectives. • Digital twin & GLS policy advisor - provides regulatory oversight for geospatial analytics and smart city planning. • Legal & regulatory expert for digital services - ensures compliance with emerging digital regulations and e-Government frameworks.	• Citizen engagement specialist - ensures digital services are accessible, inclusive, and aligned with public expectations. • Digital inclusion officer - designs and delivers digital literacy programs to bridge the digital divide. • Hybrid services coordinator- manages the integration of digital and in-person service delivery for non-digital users. • Digital ombudsman for citizen advocacy - safeguards citizen rights in digital governance and AI decision-making. • Healthcare provider onboarding specialist-supports medical professionals in integrating digital health systems. • Multilingual & accessibility support expert- ensures digital services are accessible to diverse linguistic and special-needs populations. • Open data & transparency officer- promotes open government initiatives and public data accessibility. • Blockchain public education & outreach specialist-educates citizens and businesses on blockchain applications in public administration. .

Source: Authors' elaboration under Output 1

Expert and stakeholder consultations

21. **The analytical and comparative work was complemented by extensive consultation and co-design with institutional experts and HR practitioners.** An HR Working Group, coordinated jointly with NACS, brought together representatives from over twenty central institutions. The group functioned as both an advisory forum and a validation mechanism, ensuring that the proposed framework reflected real institutional needs. The discussions focused on refining the framework's structure, identifying relevant descriptors, and defining how digital competencies could interact with the existing general competency model. Participants analysed competencies from other European frameworks and debated their applicability to different categories of civil service roles. This exchange helped clarify which competencies are universally relevant and which apply only to specific functional areas or levels of responsibility.

22. **Deliberations within the working group also shaped key design choices.** The framework was conceived as a stand-alone model aligned with, but not subordinate to, the existing general competency framework. Participants agreed that such an approach would maintain conceptual clarity while

allowing institutions flexibility to update competencies as technologies evolve. The discussions also validated the use of a three-level proficiency scale (A, B, and C) reflecting foundational, intermediate, and advanced mastery, which participants found simple, clear, and adaptable to institutional contexts.

23. **The working sessions provided insights that went beyond the technical design of competencies, encompassing practical and process-related considerations for implementation and use.** HR professionals and managers emphasised the need for credible mechanisms of certification and validation to ensure that digital skills are formally recognised within career pathways. They also supported a gradual and realistic approach to implementation, where digital competencies would first guide training and recruitment before extending into performance evaluation and promotion. This perspective reflected both international good practice and the institutional capacities of Romanian administrations. The consultations also underscored the importance of using plain administrative language and relevant examples to make the framework accessible to civil servants with diverse backgrounds.

24. **The consultation process extended beyond public institutions to include universities and private-sector training providers, such as ICDL, ensuring that the framework reflects both academic rigor and market-relevant practices.** These stakeholders contributed insights on curriculum design, certification standards, and emerging digital skill requirements, particularly in areas like cybersecurity and data analytics. Their involvement helped align the framework with existing learning ecosystems and validated its potential for integration into formal education and professional development pathways. This multi-actor approach strengthens the framework's credibility and ensures that implementation strategies can leverage diverse resources across sectors.

Pilot testing and validation

25. **A pilot testing and validation exercise was carried out to ensure that the Framework was feasible for real-world applications.** The pilot aimed to verify how well the framework's descriptors, levels, and associated instruments functioned in practice and to collect feedback that would inform the refinement of the final model. It also tested the usability of the Training Needs Assessment (TNA) tool and validated the typology of ICT roles developed earlier in the process.

26. **The pilot exercise confirmed that the proposed digital competency framework is broadly relevant for the Romanian administrative context and does not require structural redesign.** All seven competency areas were validated, with particularly high current relevance for Digital Literacy and Digital Communication and Collaboration, and rising future importance for Digital Leadership and Governance and Digital Transformation. Core business roles consistently assign higher current and future relevance to digital competencies than support services, reflecting stronger digital-transformation pressures in service delivery. At the same time, support functions anticipate significant growth in Digital Transformation, highlighting the need to modernize internal processes and workflows across HR, finance, and administration.

27. **The pilot also validated the tiered proficiency model, while underscoring the need for flexible application.** Level A (basic) emerged as a universal baseline for all roles, while Level B (intermediate) is widely relevant but should be applied selectively based on concrete job requirements rather than grade alone. Level C (advanced) was confirmed as relevant only for a narrow set of roles. As a result, only limited calibration was required, mainly to refine Level C descriptors in area 7 (Digital Leadership and Governance) toward managerial and oversight tasks, ensuring alignment with actual mandates while preserving ambition for developing digital leadership capacity.

II. A proposed Digital Competence Framework for the public administration

2.1 Framework scope

28. **The *general* digital competency framework developed under the TSI project targets the general civil service and defines the transversal digital competencies required across roles, functions, and organizational levels in the public administration.** This scope is meant to reflect the reality that digital transformation is no longer confined to specialized IT units but depends on the digital capabilities of the entire workforce. The framework therefore focuses on transversal, role-independent competencies that enable public servants to use digital tools, manage and interpret data, collaborate through digital platforms, contribute to digitally enabled service delivery, and operate responsibly and securely in digital environments.

29. **The definition of general digital competencies proposed under this project was developed in direct relation to the framework's scope, targeting transversal competencies applicable across all roles in the general civil service.** It draws on international and EU experience, notably DigComp 2.2 for its comprehensive structure of digital competence domains and proficiency levels; the European e-Competence Framework (e-CF) for its differentiation between general and specialist ICT roles; and public administration-oriented models promoted by the OECD[38], World Bank[39], and UNESCO[40]. These frameworks emphasize progression from basic digital literacy to advanced digital leadership, responsible data use, cybersecurity awareness, collaborative service delivery, and the importance of digital attitudes such as adaptability and openness to learning. These reference frameworks informed both the breadth of competencies covered and the integrated approach combining technical, behavioral, and attitudinal dimensions.

30. **Based on the review of relevant frameworks and the design process conducted in Romania, general digital competencies for public administration are proposed to be defined** as follows:

General digital competence in the public administration is the confident, critical, responsible, and effective use of digital technologies, data, and information systems to deliver, innovate, and improve public services, in ways that are secure, ethical, inclusive, and aligned with national and European digital transformation objectives. It encompasses an integrated set of knowledge, skills, and attitudes required to access, evaluate, create, and manage digital resources; collaborate and communicate effectively in digital environments; ensure data protection, cybersecurity, and ethical AI use; leverage data and digital infrastructures for evidence-based policymaking, citizen engagement, and organizational transformation; and adapt to emerging technologies and evolving societal needs.

2.2 Framework structure

31. The framework is organised around two complementary dimensions. The first distinguishes between three competency types – (i) fundamental digital skills expected of all civil servants, (ii) specialized, non-IT skills linked to digital transformation, and (iii) managerial competencies needed for leadership and strategic oversight - reflecting the different ways civil servants engage with digital technologies.

38. OECD, The OECD Framework for digital talent and skills in the public sector, 2021.
39. In the context of the GovTech Maturity Index, digital competencies are discussed in relation with the broader enabling environment that supports digital government maturity – for details please see World Bank, GovTech Maturity Index - Trends in Public Sector Digital Transformation Report, 2022.
World Bank, *Digital Progress and Trends Report*, 2023. The report emphasizes the central role of digital public infrastructure (DPI), such as identity platforms, data sharing architectures, and digital services, in enabling equitable digital development. While this report does not strictly define competencies, it underscores the need for public institutions to have the capabilities to build, manage, and utilize DPI effectively, including navigating advances in areas like AI and cloud computing.
40. Definition summarized by authors based on the detailed framework from UNESCO, *Artificial intelligence and digital transformation: competencies for civil servants*, 2022.

The second is a thematic dimension based on which competencies are grouped into competency areas.

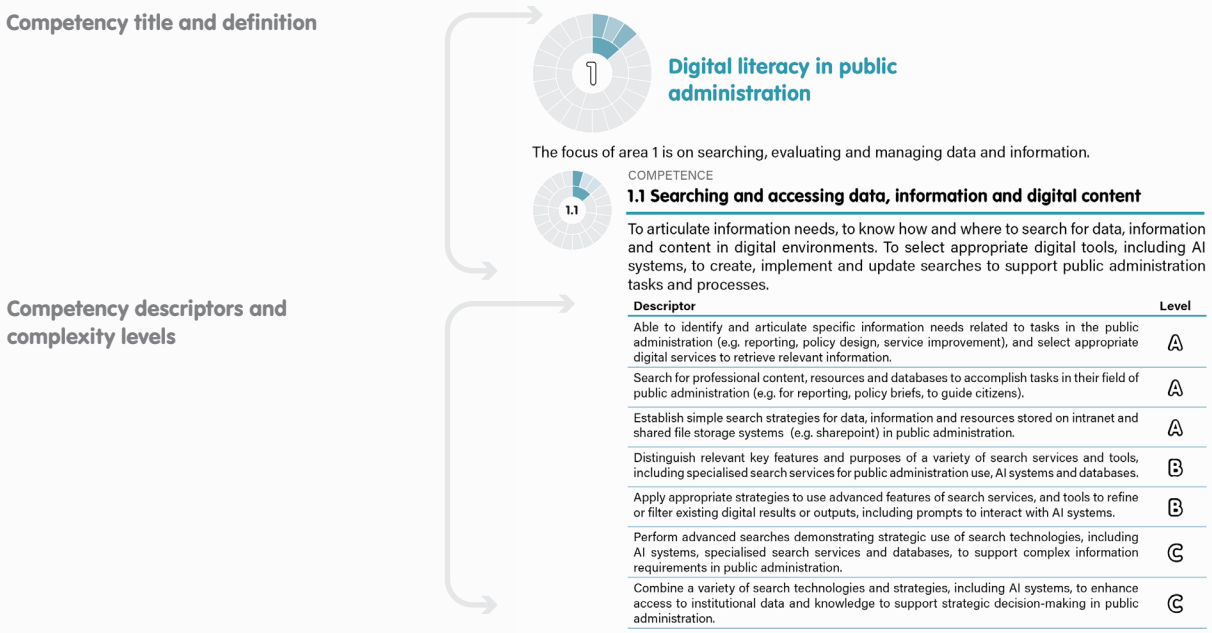
32. Seven competency areas are proposed with a total number of 22 digital competencies. Each is described across three proficiency levels (A - basic, B- intermediate, C- advanced). Each competency includes descriptors covering knowledge, skills and attitudes, enabling self-assessment, structured evaluation and the development of targeted training.

Competency types

33. In terms of competency types, three types of digital competencies are defined based on their thematic focus and scope:

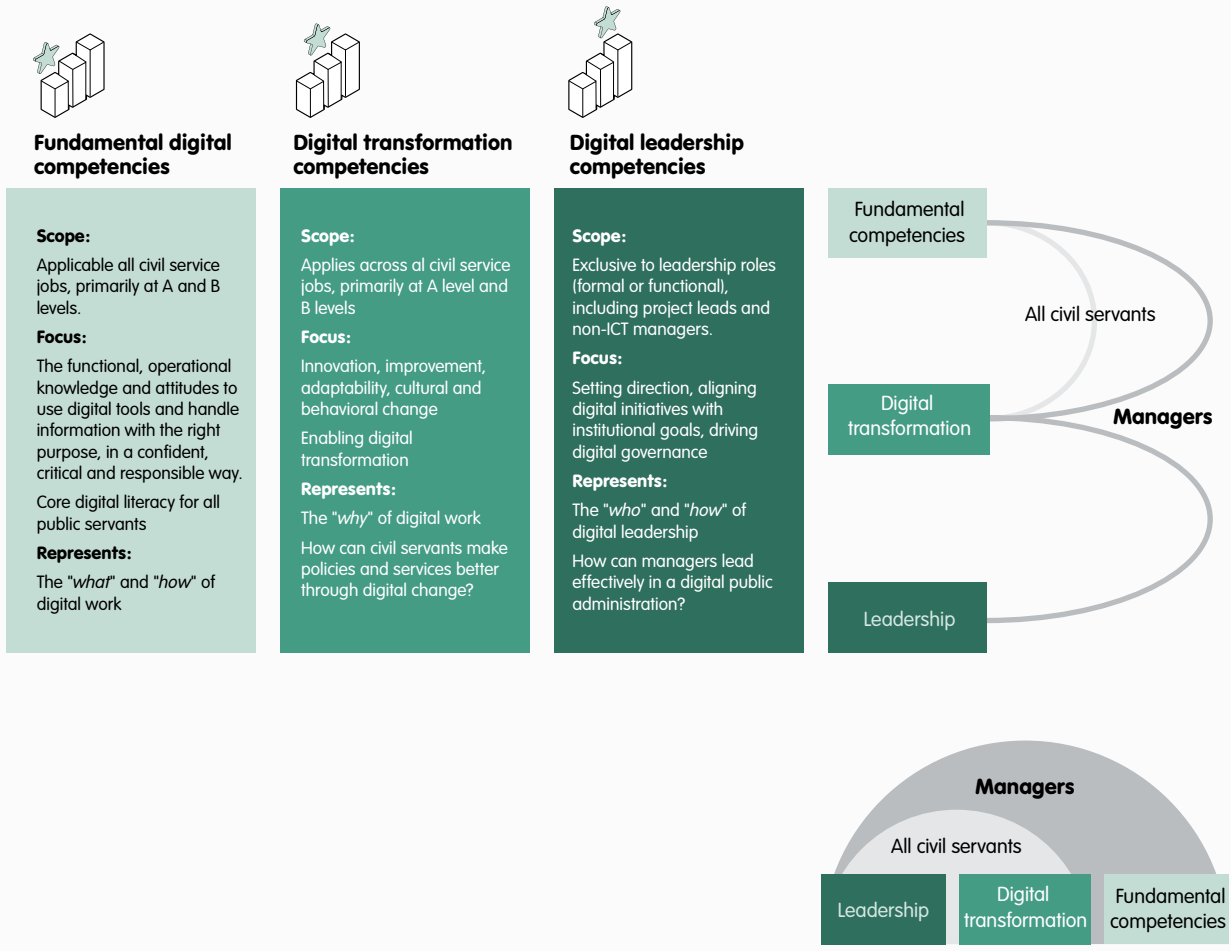
- *Fundamental competencies:* essential digital skills expected of all civil servants, enabling them to operate effectively in a digitally enabled environment.
- *Digital transformation-related competencies:* specialized, yet non-IT competencies, that support the design, implementation, or facilitation of digital transformation processes within institutions.
- *Managerial digital competencies:* competencies specific to civil servants in leadership or supervisory roles, focusing on the strategic and organizational aspects of digital transformation.

FIGURE 9: Framework elements: competency types, areas, competencies (with titles and definitions), descriptors grouped by 3 complexity levels



Source: Authors' elaboration

FIGURE 10: Various roles require different competencies



Source: Authors' elaboration under Output 2

34. **The modular proposed structure mirrors international best practice, including the following elements:**

- **Competency areas:** broad clusters that group related competencies under a common thematic dimension.
- **Competencies:** defined within each area, each with a title and a clear definition describing the core capability and its scope.
- **Proficiency levels:** each competency is described across three progressive levels:
  - *Level A, Basic:* expected of all users; covers foundational knowledge, skills and attitudes enabling a routine use of digital tools.
  - *Level B, Intermediate:* reflects more autonomous use, adaptation to different contexts, and the ability to support to others.
  - *Level C, Advanced:* involves strategic use, innovation, or oversight in digital domains.

35. **The framework applies a differentiated proficiency-level logic, with A–B–C levels reflecting task complexity and autonomy for general digital competencies in areas 1-6 that apply to both execution level jobs and managerial jobs, and managerial responsibility for digital leadership and governance under area 7.** For competency areas 1 to 6, which represent general digital competencies applicable to all civil service jobs (execution and managerial), the A – B – C levels reflect progressive complexity of tasks, autonomy and cognitive domain characteristics in knowledge, skills, and attitudes. The proposed approach implies that each digital competency is defined once, while its three proficiency levels are illustrated through a set of descriptors. In this way, the A-B-C levels operate inside each digital competency, clarifying how the same competency evolves in depth and complexity. In competency area 7, which addresses digital leadership and governance, proficiency levels A – B – C reflect increasing levels of managerial responsibility rather than purely technical progression. The levels are aligned with typical public-administration management tiers and can be mapped to national administrative structures. For Romania, the recommended A - B - C levels in area 7 were structured as follows: **Level A** corresponds to first-line managerial and coordination roles (e.g. heads of units, team leaders, and project managers), **Level B** corresponds to middle-management roles with organisational oversight (e.g. directors, deputy directors, or equivalent positions responsible for multiple units or programmes), while **Level C** corresponds to senior executive leadership roles with system-level responsibility (e.g. secretaries-general, permanent secretaries, or equivalent positions responsible for institutional strategy, governance and cross-government coordination).

36. **While DigComp defines four proficiency levels (Basic, Intermediate, Advanced and Highly Advanced) mapped on a scale from 1 to 8, with levels 7 and 8 corresponding to Highly Advanced proficiency, the proposed general digital competency framework for public administration corresponds to DigComp levels up to Advanced, with a maximum alignment at level 6 on the DigComp scale.** Thus, the proficiency levels are calibrated to what is necessary and sufficient for effective performance in public administration roles, based on the analytical review conducted under Output 1 of the TSI project. Civil servants may nonetheless pursue further self-directed learning or voluntary DigComp-aligned certification for the DigComp highly advanced level. Annex 1 includes a table presenting the correspondence between the proficiency levels in the proposed framework and the levels from DigComp.

37. **Each competency is further detailed through descriptors that reflect the required knowledge, skills, and attitudes** at each level of proficiency, supporting both self-assessment and structured **evaluation**, and creation of training content.

2.3 Framework's anchoring in DigComp

38. **The framework was designed to conceptually follow DigComp 2.2 and was subsequently updated to reflect the newly adopted DigComp 3.0, ensuring consistency with the most current EU reference model for digital competencies.** The 3.0 update captures rapid technological change since 2022, most notably the transversal integration of artificial intelligence and the introduction of more granular learning outcomes. Keeping pace with DigComp 3.0 also ensures coherence with key EU policy initiatives, including the Digital Decade Policy Programme[41] and the Union of Skills agenda, providing a future-ready foundation responsive to emerging competency needs in public administration.

39. **The design of the underlying conceptual model closely follows DigComp's areas to ensure traceability, future adaptability, and coherence with digital learning programs used across the EU, while being specifically tailored to the needs of Romania's public administration.** The conceptual model is deliberately designed with a sufficient level of detail to ensure clarity across the digital competency areas that constitute general digital competencies, while remaining proportionate and aligned with international practice. The conceptual model comprises 22 competencies in 7 areas which are adapted to the specific needs of public administration. More specifically, Areas 1–5 build on DigComp areas however adapting and extending them to reflect civil service tasks and compliance requirements, including the use of institutional data and information systems, interoperability, and responsible AI. Beyond these general digital competencies, international experience (OECD, UNESCO, World Bank, and public administration digital skills frameworks such as the ones from Spain and Italy) underlines the need for competencies related to digital transformation and leadership, which are addressed in Areas 6 and 7. Together, these components ensure that civil servants are equipped not only as digital users, but also as drivers of institutional change, providing a public administration-specific competency reference aligned with national and European reform objectives.

40. **As detailed in Table 2, the proposed model retains continuity with DigComp while adapting it to public administration realities:** 7 competencies were adapted to reflect civil service tasks and compliance environments; 5 were modified through restructuring or re-clustering to better suit institutional and service-delivery contexts; and 3 were considerably revised to incorporate expanded governance or interoperability responsibilities. In addition, 7 competencies are new, developed specifically to address public administration requirements not covered by DigComp – including leadership, governance, and digital transformation competencies. This structured adaptation ensures both EU coherence and strong sector relevance, positioning the framework as a tailored yet interoperable tool for public-administration digital capacity building.

41. https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme.

TABLE 2: Adaptation of DigComp competencies and new competencies added across the 7 areas

	The proposed digital competency framework for the public administration	DigComp 2.2/3.0	Level of modification
1.1	Searching and accessing data, information and digital content	1.1	Adapted to PA
1.2	Evaluating data, information and digital content	1.2	Adapted to PA
1.3	Managing data, information and digital content	1.3	Adapted to PA
2.1	Communicating, interacting and fostering citizen and business participation through digital technologies	2.1; 2.5	Modified for PA
2.2	Sharing and collaborating in digital teams in intra- and inter-institutional contexts	2.2; 2.4	Modified for PA
2.3	Ensuring digital integrity and accountability in public administration	2.3	Modified for PA
3.1	Developing, integrating and re-using digital content	3.1; 3.2	Adapted to PA
3.2	Delivering and contributing to digital public services	Not available	Totally new
3.3	Ensuring compliance with legal and regulatory frameworks and standards in digital environments	3.3	Heavily modified
4.1	Protecting devices and infrastructures	4.1	Adapted to PA
4.2	Managing digital identities, and protecting personal data and privacy	4.2; 2.6	Modified for PA
4.3	Supporting healthy and sustainable digital practices	4.3; 4.4	Modified for PA
5.1	Managing digital devices, including identifying and solving technical problems	5.1	Adapted to PA
5.2	Using automation tools in digital environments	3.4	Heavily modified
6.1	Contributing to digital transformation in public administration, driving innovation and improvement	5.2; 5.3	Heavily modified
6.2	Developing digital competence in the workplace	5.4	Adapted to PA
6.3	AI Literacy in public administration	Not available	Totally new
7.1	Managing performance and operations through digital technologies	Not available	Totally new
7.2	Leading team development in digital environments	Not available	Totally new
7.3	Driving and leading innovation and digital transformation	Not available	Totally new
7.4	Strengthening public services and ensuring responsible digital governance and cybersecurity	Not available	Totally new
7.5	Anticipatory and strategic thinking supporting public administration	Not available	Totally new

41. **In Table 2 above, when describing how the competences relate to DigComp and their specific tailoring to public administration, four levels of modification are distinguished.** For example, in Table 2, the rightmost column shows "Adapted to the public administration" this refers to competencies that exist in DigComp and retain their core definition, but whose wording and descriptors were tailored to reflect the specific tasks, institutional systems, and compliance obligations of the civil service. "Modified for the public administration" describes competencies derived from one or more DigComp elements that were restructured, combined, or refocused to better match public administration service delivery

contexts, resulting in recognizable links to DigComp but with altered scope or emphasis. "Heavily modified" denotes competencies that have DigComp counterparts but were substantially expanded or reframed to capture new public administration requirements such as interoperability, regulatory accountability, or governance responsibilities. Finally, "Totally new" identifies competencies with no equivalent in DigComp, developed specifically to address distinct needs of public administration, most notably in areas such as digital leadership and institutional transformation.

2.4 Framework content

42. **This section presents the reference/core version of the general digital competency framework developed under the Romania TSI project[42].** The structure retains the same thematic areas and competencies as the original framework, preserving full alignment with its conceptual model. For the purpose of international transferability, the reference version focuses on the generic competency architecture – competency areas, definitions, descriptors, and proficiency levels – while omitting country-specific features, such as the detailed mapping of competencies to Romanian civil service job categories and direct references to national HR systems and platforms (included in the national implementation model). This approach ensures that the framework content can be readily understood and reused by other EU Member States as a common competency blueprint, while still allowing for national customization through job mapping and linkage to domestic HR and training systems.

43. **The development of the nearly 200 competency descriptors was carried out in parallel with an extensive review of authoritative international sources to ensure methodological robustness and alignment with emerging digital-government standards.** By comparison, the digital competency framework from Latvia has 29 competencies and over 450 descriptors, while the framework from Spain has 17 competencies and over 250 descriptors. Although designed for Romania's administrative context, approximately one-third of the total number of 198 descriptors were directly inspired by established digital-competence and AI-governance frameworks for the public sector, including models and guidance from Australia[43], Ireland[44], Latvia[45], Spain[46], UNESCO/ITU[47], the JRC Policymaking Competence Framework[48], Apolitical's AI Readiness Check[49], and the European Commission's AI literacy materials under the AI Act[50]. These descriptors are concentrated primarily in the areas of Digital Literacy, Safe and Responsible Use of Digital Technologies, Digital Transformation, and Digital Leadership and Governance. The recently updated DigComp 3.0[51] allowed the integration of the most recent conceptual advancements in areas such as AI, data use, and digital safety.

44. **The proposed set of descriptors clarify how the three proficiency levels operate for each competency; in that sense, they are not framed as learning outcomes.** An initial set of potential learning outcomes was proposed for Romania in *Output 4* developed under the TSI project, but they were not tested and might require further calibration. The descriptors proposed below reflect the reality of public administration digital tasks as identified based on the analysis conducted in Romania and based on benchmarking with other international frameworks. As such, the proposed wording

42. This general reference version is called "distilled" version under the TSI agreement.
43. Australian Digital Capability Framework, 2022.
44. Guidelines for the Responsible Use of Artificial Intelligence in the Public Service by Department of Public Expenditure, NDP Delivery and Reform, Ireland, 2025
45. Public Administration digital skills and competences framework, Latvia, 2024
46. INAP, "Marco de Competencias Digitales", Spain, 2023.
47. UNESCO, Broadband Commission ITU, "Artificial intelligence and digital transformation: competencies for civil servants", 2022.
48. Schwendinger, F., Topp, L., Kovacs, V. Competences for Policymaking — Competence Frameworks for Policymakers and Researchers working on Public Policy, EUR 31115 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-53454-9, doi:10.2760/642121, JRC129623.
49. Apolitical, AI Readiness Check.
50. European Commission, AI Literacy - Questions & Answers, Definitions of article 4 and the AI Act, 2025
51. Cosgrove, J. and Cachia, R., DigComp 3.0: European Digital Competence Framework - Fifth Edition, Publications Office of the European Union, Luxembourg, 2025, JRC144121

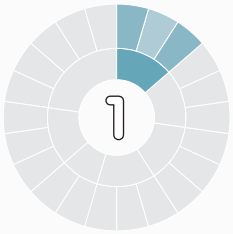
of each descriptor was refined through piloting in the Romanian context and could be potentially adapted to other public administration systems. Based on this, the current report underlines that the framework serves as a reference model, which can operate as proposed while acknowledging its scope for potential national adaptation, refinement, or further unpacking based on context-specific priorities. Also, another critical consideration is the translation of generic English descriptors into the specific language and context of implementation. Precise wording is essential and special focus needs to be placed on selecting terms and action verbs that suit the local linguistic context. Furthermore, as DigComp 3.0 is currently being translated in many local contexts, providers should determine whether to maintain strict terminology alignment or adapt the language to better fit local needs. Considering all these aspects, the proposed descriptors could be further reviewed based on consultations within the Expert Group on Public Administration and Governance - Reform Support as well as Network of Directors of Institutes and Schools of Public Administration (DISPA) - European Commission.

45. **Therefore, while the proposed conceptual framework outlines the key areas of digital competency in public administration, including the 22 competences and their descriptors, its operationalisation as an assessment instrument requires additional steps**, such as developing a valid and reliable item bank of high psychometric quality. A step-by-step illustration of the operational phases and related guiding criteria is provided within the DigCompSAT publication[52].

46. **The reference model of general digital competencies fully retains all areas, competencies and descriptors developed under Output 2.** The only change is that Romania-specific references were removed to ensure a clean, transferable version of the framework. Elements such as ROeID, Ghiseul.ro, national digital strategies or other country-specific systems were taken out, while the substance of each competency and descriptor remains unchanged. This allows the model to be used also as a neutral reference for other countries, for comparison or future adaptation.

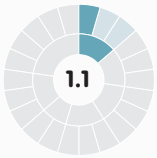
Note: To enhance transparency and usability, all descriptor sources, along with information on proficiency levels, descriptor types (knowledge, skill, attitude), and thematic tags such as AI relevance, are documented in a dedicated **accompanying spreadsheet**. This resource is intended to support training providers, curriculum developers, and institutional HR units by offering a structured and easily navigable evidence base for designing learning pathways and upskilling programmes aligned with the framework.

52. Clifford, I., Kluzer, S., Troia, S., Jakobsone, M. and Zandbergs, U., DigCompSat, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-27592-3, doi:10.2760/77437, JRC123226.



Digital literacy in public administration

The focus of area 1 is on searching, evaluating and managing data and information.

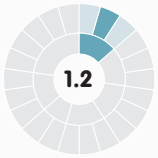


COMPETENCE

1.1 Searching and accessing data, information and digital content

To articulate information needs, to know how and where to search for data, information and content in digital environments. To select appropriate digital tools, including AI systems, to create, implement and update searches to support public administration tasks and processes.

Descriptor	Level
1.1.1 Able to identify and articulate specific information needs related to tasks in the public administration (e.g. reporting, policy design, service improvement) and select appropriate digital services to retrieve relevant information.	A
1.1.2 Search for professional content, resources and databases to accomplish tasks in their field of public administration (e.g. for reporting, policy briefs, to guide citizens).	A
1.1.3 Establish simple search strategies for data, information and resources stored on intranet and shared file storage systems (e.g. sharepoint) in public administration.	A
1.1.4 Distinguish relevant key features and purposes of a variety of search services and tools, including specialised search services for public administration use, AI systems and databases.	B
1.1.5 Apply appropriate strategies to use advanced features of search services, and tools to refine or filter existing digital results or outputs, including prompts to interact with AI systems.	B
1.1.6 Perform advanced searches demonstrating strategic use of search technologies, including AI systems, specialised search services and databases, to support complex information requirements in public administration.	C
1.1.7 Combine a variety of search technologies and strategies, including AI systems, to enhance access to institutional data and knowledge to support strategic decision-making in public administration.	C

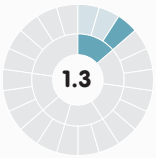


COMPETENCE

1.2 Evaluating data, information and digital content

To assess and compare the credibility and reliability of sources of data, information and digital content in digital environments. To interpret and critically evaluate them to support evidence-based decision-making in public administration.

Descriptor	Level
1.2.1 Understand that not all information and their sources in digital environments are reliable, and that some information is designed to influence (beliefs, values, citizen behaviour).	A
1.2.2 Make accurate distinctions between reliable sources of evidence for policy purposes (e.g. scientific evidence, research outputs) and other types of knowledge and information.	A
1.2.3 Know how to assess public data and their sources (e.g. Eurostat, OECD) for tasks in public administration, e.g. analysis and comparison, support decision-making processes.	A
1.2.4 Critically assess, compare and validate digital data, content and information, and their sources, based on credibility, reliability, completeness and appropriateness for public sector use.	B
1.2.5 Value the credibility and reliability of data in decision-making and policymaking, and the opportunities of using data in government.	B
1.2.6 Understand the concept of 'data-driven public administration', e.g. an awareness of the value and potential of data for supporting decision -making, process design, product and service development and solution delivery.	B
1.2.7 Use indicators to monitor activities and policies in public administration, e.g. for digital policy implementation, performance measures.	B
1.2.8 Thoroughly assess and compare a variety of data, data visualisations and content on a given topic or problem to make accurate inferences to support policy development in a given field of public administration.	C
1.2.9 Evaluate and audit strategies to analyse and interpret data to support policy development in a given field of public administration.	C



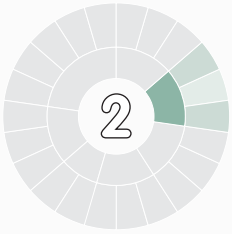
COMPETENCE

1.3 Managing data, information and digital content

To organise, store and retrieve data, information and digital content in digital environments. To collect, process and analyse them in structured digital environments to support public administration tasks and processes.

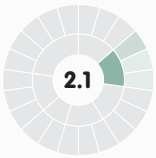
Descriptor	Level
1.3.1 Know that data and digital content can be stored in various locations, e.g. local devices, corporate network, in the cloud, and use the most appropriate one in each circumstance.	A
1.3.2 Know basic data management tools and platforms commonly used in public administration (e.g. document management systems, collaborative platforms, institutional databases, cloud).	A
1.3.3 Organise and format simple data within spreadsheets to support simple information processing and management tasks.	A
1.3.4 Organise, store and retrieve data, information and content in digital tools employed in public administration (e.g. document management systems, cloud, collaborative platforms, institutional databases).	B
1.3.5 Apply a range of data analysis techniques, including spreadsheets (e.g. using formulae, functions, macros) and AI-driven analytics, to support policy development in public administration.	B

Descriptor	Level
1.3.6 Value the importance of clearly and transparently structuring, documenting and explaining datasets for the benefit of others.	B
1.3.7 Use data cleaning and validation techniques to ensure that data and information used for documentation, reporting or decision-making is accurate and usable.	B
1.3.8 Acknowledge that data is an integral asset in public administration to support digital service delivery, organisational management and innovation.	C
1.3.9 Use big data techniques (such as data mining, simulation, AI) for data processing and analysis in public administration tasks.	C
1.3.10 Contribute to improvements of institutional standards, classification systems, electronic archiving rules and metadata to ensure easy access, traceability and management.	C



Digital communication and collaboration

The focus of area 2 is on communication and interaction with citizens and businesses through digital technologies, sharing and collaboration while ensuring integrity and accountability of public administration tasks and workflows, including when AI is used.



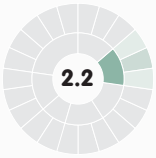
COMPETENCE

2.1 Communicating, interacting and fostering citizen and business participation through digital technologies

To communicate and interact with citizens and businesses through appropriate digital technologies to foster their engagement and trust in public administration. To adapt communication to specific contexts, and to ensure simplicity and clarity.

Descriptor	Level
2.1.1 Use appropriate digital tools (e.g. email systems, collaborative platforms, internal messaging tools) to compose, send, and manage professional communications in digital environments.	A
2.1.2 Interact through inclusive digital channels to ensure meaningful participation from diverse groups, including those with limited digital skills or access.	A
2.1.3 Use different communication styles and linguistic registers in interactions through digital technologies, depending on the tool used, and understand the need to ensure simplicity and clarity.	A
2.1.4 Understand the influence of digital and social media on public perception and participation and apply this understanding in public communication strategies.	A
2.1.5 Carefully choose the most appropriate digital communication tools to interact with citizens, and public and private organisations, depending on the legal nature, complexity and degree of formality of the content.	B
2.1.6 Able to develop and deliver digital content and presentations tailored to specific audiences and administrative purposes, using appropriate visual and technical formats.	B
2.1.7 Promote and value inclusive civic participation in digital environments by citizens, and public and private organisations, e.g. digital citizenship topics to exchange on social and political issues, use of open public data by 3rd parties.	B
2.1.8 Recognise that citizens use digital tools to engage with public administration to express and enact their digital citizenship, and to participate in society through digital technologies.	B

Descriptor	Level
2.1.9 Contribute to the development of digital environments for community empowerment and civic participation to enhance trust in public institutions, and satisfaction with services.	C
2.1.10 Assess and audit the suitability of various digital interaction tools used in public administration for specific communication and interaction goals, taking into account advanced features, complex task requirements and context.	C

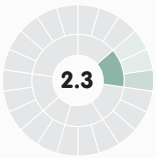


COMPETENCE

2.2 Sharing and collaborating in digital teams in intra- and inter-institutional contexts

To share data, information and digital content responsibly with others through appropriate digital technologies, interoperability standards and open data initiatives. To use digital technologies for collaborative processes to support public administration tasks and workflows.

Descriptor	Level
2.2.1 Know basic collaborative digital tools to share and work in digital teams, e.g. shared calendars, scheduling platforms, shared documents, project boards and task-tracking systems.	A
2.2.2 Use collaborative digital tools to coordinate activities, e.g. project boards, scheduling platforms, digital calendar, time reporting.	A
2.2.3 Use collaborative digital tools to co-develop materials and monitor progress within a team, e.g. shared documents, project boards, scheduling platforms.	A
2.2.4 Work with institutional tools and platforms (e.g. case management systems, interagency portals, shared databases) that support interinstitutional coordination, joint service delivery or multi-institutional workflows.	B
2.2.5 Use digital systems and protocols to securely exchange information and documents with other public institutions or external stakeholders, in compliance with interoperability and governance standards.	B
2.2.6 Manage roles and permissions in collaborative digital environments and workflow tools, e.g. authorising access to files or workflows, to share and edit files both synchronously and asynchronously.	B
2.2.7 Value open data standards to ensure the accessibility of governmental data to promote trust based on the reliability of data.	B
2.2.8 Promote the importance of documenting basic workflows in digital formats to support institutional knowledge.	B
2.2.9 Aware of various mechanisms to facilitate the reuse of an organisation's data within and across public administrations (interoperability standards, open data initiatives).	C
2.2.10 Can explain the benefits of interoperability of information systems in public administration and institutions to enhance the reuse of administrative data.	C

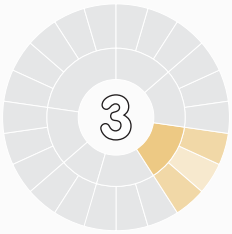


COMPETENCE

2.3 Ensuring digital integrity and accountability in public administration

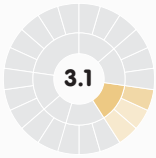
To promote ethical digital practices and good governance principles in all digital interactions and services towards citizens while respecting their rights and choices. To apply measures to take accountability for public administration tasks, including where AI is used, ensuring trustworthy and traceable processes and outputs that do not violate guidelines or policies.

Descriptor	Level
2.3.1 Apply digital etiquette and behavioural norms in interactions in digital environments ensuring respectful, inclusive and purpose-oriented interaction.	A
2.3.2 Value ethical principles when using digital technologies in professional contexts, ensuring fairness, non-discrimination, transparency and accountability.	A
2.3.3 Promote ethical digital practices by adhering to good governance principles and the code of conduct of public administration in all digital interactions and services towards citizens.	B
2.3.4 Maintain a professional digital reputation by responsibly managing one's digital footprint in work-related platforms and networks.	B
2.3.5 Apply measures to take accountability for public administration tasks where AI is used, e.g. checking that outputs are factual, non-harmful or do not violate guidelines or policies.	B
2.3.6 Acknowledge that responsible and ethical use of AI in public administration is guided by human-centric principles of fairness, accountability, transparency, safety, and ethical issues such as privacy, diversity, freedom from bias, information integrity and environmental sustainability.	B
2.3.7 Identify and mitigate risks related to digital misinformation and disinformation, including the specific risks associated with AI deployment, such as algorithmic bias and lack of transparency (like a 'black box').	C
2.3.8 Recognise the importance of considering transparency and accountability of AI systems in public administration and continuously scrutinise how AI systems might shape the interpretation of data and information.	C



Digital content and digital public services

The focus of area 3 is on creating and reusing digital content, contributing to inclusive and people-centred digital public services, while ensuring compliance with legal and regulatory frameworks in digital environments.



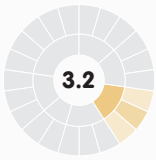
COMPETENCE

3.1 Developing, integrating and re-using digital content

To create and refine a variety of digital content while adhering to institutional requirements, ensuring reusability and digital accessibility across public administration.

Descriptor	Level
3.1.1 Know that digital content (e.g. reports, summaries, visuals, FAQs, guides, presentations) can be tailored to the needs of different target audiences (e.g. citizens, partners, private and public organisations).	A
3.1.2 Develop and modify digital content (e.g. presentations) to specific audiences and administrative purposes, using appropriate visual and technical formats.	A
3.1.3 Know how to use AI tools (e.g. generative AI) ethically and safely to generate simple digital content by developing and refining questions, commands or statements (prompts) to manage their quality.	A
3.1.4 Apply institutional guidelines for using AI systems in digital content productions within public administration tasks.	A

Descriptor	Level
3.1.5 Use institutional templates and digital text processing tools ensuring clarity, correctness and compliance with professional standards.	A
3.1.6 Value compliance with professional and institutional standards when creating, formatting and modifying digital content (e.g. official documents, visuals, institutional templates) for diverse administrative tasks.	A
3.1.7 Understand the official standards and guidelines (e.g. WCAG 2.1 and EN 301 549) related to digital accessibility of content (e.g. digital files, documents, web-based applications).	B
3.1.8 Know how to create and adapt digital content to meet digital accessibility and interoperability standards, ensuring it is reusable across different platforms and understood by different user groups.	B
3.1.9 Aware that user inputs (e.g. prompt engineering techniques) can be used to reduce the risk of biased, harmful or inaccurate outputs in generative AI tools when creating digital content with AI systems.	B
3.1.10 Document good practices, workflows or lessons learned in reusable digital formats (e.g. templates, guidelines, internal guidance), contributing to institutional knowledge.	B
3.1.11 Inclined to help others to improve their digital content (e.g. through providing useful feedback).	B
3.1.12 Create design guidelines for various types of digital materials (e.g. interactive presentations, data-driven reports, customisable for diverse audiences) optimising their reuse for administrative efficiency.	C
3.1.13 Analyse and audit digital content production, incorporating AI systems, within public administration, and take into account whether ethical, responsible and transparent processes are respected.	C



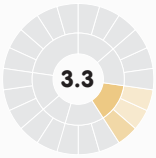
COMPETENCE

3.2 Delivering and contributing to digital public services

To contribute to the creation of inclusive, digitally accessible and people-centric digital public services for citizens and businesses through digital technologies. To support the creation and improvement of digital public services delivery, and to support citizens and businesses to interact with them.

Descriptor	Level
3.2.1 Identify the main digital public services available for citizens and companies in their field of public administration.	A
3.2.2 Aware that 'digital accessibility' means ensuring that everyone, including people with disabilities, can use and navigate public administration websites, digital files and use the services.	A
3.2.3 Open to support citizens and other beneficiaries in accessing relevant digital content, offering guidance where needed and helping adapt digital tools to user needs.	A
3.2.4 Open for collaboration to support the design of digital public services within multidisciplinary teams.	A
3.2.5 Help citizens and other beneficiaries understand, access and confidently use various digital tools in public services, ensuring inclusive and meaningful engagement in digital interactions with public institutions.	B
3.2.6 Support citizens to interact with digital services at government platforms, e.g. helping them obtain and authenticate themselves using eID.	B
3.2.7 Open to integrate formal and informal feedback from direct beneficiaries into the processes of adapting and improving digital public services.	B

Descriptor	Level
3.2.8 Contribute to the development, testing or improvement of public services supported through digital technologies, e.g. simplifying digital forms, automating steps, increasing usability and transparency.	B
3.2.9 Participate in the exploration, testing, or piloting of emerging digital tools and technologies relevant to public administration, contributing to innovation and service improvement.	C
3.2.10 Evaluate and audit the design and functionality of new digital services to ensure they meet user needs and are consistent with relevant frameworks, e.g. strategies, standards.	C

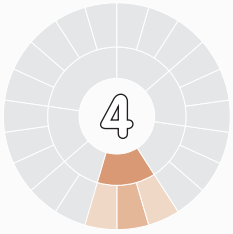


COMPETENCE

3.3 Ensuring compliance with legal and regulatory frameworks and standards in digital environments

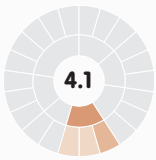
To comply with, and implement, legal and regulatory requirements and standards related to digital public services while protecting fundamental rights, ensuring fairness and promoting public trust in public administration.

Descriptor	Level
3.3.1 Recognise that different kinds of copyright and licences can apply to digital content (e.g. software, audio-visual material), including AI-generated content, and that these determine how content can be used and shared, also in public administration.	A
3.3.2 Understand the features of current legislation in relation to copyright and intellectual property, licensing, and the responsible use of digital technologies, including generative AI.	A
3.3.3 Aware of the methods identified by the legislation for a valid electronic submission of applications and declarations to public administration institutions.	A
3.3.4 Support and contribute to institutional compliance with regulations, standards and procedures applicable to one's area of responsibility (e.g. digital procurement, documentation, audit trails).	B
3.3.5 Apply key concepts related to e-Government and European developments, such as Digital Identity Regulation and European Digital Identity Wallet, and their possible implications.	B
3.3.6 Know the relevant principles from laws and EU regulatory frameworks governing data and data management, including the Interoperability Act.	C
3.3.7 Understand the main provisions of EU and national legislation in the context of public digital public services, such as the GDPR, Data Act, Data Governance Act, Digital Services Act, and relevant parts of the AI Act, considering implications and potential relevance to specific tasks.	C
3.3.8 Assist on main principles of the digital regulatory frameworks and initiatives in the context of public digital public services, e.g. Cybersecurity standards (aligned with National Cybersecurity Strategy), Data governance and interoperability (Law on interoperability, PNI platform), Cloud management and data protection (Government Cloud Infrastructure), Digital Identity Systems (eID), AI-enabled decision-making (National AI Strategy).	C



Safe, responsible and sustainable use of resources

The focus of area 4 is on protecting devices, data, privacy, and digital identity, promoting wellbeing, and ensuring responsible, sustainable use of digital technologies.

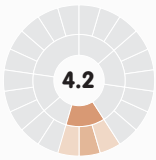


COMPETENCE

4.1 Protecting devices and infrastructures

To apply safety and cybersecurity measures to protect digital devices, content and infrastructure. To be aware of the evolving nature of risks and threats in digital environments. To follow institutional cybersecurity measures and safety protocols to ensure the continuity of digital public services.

Descriptor	Level
4.1.1 Follow and apply institutional cybersecurity practices and preventive measures (e.g. system updates, antivirus tools) to protect devices, digital content and infrastructure from cyber threats.	A
4.1.2 Generate and periodically change secure keys or passwords for the accounts used at work (e.g. ones that combine numbers, signs and letters, multi-factor authentication), knowing that since cyberattack techniques are changing, cybersecurity responses by users also need to change.	A
4.1.3 Acknowledge the importance of one's individual role in contributing to institutional safety protocols, e.g. in the secure management of devices and access to infrastructure.	A
4.1.4 Stay informed about evolving cybersecurity risks and digital threats in professional environments (e.g. phishing, spoofing, viruses, ransomware).	B
4.1.5 Implement secure data handling practices in public administration tasks to ensure compliance with cybersecurity regulations, collaborating with IT teams as needed.	B
4.1.6 Describe different categories of cybercrime, demonstrating knowledge of relevant legislation, such as the Cybersecurity Act, Cyber Solidarity Act and the European Directive on security of network and information systems (NIS).	C
4.1.7 Apply the cybersecurity policies to ensure secure handling of electronic media in public administration tasks and implement best practices like access verification and incident reporting.	C

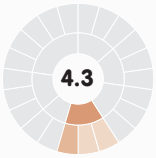


COMPETENCE

4.2 Managing digital identities, and protecting personal data and privacy

To manage digital identities (e.g. eID) to ensure secure and reliable digital identification for accessing and using digital public services, and their related digital processes. To ensure compliance with personal data regulations and privacy in public administration.

Descriptor	Level
4.2.1 Recognise the concept of digital identity as both a means of authenticating (validating) an individual, and the data generated by an individual's online activities, which can be combined from different sources.	A
4.2.2 Know that the public administration uses an e-signature system and is aware of its advantages and disadvantages.	A
4.2.3 Know how to use digital authentication services for public employees in their field of public administration and its related services, e.g. follow procedures to e-sign official documents and workflows.	A
4.2.4 Identify and apply basic measures and principles to manage digital identity and safeguard personal data, workplace and other sensitive information in digital environments.	A
4.2.5 Know the principles of how citizens can use eID to access digital public services and government platforms, e.g. Digital Identity Systems (eID).	B
4.2.6 Understand the different levels of privacy that can be set on one's own digital devices as well as on cloud services and apply them in digital work environments.	B
4.2.7 Understand key concepts in the EU related to data protection and privacy legislation, including data minimisation.	B
4.2.8 Knows that in the EU, citizens have the right to ask the administrator of digital services to access the personal data held about them (right of access), to update or correct them (right of rectification), or remove them (right of erasure, also known as the Right To Be Forgotten).	B
4.2.9 Safely manage and share personal data and other sensitive information across public administration services under current data protection and privacy legislation.	B
4.2.10 Conduct privacy risk assessment to protect sensitive data and privacy from misuse and breaches, ensuring GDPR compliance.	C
4.2.11 Aware that various types of user data (e.g. personal, behavioural, contextual) can be used to produce user profiles for predictive purposes (e.g. identify potential beneficiaries of public services).	C



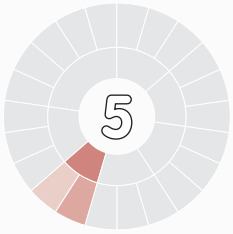
COMPETENCE

4.3 Supporting healthy and sustainable digital practices

To use digital technologies to minimize risks and threats to physical, mental and social wellbeing of oneself and others. To use digital technologies to support sustainability and environmental practices in public administration.

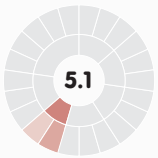
Descriptor	Level
4.3.1 Recognise individual wellbeing risks and threats associated with the use of digital technologies at work, such as negative impact on posture, sleep patterns, cyberbullying, grooming, self-perceptions, techno-stress, and types and signs of digital dependency.	A
4.3.2 Recognise the importance of energy-efficient practices at work when operating digital devices.	A
4.3.3 Contribute to a digital work culture that is respectful, inclusive, and supportive of diverse needs, fostering equitable access to digital services and tools.	B
4.3.4 Identify and act upon cases of cyber-bullying or internet fraud if they occur in the institution where they work.	B
4.3.5 Promote responsible and future-oriented attitudes in the use of digital resources (e.g. digital devices, AI systems, digital platforms), in line with institutional values and public service ethics.	B
4.3.6 Aware of the environmental impact of digital technology (e.g. energy use, device lifecycle, data storage) and apply sustainable practices when using digital tools.	B

Descriptor	Level
4.3.7 Assess and audit institutional practices in relation to health, wellbeing and inclusion in digital environments to guide future practices in a specific context.	C
4.3.8 Assess and audit ways of using digital tools to support socially and environmentally responsible behaviour in public administration, e.g. to prevent cyberbullying and to reinforce safe online use.	C



Problem-solving through digital technologies

The focus of area 5 is on the identifying and solving technical problems in digital environments, including on contributing to more efficient workflows by applying automation and programming techniques.

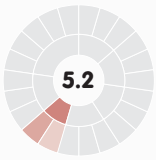


COMPETENCE

5.1 Managing digital devices, including identifying and solving technical problems

To know digital tools (e.g. devices, interfaces, software applications) and understand the basics of digital technologies used in public administration processes. To identify technical problems and to solve them through a variety of means.

Descriptor	Level
5.1.1 Use confidentially and safely institutional digital devices (workstations, printers), digital environments and core software applications for administrative work (e.g. document management systems, electronic archives, workflow and case management tools, public service delivery platforms).	A
5.1.2 Understand the basic operating logic and functionalities of digital devices, tools and infrastructures used in their field of public administration to resolve routine technical issues to complete professional tasks efficiently.	A
5.1.3 Autonomously use digital technologies to telework in their field of public administration.	A
5.1.4 Diagnose simple technical problems encountered when using digital tools, devices or systems in professional contexts (e.g. login issues, connectivity failures, file compatibility), using institutional guidance or support materials when needed.	A
5.1.5 Know a variety of alternatives to overcome technology limitations in order to perform necessary tasks at job (e.g. using alternative applications, scanning a document with a mobile device).	B
5.1.6 Document and report more complex technical issues to IT support or helpdesk teams, providing relevant context, screenshots, or error messages to ensure efficient resolution.	B
5.1.7 Coordinate with IT staff and other technology specialists to resolve technical issues affecting public administration tasks, ensuring operational continuity.	C
5.1.8 Analyse complex technical situations, both face-to-face and virtually, where employees need help to trouble-shoot a technical issue and help create new step-by-step guidance such as video tutorials and other guidelines.	C

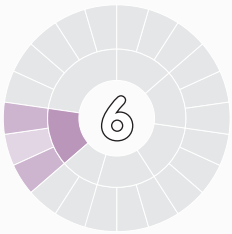


COMPETENCE

5.2 Using automation tools in digital environments

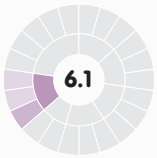
To understand and implement steps to analyse issues (e.g. identify repetitive digital tasks and processes) in public administration workflows that can be simplified, and plan and develop a sequence of instructions for a computing system to solve them or to perform a specific task.

Descriptor	Level
5.2.1 Identify repetitive and basic digital tasks in one's work that can be streamlined using simple automation tools (e.g. email filters, form templates).	A
5.2.2 Follow basic instructions to automate simple tasks.	A
5.2.3 Understand that each problem, both analogue and digital, can be unpacked into different sub-problems and can have different entry points for developing solutions.	A
5.2.4 Take initiative in proposing or implementing changes that simplify procedures, increase efficiency, or improve service quality, using available technologies or piloting new ones.	B
5.2.5 Describe (with examples) the general steps in computational thinking, such as problem decomposition, pattern recognition, algorithmic thinking and abstraction.	B
5.2.6 Assess the use of office automation tools in routine tasks to ensure ethical and responsible deployment, data accuracy, transparency of steps, and compliance with institutional standards.	C
5.2.7 Represent simple sequences symbolically, or interpret simple symbolic sequences, to incorporate computational thinking basics into relevant tasks and goals.	C



Digital transformation in public administration

The focus of area 6 is on supporting digital transformation and developing capabilities to operate autonomously in digital environments, keeping pace with digital technological developments, including AI.

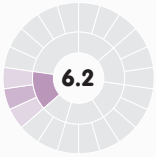


COMPETENCE

6.1 Contributing to digital transformation in public administration, driving innovation and improvement

To identify and support digital transformation initiatives, and to be open to experiment with digital technologies to innovate processes and services in public administration in a people-centric manner.

Descriptor	Level
6.1.1 Know some of the main drivers of digital transformation within their field of public administrations and its related services.	A
6.1.2 Identify some innovation initiatives that take advantage of digital and emerging technologies in their field of public administration.	A
6.1.3 Open to support organisation's leadership for digital transformation, including to new management and organisational practices (e.g. related to procurement and budgeting).	A
6.1.4 Aware that some of the tasks and workflows are better performed by using digital technologies, whereas other tasks are better performed by humans.	A
6.1.5 Engage and support the implementation of digital transformation initiatives in one's area of work, such as the adoption of new technologies, automation of workflows and digital services redesign.	B
6.1.6 Promote the importance of shaping the right environment so that digital transformation initiatives can be designed and developed in a given field of public administration.	B
6.1.7 Understand the importance of iteration and rapid feedback loops – allowing new ideas to be tested on a small scale before reaching a wider level of implementation – and the importance of incremental development approaches (e.g. each stage of a project builds on the preceding one).	C
6.1.8 Follow technological changes and disruptive developments of digital technologies, both in public administration and outside, to gather a comprehensive understanding of the needs for developing capacity and human resources in public administration.	C
6.1.9 Use approaches such as 'horizon scanning' and 'looking outwards' at the trends and drivers for emerging technologies to support innovation around the policy cycle (e.g. policy planning, policy design and impact assessment, policy implementation and policy evaluation phases).	C

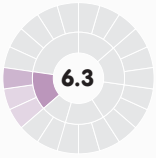


COMPETENCE

6.2 Developing digital competence in the workplace

To recognize where one's digital competence needs to be improved or updated to be adequate for working in public administration. To stay informed about digital technological developments and their personal, professional and societal implications.

Descriptor	Level
6.2.1 Open to adapt to use new digital tools and applications to complete one's work when supported by adequate training.	A
6.2.2 Aware of the training plans on digital skills and competences in their field of public administration, e.g. from public administration's e-learning campuses.	A
6.2.3 Engage with learning opportunities that best fit professional development needs (e.g. online courses, peer learning) for self-development at work and within a broader process of lifelong learning.	A
6.2.4 Apply newly acquired digital skills and competences in day-to-day tasks, evaluate their effectiveness, and refine practices accordingly.	B
6.2.5 Demonstrate motivation and responsibility for continuous digital development, modelling good digital practices and encouraging others to do the same.	B
6.2.6 Assess and audit methods to identify digital competence gaps at work (e.g. routine tasks, for remote work), and provide suggestions for new training methods and mentoring mechanisms.	C
6.2.7 Follow international trends in how the concept of digital competence and its continuum of proficiency evolves over time, e.g. by showing interest in international reference frameworks.	C



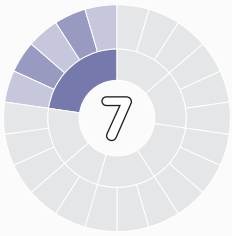
COMPETENCE

6.3 AI Literacy in public administration

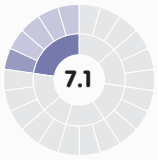
To ensure a general conceptual understanding of what Artificial Intelligence (AI) is, contexts for its application, and critical, ethical and responsible approaches to using AI in public administration tasks and processes. Understand legal requirements concerning the use of AI in public administration (e.g. AI Act).

Descriptor	Level
6.3.1 Aware that when using any AI systems in public administration, the user should be provided with a suffcient level of AI literacy.	A
6.3.2 Open to consider the opportunities of AI systems and emerging technologies for the functions of public administration.	A
6.3.3 Recognise what AI is in general terms, making a basic distinction between what is and what is not an AI system.	A
6.3.4 When using AI tools in public administration tasks, even generative AI tools freely available, aware that public administration might have rules about their use at work (e.g. they might lack suitable institutional oversight and thus pose risks for use in public administration).	B
6.3.5 When using AI tools, either institutional or free ones from the Internet, aware that inputting sensitive, proprietary or personal data into AI systems can lead to unintended consequences, e.g. leakage of this data, misuse of personal data.	B
6.3.6 Identify which types of tasks in one's regular work in public administration are more or less suitable to complete using AI tools (e.g. generative AI) and can outline safeguards in place to ensure humans can override AI systems.	B

Descriptor	Level
6.3.7 Critically evaluate some capabilities of AI to support human skills and judgement, and know that AI can also be used to substitute human skills.	B
6.3.8 Know, in general terms, relevant AI concepts (e.g. large language models, machine learning, deep learning) and examples of their use in their field of public administration.	B
6.3.9 When using AI systems at in public administration tasks, aware of the risks of the AI system and basic steps to mitigate those risks, including how legal and ethical aspects can affect the individuals they are used on.	B
6.3.10 Value the importance of staying informed about, and discussing, digital technologies' ethical and social implications in public administration (e.g. AI systems in PA, digital inclusion/ exclusion).	B
6.3.11 Contributes to the development of practices that support AI literacy guidance in public administration institutions according to legislation or industry standards.	C
6.3.12 Distinguish examples of high-risk AI systems (e.g. according to legislation) in their field of public administration, their potential negative impacts and how the persons on whom the AI system is used can exercise their rights.	C



Digital leadership and governance in the public administration



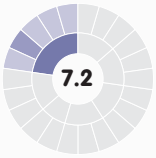
COMPETENCE

7.1 Managing performance and operations through digital technologies

To use digital technologies for planning, organising, and monitoring activities and resources, ensuring efficient achievement of institutional objectives within defined parameters.

Descriptor	Level
7.1.1 Use professional collaborative platforms for systematic activity management and monitoring team progress, e.g. through digital dashboards for KPI tracking with automated alerts and performance visualisation.	A
7.1.2 Apply concepts and principles such as: digital project management, digital workflow management and performance monitoring, e.g. dashboards, key performance indicators (KPI) and objectives and key results (OKR).	A
7.1.3 Demonstrate transparency through regular sharing of team performance indicators in an accessible format and proactively request feedback for continuous improvements.	A
7.1.4 Ensure comprehensive digital feedback systems for continuous improvement (e.g. through performance self-assessment), while applying digital documentation of evaluations with full traceability.	A
7.1.5 Apply concepts and principles such as: business intelligence, advanced performance analytics, process optimization, workforce analytics, predictive modelling and integrated management systems.	B
7.1.6 Integrate data from multiple institutional systems into unified dashboards to follow performance, using filtering and drill-down functions, to enable evidence-based resource allocation decisions and real-time operational adjustments.	B

Descriptor	Level
7.1.7 Demonstrate digital agility through adopting new performance monitoring tools and experimenting with emerging solutions for performance & process optimisation.	B
7.1.8 Promote a culture of continuous optimisation (e.g. using advanced analytics to identify bottlenecks and measurably improve public services), including those delivered through digital technologies.	C
7.1.9 Shape strategic investment decisions for digital and operational initiatives by interpreting performance intelligence and scenario analyses to optimise resource use and strengthen institutional outcomes.	C

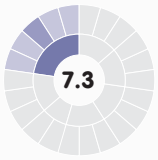


COMPETENCE

7.2 Leading team development in digital environments

To align the use of digital technologies with organisational and strategic priorities (e.g. managers support team's digital upskilling) while fostering organisational culture to support institutional performance and adaptability.

Descriptor	Level
7.2.1 Apply concepts and principles relevant to digital team development, such as digital learning, e-learning platforms, microlearning, digital skills assessment and constructive feedback.	A
7.2.2 Apply concepts and principles in digital environments, such as digital leadership, digital inclusion and emotional intelligence.	A
7.2.3 Create and support digital competency development plans for individuals with expected learning outcomes and encourage feedback mechanisms for continuous learning path adaptation.	A
7.2.4 Provide strategic direction, oversight and training opportunities for the use of AI tools in public administration to integrate them into relevant parts of the team's processes and workflows while mitigating the risk of discriminatory outcomes from AI uses.	A
7.2.5 Apply concepts and principles such as: blended learning, organizational learning, digital coaching, future skills and motivation psychology in remote work (autonomy, belonging, fairness).	B
7.2.6 Promote and ensure constant support for the team's digital development, pursuing early identification of necessary competencies, especially in AI use cases, and facilitating access to relevant learning resources.	B
7.2.7 Enable and oversee the design and roll out of structured digital upskilling programs for the team (including training on AI systems where relevant), and support translation of acquired skills into updated job descriptions and workflows.	B
7.2.8 Operate with concepts and principles such as: strategic talent development, organisational capability, future of work, digital transformation culture, talent management, leadership pipeline and digital succession planning.	C
7.2.9 Shape and drive institutional digital workforce development by ensuring and aligning learning priorities, partnerships and investments with emerging upskilling needs (e.g. AI governance, advanced data literacy, interoperability expertise).	C
7.2.10 Promote an organisational culture of continuous learning, collaboration and digital innovation, through personal example and support programs that integrate digital technologies in professional competency development.	C

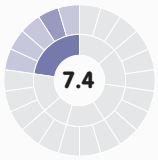


COMPETENCE

7.3 Driving and leading innovation and digital transformation

To initiate, sustain and coordinate institutional digital transformation by integrating innovation and process changes to solve complex societal problems. To mobilise necessary financial, human and social capital resources to turn ideas into value in public administration while minimising the negative impact and maximising the benefits of change.

Descriptor	Level
7.3.1 Provide strategic direction to operate with concepts and principles relevant to digital transformation in the public sector, such as people-centric public service design, accessibility-by-default, usability-testing, controlled environment testing, iterative delivery, rapid prototyping and agile methodologies applied in public administration.	A
7.3.2 Apply concepts and principles such as: innovation management, change management, design thinking, digital transformation, open innovation and digital resilience.	A
7.3.3 Coordinate, within their area of professional specialisation, the identification of opportunities for automation and digital transformation of work processes, and propose, pilot and support the implementation of process improvements (e.g. automations, AI proof-of-concepts) to optimise workflows and service delivery, in collaboration with relevant technical support units, and with attention to risk mitigation.	A
7.3.4 Apply concepts and principles such as: institutional digital maturity, digital disruption strategy, strategic digital partnerships, cultural transformation, regulatory innovation, public-private digital ecosystems and governance frameworks for digital innovation.	B
7.3.5 Support and refine the creation of criteria for evaluating and prioritising innovation ideas, taking into account conditions for controlled experimentation (digital sandboxes), and ensure the development of departmental digital transformation strategies with structured innovation pipeline processes.	B
7.3.6 Develop and support an institutional vision for digital transformation aligned with the national strategy and provide strategic direction for coordinating digital transformation initiatives.	C
7.3.7 Contribute to the development of an institutional AI roadmap, aligned with AI Act requirements and Digital Decade objectives, while ensuring organisational cultural transformation and change management processes.	C
7.3.8 Provide strategic direction to develop partnerships with actors from the technology ecosystem (e.g. with academia, private industry, civil society and other government agencies) to integrate digital solutions that meet institutional needs and increase public service value.	C

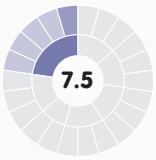


COMPETENCE

7.4 Strengthening public services and ensuring responsible digital governance and cybersecurity

To lead the creation of digital governance principles and frameworks for responsible use of data and technologies in public administration. To coordinate policies on long-term data governance, their quality, ownership and regulatory compliance ensuring transparency and interoperability of information systems and digital services.

Descriptor	Level
7.4.1 Apply concepts and principles such as: data governance frameworks, transparency by design, data lifecycle, information classification, digital interoperability, technical standards compliance, and digital ethics and integrity in public service.	A
7.4.2 Coordinate and monitor institutional procedures for data quality assurance and metadata managements (e.g. data classification procedures according to institutional standards), ensuring compliance with regulatory standards such as national classification schemes and the Once Only Principle System.	A
7.4.3 Monitor team compliance with basic cybersecurity (e.g. complex passwords, software updates, VPN usage) and personal data protection rules in digital workflows, identify and report incidents, and propose immediate corrective measures in line with GDPR and NIS2 requirements.	A
7.4.4 Provide strategic direction and collaborate with the development of digital governance policies aligned with organisational strategies to establish a long-term data culture in the organisation.	B
7.4.5 Support and oversee the data value chain for analytic techniques to discover and explore data insights, and to identify new data requirements, to address the organisation's challenges and opportunities, e.g. to solve complex problems, deliver better public services and provide evidence-led policymaking.	B
7.4.6 Contribute to the evaluation of ethical aspects of digital technology implementation, e.g. algorithmic bias, discrimination, automated decision transparency, AI ethical dilemmas in public service contexts, including environmental impact associated with AI adoption.	B
7.4.7 Advocate for the integration of digital ethics criteria and responsible AI principles (transparency, explainability, fairness) into technological transformation and innovation strategies.	B
7.4.8 Support and oversee the coordination and development of organisational digital governance strategies, aligned with a national legal framework and European regulations, including comprehensive AI and data governance frameworks for institutional implementation.	C
7.4.9 Know strategic concepts and guidelines related to digital risk management, zero trust, cyber resilience and national cybersecurity strategies.	C



COMPETENCE

7.5 Anticipatory and strategic thinking supporting public administration

To use strategic foresight to anticipate and prepare for potential changes, guiding decision-making in public administration towards more sustainable, long-term solutions. To understand systemic interdependencies and formulate anticipatory responses to institutional challenges due to technological trends impacting societies.

Descriptor	Level
7.5.1 Familiar with concepts of anticipatory and strategic foresight in public administration (the ability to anticipate future developments, problems and unexpected events) to explore strategic opportunities and develop futures visions.	A

Descriptor	Level
7.5.2 Recognise the complexity and interconnected nature of problems governments face and the need to develop the ability to understand the properties and dynamics of complex systems.	A
7.5.3 Create simple what-if scenarios to simulate the impact of policy changes to better understand systemic interdependencies (e.g. in activities and service delivery).	A
7.5.4 Operate with concepts and principles such as: strategic anticipation, organizational intelligence, complex systems analysis, scenario planning for decision support.	B
7.5.5 Promote anticipatory and systemic thinking within teams, supporting use of digital tools to understand interdependencies and anticipate decision impact on public services.	B
7.5.6 Develop and promote strategic foresight capabilities across the organisation for anticipating societal and technological trends impacting digital public services.	C
7.5.7 Contribute to foresight scenarios to mitigate the risk of discriminatory outcomes from AI uses in public administration, especially those considered high-risk under current legislation (e.g. AI Act).This includes creating scenarios on the long-term impacts of AI systems on beneficiaries to inform strategies to better mitigate bias in welfare prediction systems.	C
7.5.8 Lead the development of institutional-level horizon-scanning and foresight exercises, integrating weak signals and emerging technological trends (e.g. quantum computing, generative AI) into long-term strategic planning while aligning them with EU and national strategies (e.g. Digital Decade 2030 targets).	C

2.5 Focus on AI and Digital Transformation, building on a foresight exercise

47. **The foresight exercise underpinning the proposed digital competency framework took into consideration the longer-term technological, economic, and social forces likely to shape digital skills needs in the coming decade.** As presented in Output 1[53] developed under the TSI project, rather than assuming a single linear future, the analysis considered a spectrum of plausible trajectories, from incremental digital adoption to more disruptive, systemic transformations. Across these scenarios, several consistent drivers emerged, including accelerating automation, the diffusion of AI-enabled tools across all occupational groups, and rising expectations for data-literate and digitally autonomous workers. These drivers provided the basis for identifying competencies that would remain relevant even amid rapid technological change, ensuring the framework supports not only today's digital demands but also those anticipated in more ambitious future states.

48. **At the same time, the proposed digital competency framework assumes a moderately transformative scenario rather than a purely conservative one.** This means it anticipates substantive shifts in how work is organised, how services are delivered, and how citizens interact with digital systems, while still grounding recommendations in capacities that can realistically be developed within current institutional constraints. The emphasis on adaptability, problem-solving in technology-rich environments, and the ethical use of digital tools reflects this forward-looking stance. By articulating these assumptions more explicitly, the report aims to help first-time readers understand why certain competencies are prioritised, how they relate to long-term national goals, and how the framework remains robust even as technologies and workforce expectations evolve.

49. **The proposed model explicitly acknowledges the growing strategic role of artificial intelligence in public administration by introducing a dedicated competency on AI literacy (6.3) and by embedding AI-related descriptors across multiple competency areas.** This dual approach reflects the understanding that AI is not a standalone technical topic, but a cross-cutting capability with implications for operational work, management, and governance[54]. Competency 6.3 provides a common baseline for civil servants, ensuring a shared understanding of what AI is, how AI systems function, and how they can be used responsibly in public-sector contexts. It addresses key issues such as explainability, data protection, bias mitigation, and institutional accountability, and is designed to support compliance with Article 4 of the EU AI Act.

50. **Beyond this dedicated competency, AI-related elements are systematically integrated throughout the framework to reflect its practical use across different functions.** For example, Competency 1.1 (Searching and accessing information) includes the use of AI systems for information retrieval and prompt formulation; Competency 2.3 (Digital integrity and accountability) addresses risks linked to algorithmic bias, transparency, and responsible use of automated systems; and Competency 7.5 (Foresight and strategic thinking) covers the application of AI for predictive analytics, scenario modelling, and evidence-informed planning at whole-of-government level. This distribution ensures that AI is treated both as an operational tool and as a strategic enabler.

53. World Bank, Output 1 - Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service : Taking Into Account Relevant Policies at the National and European Union Levels, 2025. Available at: https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745.

54. Note: DigComp 3.0 builds on the initial work of DigComp 2.2 to systematically include the aspects of AI competence that are relevant for individuals to develop as part of their digital competence. AI competence is intertwined with and builds on other elements of digital competence, as AI systems are widely diffused, and increasingly embedded within existing digital technologies. In DigComp 3.0, AI is framed as one digital technology among a range of digital technologies, while keeping the focus on the digital competences themselves.

51. **Embedding AI across both technical and strategic dimensions of the competency framework equips civil servants not only to apply AI tools in their daily work, but also to critically assess their broader implications for governance, ethics, and public service delivery.** By making these expectations explicit, the model supports a more informed, cautious, and value-driven adoption of AI in the public sector. This structured and anticipatory approach is consistent with emerging international practice and closely aligned with the orientation of DigComp 3.0, which places increased emphasis on AI, data, and emerging technologies. In the context of rapid AI deployment and evolving regulatory requirements across the EU, the model provides a relevant and forward-looking foundation for building institutional capacity and ensuring responsible use of AI in public administration.

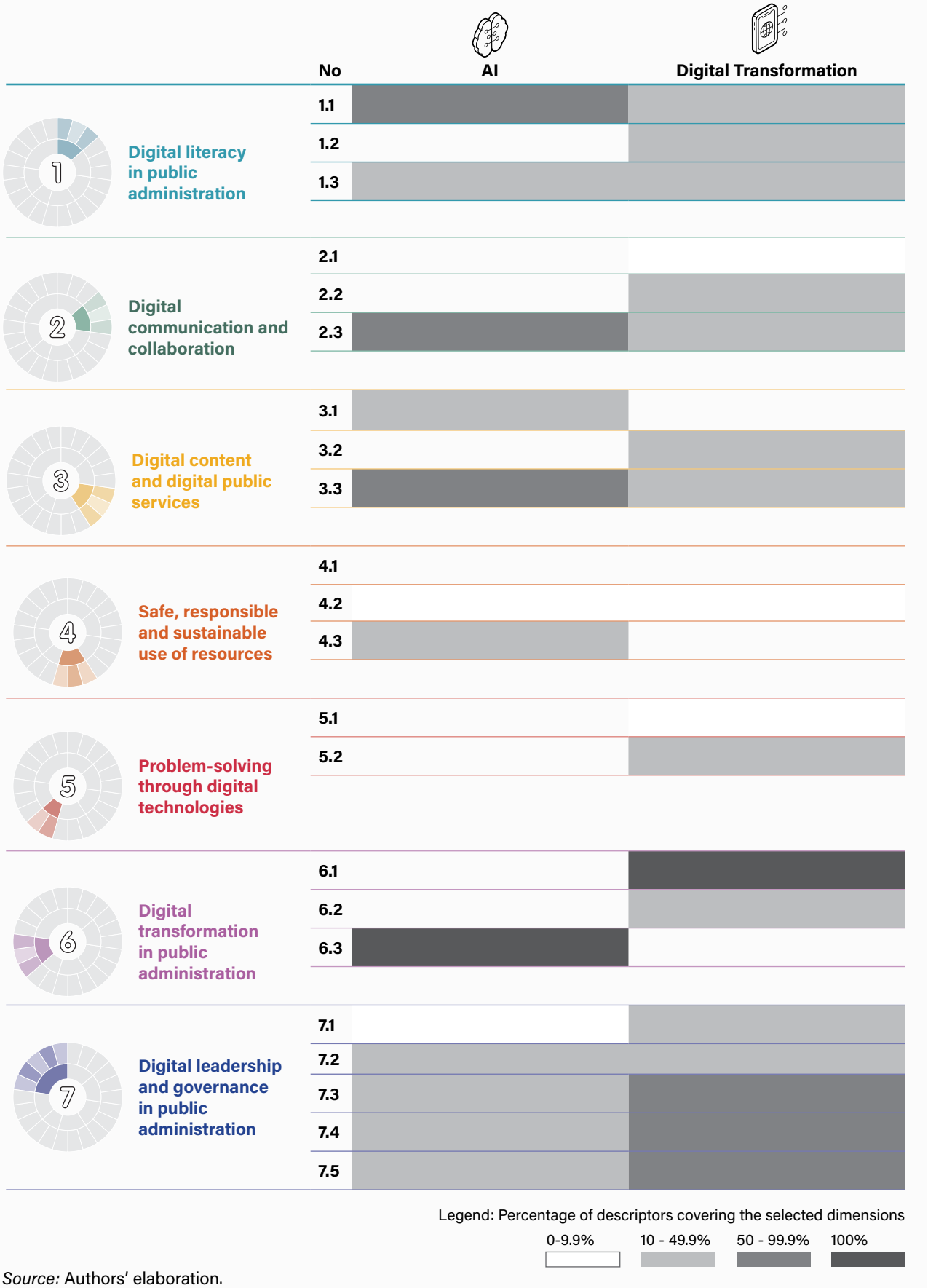
52. **Digital transformation is also addressed in the model through a coherent set of competencies spanning Areas 5, 6, and 7, which together support the integration of digital systems into both operational and managerial processes.** Competencies such as 5.1 (Managing digital devices), 6.1 (Contributing to digital transformation), and 7.3 (Driving and leading digital transformation) reflect the different levels at which digital change occurs in public administration – from day-to-day use of digital infrastructure to organizational transformation, and to strategic leadership. This structure ensures that civil servants are not only able to adopt digital tools, but also to apply digital thinking in policy design, service delivery, and management, and to align digital initiatives with institutional and government-wide priorities.

53. **The decision to establish Digital Transformation as a distinct competency area (Area 6) is central to the future-readiness of the framework.** While Areas 1–5 focus primarily on operational digital skills – including how to search for information, evaluate content, manage data, create digital outputs, communicate, and ensure cybersecurity – Area 6 captures the skills, attitudes, and responsibilities required to actively drive transformation. What may appear as overlap with operational areas reflects a deliberate distinction in orientation: for example, AI in Area 1 is treated as a tool supporting task execution, whereas in Area 6 it is framed as a strategic enabler of change, requiring understanding of ethical considerations, governance arrangements, and the broader context in which AI systems are deployed. This design makes explicit that digital transformation is not a purely technical exercise, but one that involves organizational culture, behavioral change, and institutional accountability.

54. **By positioning digital transformation as a shared responsibility across roles and functions, the framework moves beyond a narrow, IT-centric view of digitalization.** It highlights the need for public servants at different levels to engage with change management, systems thinking, and innovation, while ensuring that digital reforms are implemented responsibly and sustainably. This approach reflects an emerging international consensus that successful digital transformation in government depends as much on leadership and organizational capability as on technology itself.

55. **The heatmap below shows the focus of each of the competences on AI and Digital transformation (DT).** Currently, it shows that 8 of the general competences applicable to all civil servants (areas 1-6) include descriptors that cover pertinent aspects of AI use in civil servants' tasks using a heat scale from 0 to 4. For example, competence 6.3 "AI Literacy in public administration" shows full heat with all the descriptors covering aspects of AI, whereas for the competence 2.3 "Ensuring digital integrity and accountability in public administration", it shows that half of the descriptors cover aspects of AI.

TABLE 3: Heatmap – focus of the proposed framework – descriptors with content relevant for AI and Digital Transformation



Source: Authors' elaboration.

56. **International experience supports this direction.** In August 2024, Latvia adopted a Digital Skills and Competencies Framework for Public Administration, structured around six thematic areas and 29 competencies with 400 descriptors. The Latvian framework goes beyond basic digital literacy, explicitly incorporating competencies related to AI use, digital leadership, governance of digitalization, change management, and systems thinking[55]. Similarly, the Spanish Marco de Competencias Digitales[56] includes a dedicated area on digital transformation and is widely regarded as a mature and comprehensive model. These examples illustrate a broader trend across Europe: governments are increasingly treating digital transformation and leadership as distinct competency domains, essential for building public administrations capable of managing complexity, sustaining innovation, and delivering public value in a digital age.

2.6 Beyond general digital competencies – specialized ICT roles

57. **Digital transformation requires not only general digital competencies for all civil servants, but also clearly defined specialized ICT roles.** While general digital skills enable staff across the administration to use digital tools effectively, the design, development, operation, and governance of advanced digital systems demand distinct technical and managerial expertise. Functions such as cybersecurity management, enterprise architecture, application development, data analytics, testing, system integration, and service design cannot be delivered through generic job roles or broad competency requirements. Without explicit professional ICT profiles, administrations face blurred responsibilities, over-reliance on outsourcing, limited internal knowledge accumulation, and heightened operational and cybersecurity risks.

58. **International experience distinguishes between general digital competencies and professional ICT skill frameworks.** At European and international levels, this separation is anchored in several reference models. The European e-Competence Framework (e-CF)[57] defines structured professional ICT roles and 41 competences across five core processes (Plan, Build, Run, Enable, Manage). Cybersecurity roles are further specified through the European Cybersecurity Skills Framework (ECSF)[58]. The ESCO classification supports occupational mapping across EU labour markets, while public administration implementation models such as the UK Government Digital and Data (DDaT) Profession Capability Framework[59] illustrate how specialized ICT professions can be embedded within government systems. Together, these frameworks demonstrate that advanced digital capacity requires distinct professional role definitions that go beyond general workforce digital literacy.

59. **Against this background, the TSI project developed and tested a model for structuring specialized ICT capacity in the public administration, that proved relevant in the Romanian context.** Analytical mapping linked existing ICT functions in participating institutions to the e-CF and ECSF role profiles, complemented by practitioner consultations and international benchmarking. The resulting framework was therefore designed to be fit to the Romanian context. However, its strong anchoring in e-CF and ECSF make it adaptable to varying administrative contexts across the EU.

55. https://www.vas.gov.lv/lv/jaunums/izstradats-publiskas-parvaldes-digitalo-prasmju-un-kompetencu-ietvars.
56. https://www.inap.es/es/aprendizaje/ecosistema-competencial/marco-de-competencias-digitales.
57. https://itprofessionalism.org/professionalism/e-competence-framework/.
58. https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.
59. https://ddat-capability-framework.service.gov.uk/.

60. **A core conceptual element of the model is the distinction between ICT "roles" and ICT "jobs"[60]:**

- *Roles* define what work needs to be performed, captured as structured bundles of tasks, responsibilities, and competences – such as Systems Administrator, Cybersecurity Specialist, Developer, or Enterprise Architect. Roles are competency-based and remain independent of organizational charts. They are used to define recruitment requirements, guide training curricula, structure professional development pathways, and support workforce planning.
- *Jobs*, by contrast, define the formal, legally classified positions within national HRM systems. Jobs correspond to formal posts embedded in civil service or contract staff regimes, linked to grading and pay structures, and governed by national legislation. A single job may include one dominant role and several secondary roles, particularly in smaller administrations or agencies with limited ICT staffing capacity.

61. **Maintaining a clear analytical separation between roles and jobs enables administrations to reconcile professional workforce needs with diverse national HRM frameworks.** Role definitions allow governments to identify the actual ICT capacities required to deliver digital strategies. Job classifications determine how these capacities are embedded into formal staffing structures and career systems. This approach avoids reliance on generic job titles that obscure required competences and ensures that HR systems reflect functional realities rather than administrative labels.

TABLE 4: Proposed ICT roles based on e-CF, ECSF and the design process

No.	ICT roles proposed for the Romanian public administration
1	Business Analyst
2	Business Information Manager
3	Chief Information Officer (CIO)
4	Database Administrator (DBA)
5	Data Scientist
6	Data Specialist
7	Developer
8	Digital Transformation Leader
9	Enterprise Architect
10	ICT Operations Manager
11	ICT Specialist
12	Information Security Manager
13	Information Security Specialist
14	Network Specialist
15	Product Manager
16	Service Designer
17	Service Support
18	Solution Designer
19	Systems Administrator
20	Systems Analyst
21	Systems Architect
22	Technical Specialist
23	Test Specialist
24	User Researcher

60. See also JRC Publications Repository - A unified conceptual framework of tasks, skills and competences

62. **Under the TSI project, a proposed classification of 24 ICT professional roles was developed.** The role set is primarily derived from the e-CF profiles and supplemented with user-centred and service-delivery roles **drawn** from additional public administration frameworks, including ESCO and the UK DDaT model. The full list addresses the entire digital services lifecycle:

63. **These roles cover the spectrum of functions required for modern digital government.** Strategic leadership and ICT governance are reflected in roles such as CIO and Business Information Manager. Architecture and design are addressed through Enterprise, Systems, and Solution Architect profiles. Cybersecurity is captured through dedicated managerial and specialist roles. Infrastructure operations and continuity rely on Systems Administrators, Network Specialists, Service Support staff, and Technical Specialists. Development and data functions include Developers, Data Scientists, Data Specialists, and DBAs. User-centred digital transformation is supported through the addition of Product Managers, Service Designers, and User Researchers, reflecting the growing emphasis on accessibility, usability, and citizen trust in public digital services.

64. **For HRM integration in the Romanian job classification system, roles were proposed to be grouped into six broad ICT job families aligned with e-CF domains:**

- ICT Manager (strategic leadership and governance);
- ICT Architect (architecture and systems integration);
- Cybersecurity Specialist (security management and operations);
- ICT Service Delivery and Support Specialist (operations, testing, and user support);
- ICT Service Management Specialist (business analysis and service/process management); and
- ICT Development and Data Specialist (software development and data analytics).

65. **The framework is scalable and adaptable to different institutional sizes and levels of digital maturity.** Smaller organizations may necessarily combine several ICT roles within single jobs, while administrations operating large or critical systems progressively require deeper specialization and separation of functions. The approach does not impose rigid staffing templates but establishes a clear professional reference model that can be calibrated to national contexts, resource constraints, and differing digital transformation trajectories.

66. **A pilot process across three large participating institutions demonstrated the practical applicability of this model.** Existing ICT activities could be mapped intuitively to the proposed roles across administrations with varying mandates and maturity levels. At the same time, the pilot revealed widespread gaps: many institutions covered less than half of the professional roles required for their digital portfolios, particularly in architecture, testing, development, data management and user-centred design. Operational support functions were usually present, but advanced or strategic ICT capacities were frequently absent or performed informally.

67. **The ICT role framework therefore provides a practical diagnostic and reform instrument applicable across administrations.** It enables systematic mapping of existing ICT capacities against professional benchmarks, identification of missing or under-represented functions, detection of single-person dependencies that create continuity risks, and prioritization of recruitment or upskilling actions. Importantly, the framework remains usable even where HRM maturity is uneven, since it overlays professional role definitions onto existing job classification systems rather than replacing them.

68. **In parallel, the job-family classification offers a replicable mechanism for translating professional ICT profiles into formal public administration career structures.** Member States may operationalize these job families either within civil service career systems or through contract-based arrangements

that provide additional pay flexibility for scarce digital skills. Both approaches are used across the EU and can be combined depending on labour-market pressures and institutional traditions. The framework intentionally supports national choice rather than prescribing a single legal model.

69. **Taken together, the specialized ICT role framework and the general digital competency framework form an integrated capacity strategy for digital government.** The general framework establishes baseline digital readiness across all public servants. The ICT professional framework ensures that deep technical and managerial expertise is available where systems complexity, cybersecurity risks, and service innovation demands are highest. The job-family structure provides the HRM interface required to embed these competencies into recruitment, classification, training, and career progression systems.

70. **For EU Member States, this dual-track model offers a transferable reference for strengthening digital workforce capacity.** It supports professionalization of public administration ICT careers, reduces dependency on fragmented outsourcing, enhances cybersecurity and continuity of operations, and creates clearer pathways for attracting and retaining scarce digital talent. Most critically, it anchors digital transformation not only in technology investments or policy strategies, but in a sustainable internal workforce model capable of delivering and maintaining results over time.

III. From framework design to implementation pathways

3.1 Embedding the framework into HRM processes

71. **Digital competencies are expected to be integrated into existing HRM systems rather than treated as a parallel track.** In many Member States, elements of competency-based HRM are already in place[61], linking certain processes such as recruitment, development, mobility and performance to structured competency models. In such systems, a digital competency framework is most effective when embedded into this architecture, reinforcing and complementing existing processes rather than creating new, standalone ones. In administrations where competency-based HRM remains less developed, digital competencies can serve as a practical entry point for modernization: they represent a clear, universally relevant domain that allows institutions to experiment with competency-based methods while simultaneously addressing an urgent capability gap.

72. **Differences in HRM maturity and digital readiness across Member States fundamentally shape implementation pathways.** Public administrations vary widely in how they define job requirements, how consistently they apply competency models and how advanced their digital transformation[62] is. Some have comprehensive competency frameworks underpinning recruitment, performance and mobility; others operate with fragmented job descriptions and early-stage HR reforms. Digital readiness also differs substantially: in some administrations, the public workforce already demonstrates strong digital proficiency, while in others digital skills fall well below EU averages[63]. These structural differences determine what becomes feasible, at what pace, and through which institutional mechanisms a digital competency framework can be implemented.

73. **Aligning digital ambition with institutional capacity is essential to avoid overloading HR systems or unintentionally narrowing the talent pool.** When digital expectations are set too high in contexts with low readiness, recruitment can become exclusionary, and HRM systems may be overwhelmed by requirements they are not yet equipped to support. Conversely, administrations with more mature HR processes and stronger digital proficiency can integrate digital competencies more rapidly across the full HR cycle, from job analysis and recruitment to performance and career progression. Credible implementation therefore depends on careful sequencing: countries with weaker digital readiness should prioritise capability-building, while those with stronger foundations may embed the framework more comprehensively from the outset.

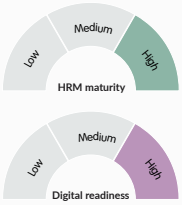
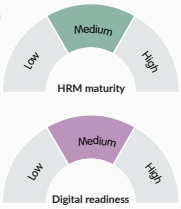
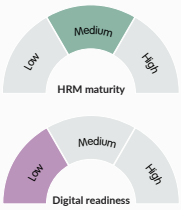
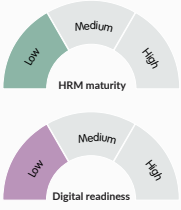
74. **In Romania, the scale of ongoing HRM reform combined with uneven levels of digital readiness across institutions calls for a staged implementation of digital competencies.** While the civil service already operates under a general competency framework and is advancing competency-based HRM reforms, digital skill levels among staff remain uneven and institutional digitalization is highly variable. Introducing digital competency requirements simultaneously across all HR processes risks creating formalistic "tick-box" assessments or unintended consequences – particularly where managers lack the capacity to meaningfully use digital skills assessment results in performance management and staff development. Raising digital expectations too rapidly, especially at entry level, could also unintentionally narrow recruitment pools and reinforce existing staffing bottlenecks. For these reasons, the project methodology prioritized learning and development as a first step, recommending only a limited and proportionate use of digital competencies in recruitment. This phased approach enables capability building before higher-stakes applications of the framework, ensuring sustainable and effective implementation.

61. European Commission. (n.d.). Organisations: managing performance, quality and people 4. Reform Support — Quality of Public Administration: A Toolbox for Practitioners.
62. The World Bank GovTech Maturity Index provides a comprehensive overview of the progress and trends in digital transformation within the public sector across 198 economies. In 2022, Romania was placed in group B, together with Bulgaria, the Slovak Republic, while the majority of European countries were in Group A.
63. Detailed data available in the EU's State of the Digital Decade Report for 2025.

75. **Rather than prescribing a single pathway, the framework supports a phased approach in which implementation can be staged over time and targeted to specific groups of roles.** In administrations with lower HRM maturity, training and development are identified as the most accessible entry point, potentially also allowing to prioritize managers, policy-making roles, or staff directly involved in digital transformation. More advanced applications in recruitment, performance management, and career progression can then be introduced progressively as capacity increases. In more mature HRM systems, a broader and more integrated roll-out across roles is feasible from the outset. This context- and role-sensitive sequencing is intended to enhance feasibility, ownership, and the long-term sustainability of digital competency reforms.

76. **Member States can therefore benefit from a structured decision tool that links HRM maturity, digital readiness and feasible implementation pathways (not only for selecting the pathway, but also for establishing the desired proficiency level, at recruitment and for progression).** The table below proposes four general indicative scenarios commonly encountered across the EU and shows how the proposed general digital competency framework can be introduced in each. These scenarios are not prescriptive but could support administrations choose a pathway aligned with institutional capacity, workforce digital skills and reform priorities. Romania corresponds most closely to Scenario 3, and its piloting experience offers transferable lessons for countries with similar conditions.

TABLE 5: Potential decision matrix

Scenario	Typical characteristics	Recommended pathway
1. 	Competency-based HRM is rooted in HR practice. Managerial capacity to use competency evidence for HR decisions is well established. Digital skills are strong across the workforce. Digital public services are advanced.	Integrate the digital competency framework across the entire HRM cycle from the outset. Use it in job analysis, recruitment, performance, mobility and strategic workforce planning. Link assessments directly to HRMIS and analytics.
2. 	Competency-based HRM exists but is uneven. For example, appraisal systems exist and produce meaningful results, but quality varies, and evaluation capacity is inconsistent. Digital skills are moderate and digitalization is progressing but inconsistent.	Introduce the framework first through job analysis and training. Apply it in recruitment only for baseline competencies. Use it in performance dialogues but avoid linking it to ratings. Expand to mobility and promotion once assessment tools are validated.
3. 	General competency frameworks exist and HRM reform is ongoing. Workforce digital skills lag behind EU averages; digitalization is uneven.	Prioritize learning and development as the primary entry point. Apply the framework in recruitment only for a limited set of essential competencies. Deploy a training platform before expanding into performance or promotion. Sequence implementation so training precedes large-scale assessment.
4. 	Competency-based HRM is minimal. Job profiles are task-oriented. Digital tools and skills are limited.	Use the framework to support basic HRM modernization. Apply it only in learning and development and preliminary job analysis. Avoid using it in recruitment or appraisal until HRM infrastructure and digital tools are available.

Disclaimer of applicability:

77. **The selection of an appropriate implementation pathway is shaped not only by levels of digital readiness and HRM maturity, but also by the normative traditions and structural characteristics of national civil service systems.** In career-based systems with strong legal regulation and standardized recruitment procedures, changes to competency requirements tend to be introduced gradually and must be carefully aligned with statutory norms to avoid procedural bottlenecks or unintended barriers to entry. In contrast, position-based or more flexible HRM systems allow faster experimentation with competency assessment tools across recruitment and performance management. Similarly, administrations where appraisal systems are compliance-driven or loosely linked to development processes may face a higher risk of "tick-box" use of digital competency assessments, reducing their developmental impact. These institutional differences directly influence how the decision matrix should be applied – determining whether early integration across the HRM cycle is feasible or whether a more cautious, capability-building sequence is needed, with learning and development preceding recruitment or appraisal applications.

78. **The considerations regarding implementation in HR processes presented in the subsequent sections 3.2 to 3.6 reflects conditions typically found in Scenario 3 countries, based on the lessons learned in Romania.** In such contexts, a gradual and capability-building approach is needed to avoid creating unintended barriers in recruitment or overburdening existing HRM systems. Member States with higher digital readiness or more advanced competency-based HRM architectures may adopt a more accelerated pathway: introducing the digital competency framework across the full HRM cycle from the outset, applying higher proficiency expectations earlier in recruitment and promotion, and integrating digital competency evidence directly into performance management and strategic workforce planning. The principles in the following chapters should therefore be adapted proportionately to each country's institutional capacity, digital skill levels and reform objectives.

3.2 Job analysis

79. **The introduction of digital competencies into HRM should begin with foundational design processes rather than high-stakes assessment mechanisms.** Within the HRM cycle, job analysis is a foundational process that defines job purpose, tasks, and required competencies, serving as the technical basis for the subsequent, decision-based HR processes[64]. While recruitment, promotion, mobility and performance management apply competency requirements to make formal personnel decisions, job analysis precedes these stages and establishes the competency expectations on which they rely. Job analysis is the natural starting point for applying digital competency expectations in a structured and proportionate way. Civil service systems already use job analysis to define the purpose, tasks and competency requirements of each role. Embedding digital competencies within this familiar process allows institutions to identify which digital skills are expected of all staff and which roles may legitimately require higher proficiency or specialised expertise. In early implementation phases, the primary value of this exercise lies in strengthening workforce planning and learning pathways, while recruitment continues to verify only a basic, common digital threshold. This enables administrations to build capability before digital expectations begin shaping high-stakes selection decisions.

80. **In the Romanian civil service context, a distinction is made between general competencies, which apply to all civil servants, and specific competencies, which apply only to particular roles.** Within this framework, general digital competencies should be treated as transversal requirements for nearly all roles, while specific digital competenecies should be reserved for genuinely specialised roles. General digital competencies described in this framework are relevant, in varying degrees, across the entire civil service and should appear in the "general competencies" section of job descriptions. By

64. Armstrong, M., & Taylor, S. (2020), *Armstrong's Handbook of Human Resource Management Practice*, London: Kogan Page Publishers.

contrast, specialised digital competencies should apply only to a small number of roles in which digital technology is the core of the job (e.g., cybersecurity specialists, data scientists, systems architects). Evidence from piloting in Romania and from similar administrations suggests that most non-ICT roles do not require new "specific" digital competencies; instead, they require adjustments in the proficiency level of selected general competencies, depending on the complexity of their digital tasks. This principle prevents inflation of requirements and supports fair mobility across institutions.

TABLE 6: Key differences between general and specific digital competencies

Applicability

General digital competencies

Required, in varying degrees, for all civil servants to perform effectively in modern administrative contexts.
Example: on cybersecurity - recognizing threats and applying safe digital practices in all the digital tasks.

Specific digital competencies

Relevant only for technical or specialized roles where digital technology forms the core of the job.
Example: developing and maintaining cybersecurity protection government web platforms.

Relation to digital technology

General digital competencies

Technology is a means to perform tasks, communicate, and make decisions.
Example: Using automation tools to prepare reports or administrative acts.

Specific digital competencies

Technology is the core purpose of the role - creating, maintaining, or securing systems.
Example: Designing and programming automation systems that others use to prepare reports.

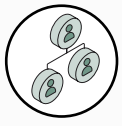
Career trajectory

General digital competencies

Evolves with seniority - from operational use to managerial and strategic digital governance.
Example: Digital Communication - from writing emails to managing online reputation.

Specific digital competencies

Deepens within a narrow technical domain, leading to higher specialization.
Example: Cybersecurity - from checking settings to conducting testing.



Mobility

General digital competencies

Ensures broad mobility across functions - transferable to multiple administrative areas.
Example: Data management skills applicable in HR, procurement, or policy departments across different ministries.

Specific digital competencies

Enables limited mobility within similar technical roles.
Example: A statistician moving to another similar role in a different institution.

Training pathway

General digital competencies

Developed through standard institutional training or guided workplace learning.

Example: "Data Analysis with Excel and Power BI."

Specific digital competencies

Requires specialized certification or intensive industry-recognized training.

Source: Authors' elaboration under Output 3

81. **The introduction of a digital competency framework supports the systematic clarification of digital requirements in job descriptions, moving from generic formulations to structured, competency-based specifications aligned with actual job needs.** Diagnostics conducted in Romania[65] revealed that digital expectations were often expressed through generic references ("good computer skills"), tool-specific mentions ("Microsoft Office", "Teams") or requirements inherited from the incumbent rather than derived from the job itself. Similar issues have been observed in various public-administration reform exercises across Europe. A structured digital competency framework helps address these inconsistencies by translating ad-hoc formulations into clear, task-anchored competencies expressed at appropriate proficiency levels, thereby improving fairness, transparency and coherence across institutions.

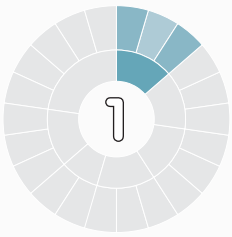
3.3 Recruitment

82. **Recruitment is the first HR process where digital competencies can be systematically applied, but only for a limited subset of baseline skills. At entry to the civil service, recruitment should verify a common** minimum digital threshold applicable across job families, rather than the full digital competency framework. This subset typically corresponds to areas 1–5 (information and data literacy, digital communication and collaboration, content creation, safety, and problem-solving) at a basic level of proficiency. Testing more advanced or role-specific digital skills at entry would be disproportionate, costly, and often disconnected from the context in which those skills will actually be applied.

83. **Entry-level digital testing should remain simple and common for all candidates, with more complex assessments postponed to later stages.** In line with practice in several Member States and at EU level, a common digital-literal or "office tools" test can be gradually reframed as a technology-neutral DigComp-aligned baseline assessment, without multiplying exams or introducing role-specific digital tests at entry. This keeps recruitment manageable and fair, especially for junior roles, while setting a transparent minimum standard for digital readiness that applies to all new civil servants. Keeping entry testing limited to a common baseline is consistent with international practice, including EU recently updated EPSO AD competitions, where all candidates sit the same digital-literacy assessment regardless of their future assignment[66].

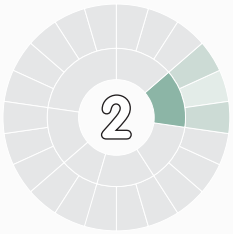
65. Based on the analysis of job descriptions conducted as part of Activity 1 under the TSI project, as reflected in *Output 1*.
66. More information available at: https://eu-careers.europa.eu/en/administrators-ad-generalists.

TABLE 7: Example set of general digital competencies that could be tested in recruitment (as developed for Romania)



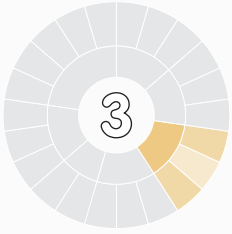
Digital literacy in public administration

Competency	Tested in recruitment
1.1 Searching and accessing data, information and digital content	✓
1.2 Evaluating data, information and digital content	✓
1.3 Managing data, information and digital content	✓



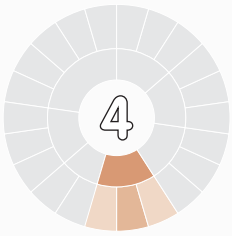
Digital communication and collaboration

Competency	Tested in recruitment
2.1 Communicating, interacting and fostering citizen and businesses participation through digital technologies	✓
2.2 Sharing and collaborating in digital teams in intra and interinstitutional contexts	✗
2.3 Ensuring digital integrity and accountability in public administration	✗



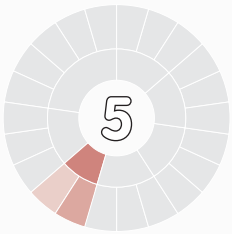
Digital content and digital public services

Competency	Tested in recruitment
3.1 Developing, integrating and re-using digital content	✓
3.2 Delivering and contributing to digital public services	✗
3.3 Ensuring compliance with digital regulatory frameworks and standards	✓



Safe, responsible and sustainable use of resources

Competency	Tested in recruitment
4.1 Protecting devices and infrastructure	✗
4.2 Managing digital identities and protecting personal data and privacy	✓
4.3 Promoting healthy and sustainable digital practices	✗



Problem-solving through digital technologies

Competency	Tested in recruitment
5.1 Managing digital devices, including identifying and managing technical problems	✓
5.2 Using automation tools	✗

84. **Higher digital proficiency and specialised digital skills should be addressed initially through training and job-based selection, not national entry examinations.** In an early implementation phase, roles that require higher digital proficiency (for example, advanced data work in policy units or specialised content management in communication departments) can be addressed through targeted upskilling programs or job-specific selection tests run by individual institutions. Only when a digital-skills assessment platform is mature and widely used should Member States consider integrating differentiated digital profiles into central recruitment exams, and even then, in a proportionate, evidence-based manner.

3.4 Performance management

85. **Digital competencies should enter performance management later, and only in a developmental not punitive way.**[67] Introducing digital competencies into performance appraisal too early, before training opportunities and diagnostic tools are in place, risks unfairness and can undermine trust. A more sustainable approach is to use digital competencies initially to structure conversations about

67. For the detailed recommendations for Romania, please see World Bank, *Recommendations for the introduction and operationalization of the digital competencies in the Romanian public administration*, Output 3, 2025, developed under the TSI project Developing a General Digital Competency Framework for Civil Servants in Romania.

development, not to influence scores or financial rewards. For example, a section of the performance form can record digital learning needs and planned actions ("Digital Development Plan"), without assigning ratings. This allows managers and staff to use the framework to plan future skills without turning digital competencies into a new high-stakes metric.

86. **Digital competencies should not be simply rated by managers within the performance appraisal process.** Unlike general civil service competencies that are often described in behavioural indicators, digital skills require objective, evidence-based assessment to ensure consistency, fairness, and credibility. Relying solely on subjective managerial scoring risks reinforcing the same shortcomings observed in traditional appraisal systems – inflated ratings, inconsistent standards across institutions, and limited diagnostic value for development planning. For this reason, digital competencies should be assessed primarily through dedicated tools and platforms that generate standardized evidence of proficiency (for example, skills testing, simulations, or certified training outcomes. This results should then be interpreted in relation to the individual's role, responsibilities, and broader work context, and used by managers to support holistic developmental discussions and tailored developmental plans, rather than assign scores. This approach ensures that digital competency evaluation remains technically robust, comparable across institutions, and genuinely supportive of capability building, rather than becoming another formalistic rating exercise.

87. **As set out above, if the system is capacitated, digital competencies should be used to inform forward-looking performance dialogues:** identifying capability gaps, supporting learning plans, and linking development actions to future work objectives, rather than contributing to summative ratings or financial consequences. Strengthening the role of digital competencies in performance management could include using certified digital skills evidence to substantiate assessments of selected general competencies or incorporating defined digital proficiency expectations into leadership performance objectives. Any such expansion must remain anchored in development-oriented use and be proportionate to institutional readiness.

3.5 Promotion and mobility

88. **The introduction of digital competencies into promotion and mobility should be phased and conditional on system maturity.** In early implementation stages, career progression mechanisms should remain unchanged, as digital competencies can only be applied fairly once essential enabling conditions are established. These preconditions include universal access to standardized and objective assessment tools, structured training programs aligned with the digital competency framework, and clear mechanisms for the recognition or certification of acquired proficiency. Until these elements are operational, digital competency evidence should be used solely for developmental purposes and should not influence promotion or lateral mobility decisions, ensuring that progression remains equitable and consistent across institutions.

89. **Once system readiness is confirmed (demonstrating that digital skills assessments and certification pathways are fully functional) digital competencies may be integrated into promotion and mobility procedures.** In more advanced contexts across the EU, this may involve requiring candidates for higher-level roles to demonstrate attainment of the digital proficiency level associated with the target position through validated testing platforms, recognized certificates, or scenario-based assessments linked directly to job requirements. Supported by updated HR information systems capable of storing and verifying certified competency data, this approach enables administrations to embed digital capability into career progression in a transparent, comparable, and evidence-based manner, proportionate to institutional maturity.

3.6 Learning and development

90. **Digital competency frameworks in public administration can add impact and value through their translation into concrete implemented actions such as guiding on the job training and further development of professional learning and tools.** International experience shows that the most successful administrations treat digital frameworks as engines for upskilling, not only as instruments for selection or appraisal. This means using the framework to design curricula, structure training catalogues, develop learning pathways, and guide investments in digital academies, rather than tying digital competencies to promotion or pay. In this way, digital capability is built systematically across the workforce before higher-stakes applications are considered.

91. **When applied through learning and development systems, a digital competency framework provides a natural and pragmatic entry point for implementation.** Using the framework first in training allows administrations to prioritise specific target groups - such as managers, policy-making roles, or teams leading digital transformation - and to calibrate learning interventions to clearly identified needs, including AI, data use, cybersecurity, or service digitalisation. This approach enables early, visible results and focuses resources where they are most impactful, while avoiding the risks associated with introducing the framework immediately into high-stakes HR processes. In this context, job analysis plays a complementary role, helping to identify role-specific competency gaps and to fine-tune training content and proficiency targets, without being a prerequisite for initial implementation. As an entry point, targeted application in training supports gradual uptake, institutional ownership, and a structured expansion of digital skills development across the civil service.

92. **In Romania, the framework design explicitly distinguishes between system-level minimum digital competency proficiency thresholds used for recruitment and higher proficiency targets applied for training and development purposes[68].** Minimum thresholds were proposed to safeguard fairness and accessibility in entry competitions, ensuring that overly demanding digital competency requirements do not create unnecessary barriers to recruitment. At the same time, the pilot demonstrated that many institutional roles require digital capabilities exceeding these baseline standards. Consequently, the project recommended that training programs be targeted toward the higher proficiency levels identified through detailed job analysis, calibrated to the actual operational demands of specific institutions and units. This approach ensures that while recruitment remains proportionate and inclusive, workforce development is evidence-based and differentiated, directing investment toward the digital skill levels needed for effective service delivery in each institutional context.

93. **Training strategies should prioritise foundational digital competencies for all staff, using modular and flexible formats.** For the general civil-service population, priority should be given to areas such as information and data literacy, digital communication and collaboration, basic content creation, cybersecurity, and the responsible use of digital tools. These competencies are best developed through short, targeted modules - micro-learning, e-learning, workshops, and blended courses - that map directly to real administrative tasks (e.g., searching for legislation, managing digital files, using collaboration tools, or applying basic cyber hygiene). Grouping competencies into practical themes ("working safely in the digital office", "making decisions with data", "serving citizens online") is often more effective than treating each competency in isolation.

94. **Leadership development in digital competencies is essential for sustained transformation.** Digital transformation cannot be driven solely from IT departments; it requires middle and senior managers who understand data, digital services, cybersecurity, and AI enough to make informed decisions. Leadership-focused training pathways - sometimes branded as "Digital Leadership Academies" -

68. For the detailed recommendations for Romania, please see World Bank, *Recommendations for the introduction and operationalization of the digital competencies in the Romanian public administration*, Output 3, 2025, developed under the TSI project Developing a General Digital Competency Framework for Civil Servants in Romania.

can include topics such as data-driven decision-making, service design and user-centricity, AI ethics and governance, cybersecurity governance, and leading digital change. Including practical projects, peer learning, and mentoring helps ensure that digital leadership development translates into tangible improvements in how institutions operate.

95. **Learning offers should be curated into role-aware pathways that translate assessment results into concrete next steps.** Once a digital competency framework and (ideally) a TNA platform are in place, training provision should be organised into clear pathways that reflect different roles and levels of responsibility. Baseline courses (e.g., cyber hygiene, safe data handling, basic collaboration tools) can be mandatory for all staff, while more advanced modules target analysts, project managers, digital transformation leads, or ICT professionals. Assessment results from self-assessment or testing can automatically route staff into recommended pathways, making the connection between diagnosis and development visible and actionable.

96. **A practical sequencing approach - particularly when fiscal or operational resources are limited – could be to begin with middle-management roles, given their central function in translating strategic directives into operational practice and shaping team-level norms.** Their importance is also underscored in the JRC's Professional Interoperability Profiles (see Box 6 in section 5.2 of this report), which highlight the need for coherent coordination and supervisory capability to sustain digital transformation across organisational units. In parallel, early investment in senior leadership may be essential in highly decentralised systems, where leadership commitment is critical for establishing consistent expectations, aligning fragmented initiatives, and signalling institutional support for new ways of working. Depending on the context, a third group that may merit early attention are digitally intensive or high-impact operational roles, such as those managing core information systems or frontline services that anchor digital workflows; strengthening these profiles can generate quick wins and demonstrate the practical value of the competency framework. Prioritising these groups helps create the enabling conditions needed for broader workforce development and increases the likelihood that subsequent capacity investments will translate into sustained improvements in practice.

97. **While this report focuses on the strategic use of the digital competency framework for learning and development and on the principles guiding assessment and progression across roles, detailed operational examples - including assessment formats, testing methods, and illustrative sample questions for recruitment, promotion, and training - are developed under Outputs 3 and 4 of the TSI project,** which address the legal, procedural, and implementation aspects of operationalizing the framework.

BOX 2: From competency framework to leadership practice: learning must be targeted

Digital competency descriptors only become effective when they are translated into learning content linked directly to public administration mandates, managerial responsibilities, and operational tasks. Generic "digital skills" training has limited impact unless it mirrors the real functions of civil servants: planning reforms, allocating resources, managing data, overseeing digital projects, coordinating institutions, and ensuring accountability.

A relevant example is the recent program for leadership development[70] that was developed by the Bank in collaboration with NACS under the Reimbursable Advisory Services on Support to NACS on HRM reform. The program was piloted in August – December 2025 and covered the full spectrum of competencies applicable to high level civil servants, including targeted digital competencies. These were informed by the analytical work developed under the current TSI project. Program content was developed through three multi-stakeholder visioning and TNA workshops with representatives of central HRM institutions, line ministries, training providers, academia, and civil society. Several strategic drivers - including AI uptake, acceleration of digitalization, anticipatory governance needs, evidence-based policymaking requirements, and fiscal and workforce constraints - were translated into competency priorities. These shaped applied learning areas focused on strategic leadership for digital transformation, data-driven management, governance of digital initiatives, cross-institutional coordination, and organizational change management.

For a dedicated module, the program used this digital competency framework (at that point in time, in a draft status) as a reference for defining learning objectives by systematically contextualizing each descriptor into role-specific learning outcomes, framed around senior management decision-making and reform implementation responsibilities. Participants conducted digital maturity assessments of their institutions, mapped process bottlenecks, distinguished between simple document digitization and true service transformation, and designed institutional digital transformation action plans aligned with strategic goals and governance standards. Case-based exercises and situational evaluations ensured that competency development was consistently anchored in realistic managerial tasks rather than technical system design.

The pilot learning program thus provided clear evidence that targeted development of digital competencies for managers - applied to their concrete leadership mandates - is critically needed. Senior civil servants require structured learning environments that allow them to practice navigating digital reform challenges, not only acquire conceptual knowledge. Linking competency frameworks to role-based learning programs strengthens adoption, accelerates culture change, and equips public administration leaders to effectively govern digital transformation rather than delegating it exclusively to ICT units.

3.7 Creating institutional conditions that support implementation

98. **Successful implementation of a digital competency framework depends on clear institutional mandates and coordination mechanisms.** Even the best-designed framework will have limited impact if no institution "owns" its implementation or if responsibilities are fragmented. A common model in Member States is to designate (i) a national civil service training institution to lead on learning and content, (ii) a central HR authority to align frameworks with career and HR rules, and (iii) a digital or ICT agency to ensure coherence with digital government strategies and specialised ICT roles. Clear role descriptions, formalised in legislation or government decisions, help prevent overlaps and gaps.

99. **A multi-stakeholder governance board can steer implementation, maintain coherence, and resolve trade-offs.** Because digital competencies touch HRM, training, and digital transformation, joint governance is essential. A steering group bringing together the training institution, HR authority, digital agency, and key ministries can approve the implementation roadmap, monitor progress, validate updates to the framework, and arbitrate on issues such as digital requirements for new job families. Including representatives of local government, agencies, and social partners where appropriate reinforces buy-in and ensures that the framework reflects the diversity of public employment.

100. **Phased implementation helps manage risk and build trust across the administration.** Member States benefit from treating digital-competency implementation as a multi-year journey rather than a one-off reform. A typical sequence might start with: (i) integrating digital competencies into job analysis

69. World Bank, *Report with proposal for a Capacity Enhancement Program for senior management civil servants*, developed under the Reimbursable Advisory Service on Support to NACS on HRM reform in Romania, 2025.

and recruitment at a basic level; (ii) developing and scaling digital learning offers and TNA tools; (iii) using digital competencies in performance dialogues as a developmental reference; and (iv) only later integrating them into promotion and mobility criteria. This staged approach allows administrations to test tools, adjust expectations, and build capacity before digital competency evidence begins to influence high-stakes decisions.

101. **Pilot testing and adaptation in diverse institutional contexts is critical to ensure usability, fairness, and scalability.** Before national rollout, Member States should pilot digital-competency concepts and tools and processes in different types of organisations - for example, a central ministry, a regional or deconcentrated service, and a municipality. Feedback from pilots helps calibrate item difficulty, refine guidance, improve user interfaces, and identify institutional bottlenecks, reducing the risk of failure or resistance during broader deployment.

102. **Institutional focal points can act as local champions and coordinators for digital competency implementation.** Many administrations appoint digital transformation officers, digital skills coordinators, or "change agents" within ministries and agencies. These focal points help interpret the framework locally, support job-analysis exercises, promote participation in digital-skills assessments and training, and act as the liaison with central authorities. Investing modestly in such roles often yields large returns in terms of adoption, troubleshooting, and cultural change.

103. **Monitoring and evaluation frameworks are needed to track participation, capability growth, and equity.** Member States should define a small, meaningful set of indicators to monitor the implementation of digital competencies: participation in TNA and training, completion rates, changes in average digital competency scores, closure of identified gaps, uptake of micro-credentials, and progress in high-priority areas such as cybersecurity, data literacy, or AI. Disaggregation by region, gender, age, institution type, and job family helps identify structural disparities and ensure that digital upskilling does not deepen existing inequalities.

104. **Transparency and open reporting can reinforce accountability and collective learning.** Publishing high-level, anonymised data on digital-skills assessments and training - such as the number of civil servants assessed, average competency levels, and participation in key courses - can motivate institutions, support cross-country or cross-sectoral benchmarking, and demonstrate progress to the public. Many administrations already publish dashboards or annual reports on digital skills; extending this practice to public administration staff can signal the seriousness of the digital transformation agenda.

105. **Regular reviews and external feedback loops help keep the system relevant and aligned with evolving EU and national priorities.** Digital technologies, EU regulations (for example on AI, data, or cybersecurity), and citizen expectations evolve rapidly. Member States should therefore plan periodic reviews - every three to five years - of their digital competency frameworks, assessment tools, and learning systems. External evaluations, peer reviews with other countries, and structured consultation with public servants and external stakeholders can provide valuable insights for updating competency descriptors, re-prioritising learning areas, and refining the link between digital competencies and HR processes.

106. **In the medium term, integration with EU-level initiatives can strengthen portability and mutual recognition of digital skills.** As the EU develops common tools and standards for digital skills, including DigComp-based certifications and European-level academies, Member States can align their frameworks and recognition systems accordingly. This supports mobility of public servants across borders, enables shared investments in content and platforms, and ensures that national digital-competency reforms are part of a broader European learning ecosystem.

BOX 3: The pilot process from Romania: the model is relevant but requires flexibility in application

The pilot process in Romania assessed both current and future relevance of each digital competency and proficiency level using a standardized 1–5 scale, where 1 indicated "not relevant" and 5 "critically relevant." Relevance captured not only competencies already applied in daily work, but also those considered important for effective future performance as digitalization progresses, even where enabling systems are not yet fully in place. The comparison of current and future ratings generated a "relevance shift" indicator, highlighting anticipated changes driven by reform and technology adoption.

For analytical purposes, a relevance threshold of 3 was applied to distinguish competencies considered substantively relevant from those of marginal importance, ensuring that conclusions and calibration recommendations reflect competencies with practical significance for job performance and workforce planning.

Pilot testing across Romania's public administration confirmed that the proposed general digital competency framework is relevant across diverse institutional functions, including both core business units (policy development and service delivery) **and support services** (HR, finance, procurement, administration). While core business roles currently face stronger and faster-growing digital demands – driven by citizen-facing transformation pressures – support services also anticipate substantial increases in digitally enabled workflows, particularly in digital transformation and collaboration. Across all functions, foundational digital literacy and digital communication are already essential, reflecting the normalization of digital tools in everyday administrative work.

The pilot further demonstrated the value of a tiered proficiency model applied flexibly rather than uniformly. Basic proficiency (Level A) emerges as universally necessary for all civil servants and should be treated as the baseline across administrations. Intermediate proficiency (Level B) is widely relevant but must be targeted selectively to roles with demonstrable operational, analytical, or coordination needs rather than assigned automatically by grade. Advanced proficiency (Level C) is necessary only for a limited subset of leadership, governance, and strategic coordination roles and should not be mandated broadly across career structures. These findings highlight the importance for Member States of calibrating proficiency expectations through job analysis and evidence rather than applying uniform thresholds. While minimum levels can be defined system-wide – particularly for training prioritization – recruitment thresholds should remain proportionate, focused initially on basic competencies, with higher proficiency levels targeted through learning and development efforts in roles where genuine performance needs exist. This flexible calibration framework enables administrations to address real skill gaps at both system and institutional levels while safeguarding fairness, feasibility, and workforce participation during implementation.

FIGURE 11: Pilot results for future relevance across the 7 competency areas

	A	B	C
Digital literacy in public administration	4.9	4.8	2.1
Digital communication and collaboration	4.8	4.4	3.2
Digital content and digital public services	4.4	4.1	1.7
Safe, responsible and sustainable use of resources	5.0	3.8	1.8
Problem-solving through digital technologies	5.0	4.2	1.0
Digital transformation in public administration	4.9	4.5	1.8
Digital leadership and governance in the public administration	3.8	2.8	2.0
	Competency Level		

A = Basic, B = Intermediate, C = Advanced

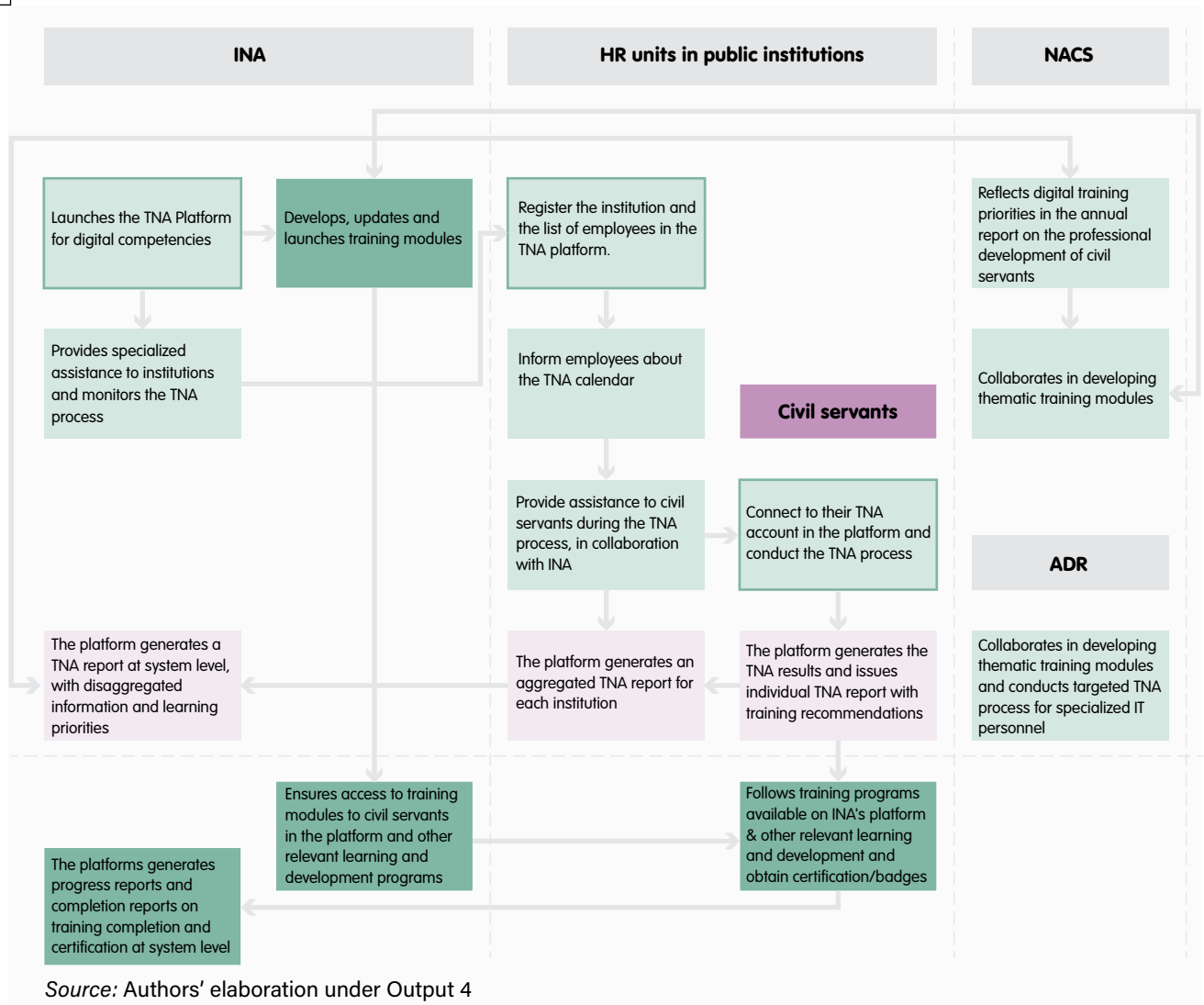
Source: Digital competency pilot / World Bank team calculations

IV. Training Needs Assessment and Learning as the operational backbone

4.1 Redesigning the TNA process for digital skills

107. **A digital TNA platform is the backbone of a modern approach to assessing and developing digital skills across government.** A unified framework, adapted to the realities of public administration, provides a consistent reference for describing what "digital competence" means across job families, institutions and seniority levels. The competency framework offers this shared language by grouping digital skills into seven areas, six applicable to all staff and one specific to managers. International experience shows the practical value of such models: the Basque Country's IKANOS[70], Latvia's Digital Academy[71], and France/Belgium's PIX[72] all use DigComp-aligned frameworks to structure TNA instruments, training catalogues, and certification schemes. In these systems, the framework anchors the entire capability cycle - diagnosis, learning pathways, validation, and workforce planning - ensuring coherence and comparability across the public administration.

FIGURE 12: TNA process for digital competencies recommended for Romania



Source: Authors' elaboration under Output 4

70. IKANOS tool is used for digital self-diagnosis, producing individualized roadmaps that support long-term development. IKANOS official webpage https://ikanos.eus/en/digital-competences/
71. Source: Consultations with the Governmet's Digital Academy, School of Public Administration, Latvia – interviews conducted under the TSI project as part of the research phase.
72. The *PIX* platform, managed by the French Ministry of Education and DINUM, has a dedicated track for public administration. It uses interactive, task and performance-based exercises, such as managing documents, evaluating information sources, or applying cybersecurity practices, to assess actual capability. More information available at https://www.campus.numerique.gouv.fr/pix-fonction-publique-d%C3%A9tat/.

108. **Strengthening TNA requires recognising where Member States sit within the TNA maturity model and shifting toward a strategic, evidence-based approach.** Across the EU, TNA practices range from ad-hoc (Initial stage), to standardised but input-driven (Repeatable), to systems where L&D is integrated with HRM and guided by competency frameworks (Managed), and finally to strategic systems that use TNA to anticipate capability needs and support reform (Strategic stage). Many administrations remain in the Repeatable or early Managed stages, where processes are legally defined but remain formalistic and heavily linked to annual appraisals. For example, Romania was assessed in the "Managed but formalistic" stage[73], with a TNA system that relies on compliance-driven data collection and bottom-up reporting with limited strategic focus. Moving from such a model to a strategic, evidence-based digital capability system requires embedding digital competencies in the TNA cycle, using foresight to anticipate emerging roles, and shifting from perception-based needs identification to structured diagnostics aligned with the digital competency framework.

4.2 Digital TNA platforms: from assessment to actionable learning decisions

109. **A digital TNA platform must provide a comprehensive functionality set that supports assessment, learning, reporting, and governance.** Modern platforms centralise the end-to-end TNA process within a structured, secure environment that is accessible to staff, managers, HR units, and national coordination bodies. Core functionalities include account and role management, adaptive self-assessment tools, knowledge checks, scenario simulations, automated skill profiles, learning pathway generation, dashboards, reporting tools, accessibility features, and audit trails. These functionalities enable consistency, reduce administrative burden, and ensure that assessments produce directly actionable insights. Table 8 below summarises the key functionalities of a full-fledged digital TNA platform modelled on leading EU and OECD systems. However, even the most sophisticated functionality set will underperform without clear mandates and strong safeguards around governance and data use.

TABLE 8: Key functionalities for the TNA platform

Account & role setup	
What it should do	
Identify who is assessed and for which role/profile.	
End-user features	
Single sign-on; select role/unit; short onboarding.	
Admin/HR features	
Bulk user import; role catalog; cohort creation.	
Data captured & outputs	
User ID, role, unit, seniority, consent.	
Transparency & KPIs	
% onboarded; active users by institution.	
Integration safeguards	
SSO with gov ID; RBAC; GDPR consent logs.	

73. World Bank, *Output 1 – Report identifying enabling conditions for Training, Deliverable 1.1 Report on training needs assessment for public administration staff*, developed under the Reimbursable Advisory Services Agreement on Strengthening the INA's Capacities to Improve the Training Policy Framework in the Romanian Public Administration (P169456). Available at: https://ina.gov.ro/wp-content/uploads/2023/03/INA-RAS-Output-1.1-TNA-report-Copy.pdf.

Self-assessment (Likert)

What it should do

Rapid baseline against the national digital CF.

End-user features

10–15 min questionnaire; progress bar; save & resume.

Admin/HR features

Editable item bank; routing by role; A/B test items.

Data captured & outputs

Raw item responses; sub-scores by comp

Transparency & KPIs

Completion rate; median score by domain/role.

Integration safeguards

Item versioning; accessibility (WCAG).

Knowledge checks

What it should do

Objective benchmark on core topics (e.g., cyber).

End-user features

Short quizzes; immediate feedback.

Admin/HR features

Question pools; randomization; pass marks.

Data captured & outputs

Scores; pass/fail; attempt history.

Transparency & KPIs

Pass rates; retake rates; time-to-pass.

Integration safeguards

Proctoring options (if needed).

Task/ mini-simulations (optional pilots)

What it should do

Evidence of “can-do” skills for selected roles.

End-user features

Scenario tasks; sandbox exercises.

Admin/HR features

Assign to target roles; scoring rubrics.

Data captured & outputs

Scenario scores; artifacts (files, logs).

Transparency & KPIs

assessed; avg score vs benchmark.

Integration safeguards

Limited to selected competencies

Automated skill profile

What it should do

Turn results into a clear skills map.

End-user features

Personal dashboard; strengths/ gaps by competence/level.

Admin/HR features

Configurable thresholds/levels (DigComp-aligned).

Data captured & outputs

Profile level per domain; gap list vs role.

Transparency & KPIs

Share of staff meeting baseline by unit/role.

Integration safeguards

Clear explanatory text; printable PDF.

Learning pathway & nudges

What it should do

Route gaps to training offers.

End-user features

Recommended courses (internal/external); enroll button; calendar; reminders.

Admin/HR features

Curate catalog; map courses to gaps; micro-nudge engine.

Data captured & outputs

Click-throughs; enrollments; completions.

Transparency & KPIs

Enrollment → completion conversion; time-to-enroll.

Integration safeguards

LMS/HRIS API; vendor metadata.

Individual report

What it should do

Give each user an actionable plan.

End-user features

Downloadable report; "what to do next."

Admin/HR features

Report template branding; manager view (opt-in).

Data captured & outputs

PDF/HTML report; version timestamp.

Transparency & KPIs

% who open/download report; follow-up uptake.

Integration safeguards

Privacy by default; user controls sharing.

Manager/Institution dashboards

What it should do

Support team-level planning.

End-user features

(If enabled) team snapshot for supervisors.

Admin/HR features

Aggregated heatmaps by unit/role; filters; export.

Data captured & outputs

Anonymized aggregates; suppression rules.

Transparency & KPIs

Coverage by unit; avg gaps; course uptake.

Integration safeguards

System-level transparency

What it should do

Provide public, system-wide metrics.

End-user features

Public “stats” page with high-level figures.

Admin/HR features

Configurable open-data feed; periodic publication.

Data captured & outputs

Counts only (exclude any personally identifiable information)

Transparency & KPIs

How many tested (12 mo); how many trained; avg completion time; % at/above baseline; courses per user.

Integration safeguards

Open data; release calendar.

Certification / micro-badges (optional)

What it should do

Recognize achievement where relevant.

End-user features

Digital badges/certificates; wallet download.

Admin/HR features

Define criteria; verify; revoke.

Data captured & outputs

Issued credentials registry.

Transparency & KPIs

badges issued; validity; renewal rate.

Integration safeguards

Standards-aligned badges; audit trail.

Notifications & comms

What it should do

Drive adoption and completion.

End-user features

Email/SMS/app reminders; “What’s new” updates.

Admin/HR features

Campaign scheduler; templates; cohorts.

Data captured & outputs

Open/click rates; reminder cadence.

Transparency & KPIs

Completion uplift vs control.

Integration safeguards

Opt-out controls; language variants.

Accessibility & language

What it should do

Ensure equitable access.

End-user features

RO/EN UI; screen-reader support; low-bandwidth mode.

Admin/HR features

Content QA; glossary.

Data captured & outputs

Accessibility test logs.

Transparency & KPIs

Accessibility conformance score.

Integration safeguards

WCAG 2.1 AA compliance.

Audit, logs & security

What it should do

Guarantee integrity and compliance.

End-user features

Session timeouts; device warnings.

Admin/HR features

Full audit logs; role-based data access.

Data captured & outputs

Event logs; consent/audit exports.

Transparency & KPIs

Mean time to resolve incidents.

Integration safeguards

ISO27001 controls; DPIA; retention policy.

Source: Authors' elaboration under Output 4

110. **Clear governance, institutional ownership, and strong data-protection safeguards are prerequisites for sustainable platform operation.** International practice shows that digital learning platforms thrive when roles are clearly allocated and backed by stable mandates. International practice shows that platforms thrive when roles are clearly allocated and backed by stable mandates. A common model is tripartite: a national civil-service training institution leads learning design and platform operations; a central HR authority ensures alignment with competency frameworks and HR processes; and a national digital agency maintains coherence with cybersecurity, interoperability, and ICT-professional pathways. This arrangement ensures methodological continuity, strategic alignment, and technical integrity. Equally important are robust data-governance safeguards: controlled access rights, DPIAs, GDPR-compliant processes, audit logs, and explicit rules separating TNA diagnostics from performance appraisal. Countries such as France, Latvia, and Canada have demonstrated that maintaining this developmental, not punitive, approach is essential for trust, accuracy of self-assessment, and high participation rates.

111. **Platform-generated insights must be translated into decision-oriented learning, reporting, and planning mechanisms.** The value of a digital platform lies not only in its assessments but in the learning and workforce-planning actions it enables. At individual level, platforms generate personalised competency reports and tailored learning pathways, directing staff to specific modules mapped to their gaps. At institutional level, dashboards provide benchmarks, highlight persistent gaps, and support the development of costed training plans. At system level, aggregated reports inform budget allocations, training procurement, national priorities, and long-term reform planning, mirroring Spain's portfolio-based approach under INAP or Latvia's system-wide dashboards. To support transparency

TABLE 9: Proposed minimum set of indicators for monitoring

Indicator	Description	Disaggregation
Participation rate	% of civil servants who completed TNA or upskilling modules	Region, institution, gender, function
Completion rate	% completing all required digital skills training modules	Institution, gender, role type
Gap-closure rate	% reduction in employees below baseline digital skills (pre/post TNA)	Region, institution, seniority
Average score improvement	Change in digital competency score after upskilling interventions	All cohorts
Time-to-complete (median)	Median days from TNA assignment to module completion	Institution, region
Remediation success rate	% completing follow-up/remediation within 30–60 days	Thematic area, region, role, gender
Advanced skills enrolment	% enrolling in elective/advanced digital modules	Region, role, institution
Thematic gap rate	% of staff below baseline in key thematic areas grouping different competencies (e.g., cybersecurity, data analysis, AI,)	Thematic area, role, institution
Most-improved thematic area	The competency area showing the largest average score increase post-upskilling	Thematic area, institution
Persistent gap area	The skill area with lowest gap-closure rate, signaling need for focused action	Thematic area, institution
Micro-credential/ badge diversity	Number and distribution of different digital badges or micro-credentials earned	Badge type, institution, region
Voluntary elective participation	% of staff opting for non-mandatory digital upskilling beyond baseline modules	Institution, role, level
Satisfaction/ feedback score	Staff satisfaction with training content and usefulness	Institution, region
Certification rate	% earning recognized digital credentials (badges, certificates)	Role, gender, institution, sector

Source: Authors' elaboration under Output 4

and monitoring, platforms should capture a minimum set of indicators, participation, gap closure, remediation success, completion rates, and skill gains, as summarized in Table 8 below.

112. **Diverse assessment methods must be integrated to ensure validity, reliability, and relevance across the workforce.** Different tools serve different purposes: self-assessments reveal perceived capability levels and quickly scale across government; knowledge tests provide objectivity; task-based assessments offer high validity for job performance; and emerging conversational AI tools may complement early-stage diagnostics where appropriate and ethically compliant. The selection and combination of these methods should be guided by the competency framework, role characteristics, and institutional maturity. Table 10 summarises advantages, limitations, and best uses for each method, drawing on OECD and EU examples. These methods only add value, however, when their outputs are systematically connected to learning offers, recognition mechanisms and HR decisions through the platform and associated processes described above.

TABLE 10: Digital-skills assessment methods in public administrations: advantages, limitations, OECD/EU examples, and best HR uses (including hybrid approaches)

Assessment Method	Advantages	Limitations	OECD/EU Examples	Best uses in HRM
Self-assessment	**Scalable and low** cost for whole-of-government **Good for baseline** TNA and awareness **Engages staff** with dashboards/ roadmaps **Easily localized** to civil-service use cases	Subjectivity and bias (over/under-estimation) Limited validity if descriptors vague Needs triangulation with other evidence	Basque Country " IKANOS self-diagnosis tool PIX (France/ Belgium) self-reflection JRC DigCompSat item bank	Training needs assessment (baseline) Awareness raising & portfolio planning Annual/regular workforce surveys
Knowledge-based test	**Objective scoring** and **comparability** across cohorts Efficient **online proctoring** Works well for **compliance-critical** areas (e.g., cybersecurity)	Tests knowledge rather than applied ability Requires item design and refresh May disadvantage test-anxious participants	**PIX** (France/ Belgium) **OECD Education & Skills Online** (PIAAC-linked)	Compliance and screening for compulsory domains Entry/ placement tests for targeted courses Monitoring progress in foundational skills
Task-based/ Performance assessment	**High validity** for job performance **Provides evidence** of can do™ skills Supports portfolio-style **credentialing/**micro-certificates Strong fit for advanced or **specialist roles**	High cost/logistics (scenario design, scoring, proctoring) Slower to deploy at scale Requires equipment and accessibility considerations	Basque Country BAIT certification (proctored) IT Txartela exams in Spain	Selection for advanced/ specialist roles Credentialing/ certification Program evaluation after training
Conversational (Chatbot-based) assessment	**Engaging UX** for enhanced uptake **Adaptive probing** to accurate identification of competency level **real-time feedback** to managers and employees **Low marginal cos**t at scale	Validity/reliability not on par with task tests; prompt - sensitivity/ "hallucinations"; Unsuitable for high-stakes certification	Early experiments - Switzerland "DigiBot" university pilot Early DDaT-aligned prototypes (pilot stage)	Formative diagnostics (onboarding, pulse checks) **Can complement**, not replace, other methods.

113. **A digital learning platform becomes meaningful only when assessment results feed directly into learning, recognition, and career development ecosystems.** International evidence shows that platforms create value when they serve as the engine of continuous capability development, routing staff into recommended learning opportunities, linking results to curated course catalogues, and supporting recognition through micro-credentials or digital badges. France's PIX, Italy's "Deep Skills" initiative, and Canada's Digital Academy demonstrate how platform results can feed into everything from basic digital literacy modules to advanced academies in data science, cloud services, cybersecurity, or service design. When integrated effectively, platforms support both developmental objectives and broader workforce-management needs, including strategic HR planning, role redesign, and updates to national competency frameworks.

114. **Although AI is sometimes framed as a separate upskilling workstream, in practice AI-related competencies are most effectively assessed as part of broader digital competency evaluations.** Existing assessment systems typically rely on structured questionnaires, self-assessment tools, and scenario-based tests to identify proficiency gaps in areas such as AI literacy, data use and ethics, and algorithmic decision-making. Embedding AI-related checks within the general digital competency framework ensures that public servants are assessed coherently and consistently alongside other core digital skills, while still allowing institutions to flag more advanced or role-specific AI capability needs. At the same time, this assessment approach does not preclude targeted AI training from being designed and delivered as a distinct learning pathway. On the contrary, it enables administrations to use assessment evidence to prioritize specialized AI learning interventions for selected roles and functions, while maintaining overall coherence with the wider digital skills framework and evolving requirements for responsible and lawful use of AI in the public sector.

4.3 Certification, validation and recognition of digital competencies

115. **A coherent certification and recognition ecosystem is essential for embedding digital competencies in HRM processes.** A digital competency framework remains a descriptive tool unless Member States establish robust mechanisms to verify skills, recognise prior learning, and translate credentials into recruitment, training, mobility and career development. Administrations typically encounter parallel pathways - university diplomas, vocational qualifications, vendor certifications, online micro-credentials, and CPD attestations from public training institutions - that rarely map to a shared reference model. This fragmentation creates inefficiencies: some candidates are over-tested despite holding equivalent qualifications, while others cannot demonstrate skills because their prior learning lacks formal recognition.

116. **DigComp-based certification and recognition models increasingly form the backbone of digital-skills recognition in some Member States.** The adoption of DigComp and national variants has created a shared vocabulary for describing and measuring digital competence, enabling alignment between certification schemes, training curricula, university modules, and public administration competency frameworks. When systems use a unified reference model, HR units can interpret credentials consistently, institutions can compare skill profiles, and civil servants benefit from transparent pathways linking informal learning, formal validation, and career development. Without such alignment, recognition systems remain ad hoc, undermining HRM coherence and limiting labour mobility within the public sector.

117. **In Romania, ICDL/ECDL remains an important component of the ecosystem, but it cannot serve as the sole standard. ICDL certificates provide verification of foundational digital skills and are often mapped to DigComp across Europe.** ICDL certificates provide verification of foundational

digital skills and are often mapped to DigComp across Europe. However, modern digital capability extends well beyond office tools. Public servants increasingly require competency in data literacy, cybersecurity awareness, content creation, digital communication, responsible AI use, and problem-solving in digital systems. Member States therefore integrate ICDL as one recognised pathway within a broader certification architecture, rather than as the exclusive benchmark.

118. **Higher education institutions represent an underutilised channel for recognising digital skills already acquired by future public servants.** Universities across Europe offer IT degrees, interdisciplinary programs (informatics, digital governance, e-government), and modules embedded in public administration, law, or economics degrees. These modules often align - implicitly or explicitly, with DigComp areas such as data literacy, content creation, problem-solving, or digital safety. Yet in some Member States, such competences do not automatically translate into recognition within civil-service recruitment or HR systems. By referencing or making links to DigComp in Diploma Supplements or through micro-credentials, universities could become active contributors to national digital-skills recognition ecosystems.

119. **Non-formal and online learning pathways provide flexible and scalable options but require structured validation mechanisms.** Online learning platforms (e.g., Coursera, edX, Udemy, Open University micro-credentials), vendor academies (Microsoft, Google, Cisco), and private training providers now offer hundreds of digital-skills programs aligned with DigComp or sectoral standards. These programmes are widely used by civil servants because they are accessible, modular, and up-to-date. Without official validation routes, their certificates often cannot be recognised formally in HRM processes. Member States therefore need mechanisms to verify relevance, ensure quality, and map outcomes to national public-administration frameworks.

4.4 Institutionalisation and phased adoption of digital-skills TNA systems

120. **Clear institutional ownership is essential for the sustainable delivery of a digital-skills TNA system.** A platform-based TNA process can only function if a single institution is explicitly mandated to lead its design, operation, and evolution. This institution must act as the Product Owner of the digital TNA platform, hold a multi-year budget, and maintain a dedicated team responsible for platform governance, content development and user support. To ensure coherence across the HRM system, a central HR authority should safeguard the alignment between the digital competency framework and broader HR processes, including recruitment, mobility, and workforce planning. In parallel, a national digital body should update digital-skills priorities (for example, in cybersecurity, AI, or data governance), ensure that emerging technological standards are reflected in assessments, and coordinate the upskilling of specialised ICT roles through a separate but connected capability stream. A joint governance structure, bringing together HR, digital, and training mandates, should oversee the product roadmap, adoption targets, and periodic validation of expected digital proficiency levels by role.

121. **Integrating assessment with learning and recognition systems is critical to translate diagnostics into development.** A digital TNA platform must be embedded within a broader learning ecosystem so that assessment results automatically generate actionable next steps. This requires a structured, competency-tagged training catalogue that spans national training institutions, universities, and EU-level resources such as the Interoperable Europe Academy [74]. Role-aware learning pathways should be auto-generated after each assessment, combining mandatory baseline modules (for example, annual cybersecurity hygiene with simulated phishing) with elective deepening options tailored to individual

74. Interoperable Europe Academy, developed by the European Commission, is a model initiative supporting digital skills for interoperability for civil servants across the EU. The Academy provides online courses, workshops and webinars that focus on general and advanced digital competencies required to implement interoperability policies and drive digital transformation in government settings. https://interoperable-europe.ec.europa.eu/collection/interoperable-europe-academy.

profiles. Micro-credentials and digital badges can reinforce motivation and provide incremental recognition, remaining separate from formal appraisal at first but designed to integrate with career development and talent-mapping systems as the ecosystem matures. Training should be organized by thematic clusters, such as data literacy, AI awareness, digital communication, or secure digital practices, reflecting the interdependent nature of digital tasks in public administration rather than a one-competence-per-module model.

122. **Gradual and iterative implementation reduces risks, builds trust, and supports system-wide adoption.** Early phases should focus on piloting the platform and associated tools, testing assessment items, dashboards, and user journeys in diverse institutional environments. Feedback from these pilots should be used to refine guidance, simplify user experience, and improve technical robustness. Institutions should designate focal points responsible for communication, troubleshooting and uptake, and run short, thematic campaigns, such as cybersecurity month or AI awareness cycles, to encourage participation. A monitoring framework with a small, meaningful set of indicators (including participation, completion, gap-closure, score improvement, remediation rates, advanced-skills enrolment, persistent gaps, badge uptake, satisfaction and certification rates) should track both equity and impact. Disaggregation by region, institution, role and gender supports transparency and ensures that digital capability development does not widen existing disparities.

123. **A phased roadmap enables institutions to build stable capacity and ensure long-term institutionalisation. A five-phase model offers a practical structure for sequencing activities:**

- **Phase 1. Governance setup and decision on delivery model (months 0–3):** formalise institutional mandates, establish the governance board, and choose between delivery models (in-house development, outsourced build, or hybrid).
- **Phase 2. Detailed design and prototyping (months 3–8):** prepare functional and technical specifications, develop the initial item bank, prototype key workflows, and review data-protection requirements.
- **Phase 3. Platform development and pilot deployment (months 8–16):** build the full platform, conduct multi-institution pilots with several thousand users, refine assessment logic and dashboards, and document implementation guidance.
- **Phase 4. National rollout and capacity building (months 16–28):** extend platform access across the civil service, embed the TNA cycle into regular HR processes, integrate with learning-management systems, and issue annual individual, institutional and system-level reports.
- **Phase 5. Continuous improvement and transparency (months 28–36 and ongoing):** establish periodic review cycles, update competency descriptors and item banks, integrate micro-credential ecosystems, and progressively align with EU-level digital academies and certification frameworks.

124. **When these conditions are in place, digital-skills TNA becomes a permanent, trusted component of strategic workforce development.** Fully institutionalised systems shift from reactive training procurement to sustained capability-building aligned with national digital-government priorities. Over time, the digital TNA **platform** becomes a core instrument for strengthening the digital maturity, resilience and interoperability of public administrations, ensuring that workforce development keeps pace with evolving EU policy, technological change, and the growing complexity of digital public services.

V. From lessons learned to opportunities

125. **This section distils a set of key lessons from the assessment and design process conducted in Romania**, building upon recurring patterns observed across outputs, and highlighting where specific design and sequencing choices proved critical for feasibility, legitimacy, and institutional uptake. The lessons are therefore intended to be read collectively, as mutually reinforcing insights into how digital competency frameworks function in real public-administration environments.

126. **Taken together, the lessons also point to a common set of system-level risks that can undermine impact if not addressed holistically.** These include treating competency frameworks as static or purely technical instruments, underestimating the importance of HR integration and learning systems, applying uniform proficiency requirements without role differentiation, or replicating European reference standards without sufficient adaptation to administrative realities. The Romanian experience shows that these risks do not arise from individual design flaws, but from misalignment between frameworks, governance arrangements, HR processes, and institutional maturity. For this reason, the lessons emphasise coherence, adaptation, and sequencing as cross-cutting implementation principles, rather than prescribing a single operational blueprint, leaving Member States flexibility to translate them into concrete actions aligned with their own contexts.

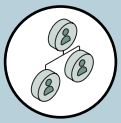
127. **Given the pressing challenges raised by the fast pace of digital transformation and AI uptake, the lessons learned highlight the need for targeted and effective operationalization of the digital competency framework.** In contexts with uneven HRM maturity and fragmented digital capability – such as those identified in Romania at baseline – failing to apply a targeted and sequenced approach carries measurable risks. Without a coherent digital competency framework linked to HR processes, skills gaps remain largely invisible, preventing targeted training, differentiated workforce planning, or evidence-based prioritisation of investment. The Romanian diagnostics showed that, in the absence of structured competency data, training provision tends to be supply-driven, generic, and weakly aligned with job requirements, while digital-system investments proceed without corresponding capability development[75]. This misalignment increases the risk of underutilised platforms, uneven adoption across institutions, and limited return on investment in both digital infrastructure and skills programmes. More broadly, where digital competencies are not operationalised through HRM tools, administrations struggle to move beyond awareness-raising towards sustained behavioural change, limiting their ability to effectively and efficiently develop and deploy national and EU-funded digital investments and to meet evolving regulatory and governance requirements, including in areas such as cybersecurity, data protection and AI oversight.

128. **The nine lessons summarized in this section show that the potential impact of the digital competency framework for the public administration can be maximized if the framework is anchored in a solid standard – such as the European DigComp framework, adapted to public-administration realities, differentiated by proficiency, integrated into HRM and learning systems, complemented by professional ICT capacity, and governed through adaptive mechanisms.** Treating any of these elements in isolation increases the risk of limited uptake and weak returns on investment in digital skills and systems.

75. As detailed in Output 1 under the TSI project- World Bank, Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service: Taking into Account Relevant Policies at the National and European Union Levels, 2025. Available at: https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745.

FIGURE 13: Key lessons learned from the Romanian assessment and design process

Lesson 1:
A core set of general digital competencies can be justified as common across EU public administrations



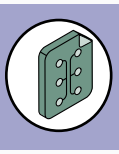
Lesson 2:
DigComp provides the necessary European reference standard, but should be adaptatively tailored for the public administration, using a co-design process

Lesson 3:
DigComp is the foundation, while digital transformation and digital leadership competencies should be seen as system requirements, not optional add-ons

Lesson 4:
Proficiency differentiation is essential to fairness and feasibility

Lesson 5:
AI competency needs to be embedded in digital competency frameworks, but managed as an adaptive layer responding to rapid technological and regulatory change

Lesson 6:
Framework impact depends on HR integration, not only on technical design



Lesson 7:
Learning systems should lead reform sequencing

Lesson 8:
General digital upskilling cannot substitute professional ICT capacity

Lesson 9:
System reform benefits from phased, adaptive governance

Source: Author's elaboration

5.1 Key lessons learned

Lesson 1 – A core set of general digital competencies can be justified as common across EU public administrations

129. **The needs assessment conducted under Output 1 demonstrated that core digital competencies apply consistently across diverse public-administration functions, regardless of sector, organisational mandate or institutional size.** The combination of large-scale NLP-assisted job analysis and structured interviews confirmed that digital tasks are now embedded in essentially all categories of administrative work: policy design, service delivery, case management, inspection, support units (HR, budget, procurement). This empirical finding validates the assumption underpinning EU reference frameworks, such as DigComp 3.0 that digital competence is a transversal workforce capability rather than the domain of ICT units alone; this is relevant also for achieving the targets set under the Digital Decade Policy Programme[76], which call for a substantial increase in the share of adults with basic digital skills and a significant expansion of digitally proficient professionals[77]. Ensuring that digital competence is developed across the full breadth of the public administration workforce will be essential for contributing to, and benefiting from, progress toward these 2030 objectives.

130. **At the same time, the analysis showed that while the relevance of digital competencies is rather universal, required proficiency levels vary significantly by role and function.** This distinction justified the project's choice to design a general framework applicable across the whole civil service, but calibrated through differentiated proficiency levels rather than uniform thresholds. The lesson for other Member States is that a single digital competency framework can credibly cover the **full** administration, provided that implementation mechanisms allow structured differentiation by job complexity and responsibility.

131. **The core set of digital competencies required of civil servants is remarkably similar across Member States.** The review of international experience across Outputs 1 and 4 provided the evidence that digital competencies can be structured along similar pillars. This opens up valuable opportunities for collaboration, allowing countries to share models, methodologies, and tools for assessment and learning. The use of existing European cooperation networks such as the Expert Group on Public Administration and Governance - Reform Support, the Network of Directors of Institutes and Schools of Public Administration (DISPA), the European Public Administration Network (EUPAN)[78] and the Digital Europe Programme, as well as digital skills platforms already developed by the European Commission, can accelerate collective progress.

76. https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme.
77. The ambitions set for the area of skills in the Digital Decade are that, by 2030, at least 80% of all adults should have at least basic digital skills, and that there should be 20 million employed ICT specialists in the EU, with increased women's participation. Information available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe.
78. https://www.eupan.eu/.

Lesson 2 - DigComp provides the necessary European reference standard, but should be adaptatively tailored for the public administration, using a co-design process

132. **The assessment and design processes conducted under the TSI project confirmed that DigComp is a robust and internationally legitimate reference standard for structuring general digital competencies in public administrations.** Its comprehensive coverage of digital domains aligned closely with the transversal skill needs identified through Output 1 across Romanian institutions. Anchoring the national framework in DigComp ensured full coherence with EU digital-skills policy initiatives, including the Digital Decade targets, the European Skills Agenda, and emerging certification and micro-credentialing schemes – safeguarding interoperability with future EU-wide learning platforms and mutual recognition efforts.

133. **However, the design work under Output 2 demonstrated that DigComp needs to be functionally adapted so that it can be applied to the civil service.** As a generic, transversal framework, DigComp requires adaptation to specific use contexts, and hence was used as a starting point. Public administration operates with strategic policy objectives under legal mandates, compliance frameworks, accountability obligations and organisational hierarchies that are not captured specifically in DigComp. Consequently, many competencies required adaptation, restructuring, expansion or additions to incorporate operational realities such as institutional data governance, interoperability obligations, regulated service delivery workflows, procurement and audit constraints, and ethical oversight of AI systems. This resulted in a systematic differentiation between "adapted," "modified," and "new" competencies within the proposed framework, ensuring fidelity to DigComp while rendering the model administratively usable.

134. **The development of the proposed General Digital Competency Framework for the Public Administration drew on a range of European and international reference sources to ensure methodological robustness and policy coherence.** DigComp 2.2 (updated as 3.0) served as the primary structural backbone, providing the common EU taxonomy and proficiency logic for general digital skills. Complementary inputs were drawn from the OECD *Framework for Digital Talent and Skills in the Public Sector* and the OECD report *Developing Skills for Digital Government*, which informed the inclusion of governance, delivery and leadership dimensions specific to the public sector. UNESCO's *Artificial Intelligence and Digital Transformation Competencies for Civil Servants* provided analytical grounding for integrating ethical, attitudinal and responsible-AI dimensions into the competency model. Practical national models, notably Italy's *Syllabus for Digital Skills for the Public Administration* and Spain's *Digital Competencies of Public Employees: Reference Framework*, were reviewed to extract implementation approaches linking competency frameworks to training platforms, certification pathways and HR processes[79]. Together, these sources ensured that the Romanian framework aligns with relevant EU and international standards while reflecting operational lessons from comparable public administration reforms.

135. **The experience confirms a key transferability lesson for Member States:** DigComp should remain the common European backbone for public administration digital competency frameworks, but impact depends on translating that standard into sector-specific language tied to civil service functions, legal responsibilities, and HRM processes. Without such adaptation, frameworks remain pedagogical tools rather than operational HR instruments – disconnected from recruitment standards, training curricula, and competency-based career development systems that underpin real administrative capacity building.

79. Cited sources available at: DigComp 3.0, the OECD Framework for Digital Talent and Skills in the Public Sector, OECD report Developing Skills for Digital Government, UNESCO's Artificial Intelligence and Digital Transformation Competencies for Civil Servants, Italy's Syllabus for Digital Skills for the public administration, Spain's Digital Competencies of Public Employees: Reference Framework.

136. **The Romanian experience supports a broader conclusion: EU alignment is achieved through adaptation and localisation, not replication.** Maintaining conceptual consistency with DigComp 3.0 ensured coherence with EU digital-skills policy and mutual learning across Member States, but operational usability depends on adapting terminology, performance expectations and examples to real civil-service mandates. Similarly, linking general digital competencies to professional ICT frameworks such as the e-Competence Framework (e-CF) and the European Cybersecurity Skills Framework (ECSF) demonstrated that coherent adaptation across frameworks is possible without losing standardisation benefits.

137. **The TSI project also demonstrated that the design and any future adaptations of the proposed model strongly benefit from a collaborative, participatory design process rather than a purely expert-driven exercise.** Under Output 1, the Romanian framework was shaped through structured engagement with civil servants and managers from multiple institutions, using interviews, working groups and job-task mapping workshops to test the practical meaning of proposed competencies against real operational workflows. This iterative consultation process allowed descriptions and proficiency expectations to be adjusted to reflect institutional language, service delivery realities and existing HRM practices, ensuring that the final framework was both technically robust and administratively usable. The experience confirms that co-design with practitioners is essential for transforming abstract competency standards into operational instruments that institutions recognize as legitimate and relevant.

Lesson 3 - DigComp is the foundation, while digital transformation and digital leadership competencies should be seen as system requirements, not optional add-ons

138. **Areas 1 - 5 of the proposed framework remain closely aligned with DigComp and define the transversal digital skill foundation required across the civil service.** These areas (digital literacy, communication and collaboration, digital content and public services, safe and responsible digital use, and problem solving) correspond directly to the competency domains of DigComp 3.0 and capture the skills needed to operate effectively in digitally mediated administrative environments. Evidence from the assessment phase confirmed that these competencies are relevant across all institutional functions, from policy-making roles to frontline service delivery and internal support services, forming a shared baseline for modern public administration work.

139. **The introduction of Area 6 – Digital Transformation reflects the recognition that modern public administrations require competencies that go well beyond the effective use of digital tools.** Drawing on OECD and UNESCO frameworks, the Romanian model embedded capabilities related to digital transformation, to enable process redesign, innovation management, agile delivery, automation, and the scaling of digital initiatives. These competencies enable civil servants not only to work in digital environments, but to actively identify opportunities for digitalization, design and test new service solutions, evaluate transformation investments, and coordinate implementation across organizational boundaries. Importantly, these competencies are treated as distinct from general innovation or change-management competencies typically found in civil-service leadership or management frameworks. While traditional competencies address generic leadership behaviours - such as initiative, adaptability or team leadership, Area 6 captures the application of these behaviours in explicitly digital contexts.

140. **Area 7 – Digital Leadership and Governance - addresses an additional, frequently overlooked system need: the digital capability of managers and senior coordinators responsible for workforce development, performance oversight, data governance, regulatory compliance, and ethical use of emerging technologies such as AI.** Competencies in this area cover digital workforce planning, learning ecosystem management, performance management in the context of digital workflows, data

governance frameworks, cybersecurity oversight, regulatory compliance (including GDPR and the AI Act), and strategic foresight. These are not specialist ICT functions but core leadership responsibilities in a digitally enabled administration. Their explicit inclusion ensures that digital accountability is anchored at decision-making levels rather than delegated entirely to technical teams. The lesson emerging from the TSI experience is that without formally defining and developing managerial digital competencies, public administrations risk building digital infrastructure without the governance capacity needed to operate it responsibly and effectively.

141. **The inclusion of Area 7 does not imply that managers are disengaged from the foundational competencies of Areas 1–5.** On the contrary, managerial and senior roles are expected to demonstrate increasing levels of proficiency in digital literacy, communication, content creation, safety and problem solving. In those areas, progression in proficiency reflects greater technical depth in applied use - for example, interpreting operational data dashboards, using effectively digitally enabled workflows, ensuring compliance with cybersecurity practices - without entering the specialized development or operating functions reserved for professional ICT staff. Managers must therefore master the use and oversight of digital systems rather than their technical design or implementation. However, this progression of technical proficiency alone is not sufficient to capture the distinctive leadership responsibilities of managerial roles in digitally transforming administrations. Competencies relating to organisational innovation, strategic change management, service transformation, workforce development, governance oversight and ethical accountability cannot be subsumed into general competency domains such as "initiative," "leadership," or "problem solving" without losing their digital specificity. For this reason, Area 7 shows that leading change in a digital public administration requires a qualitatively different set of competencies than merely applying tools more expertly. They address the capacity to steer institutional redesign, manage cross-functional digital initiatives, govern emerging technologies such as AI, and build organisational learning systems.

Lesson 4 - Proficiency differentiation is essential to fairness and feasibility

142. **The TSI work confirmed the value of structuring digital competencies across different proficiency levels, streamlined in three proposed levels (A-B-C), while differentiating their application between Areas 1–6 and Area 7.** In Areas 1–6 proficiency progression reflects mainly the increasing technical depth, complexity of tasks and autonomy of use required by different roles, without entering the specialised ICT domain. In contrast, in Area 7 – Digital Leadership and Governance – the proficiency levels represent qualitatively different leadership and organizational responsibilities, ranging from contributing to improvement initiatives (A), to coordinating transformation programs and managing digital performance (B), and to steering institutional change, governance frameworks, and strategic partnerships (C). This distinction ensures that proficiency levels capture both technical progression and leadership function differentiation, reflecting the realities identified through the Romanian job analysis and assessment phases.

143. **When it comes to the operationalization of the proficiency levels in HRM, the project confirmed that system-wide baseline capability expectations need to be combined with a differentiated use of proficiency levels in certain HR processes.** In Romania, the three-level model (A–B–C) enabled the definition of a common minimum digital threshold for recruitment, aligned with EU entry-level practice (e.g. EPSO testing model), while allowing higher proficiency levels to be addressed primarily through learning and development pathways rather than selection mechanisms. This avoided creating undue recruitment barriers for roles that do not require advanced digital expertise at entry, while still establishing ambitious skill development targets for the workforce as a whole.

144. **Proficiency expectations were calibrated to real job requirements identified through task analysis, enabling institutions to use higher levels (B and C) as development objectives and progression**

targets, not automatic gatekeepers for entry or mobility. For EU Member States, the lesson is that successful operationalization depends on differentiated application of proficiency: baseline levels validated at recruitment, and higher levels built through **structured** training and validated through later career mechanisms. This approach preserves recruitment accessibility, protects equity and mobility, and ensures that skill development remains demand-driven rather than compliance-driven.

Lesson 5 – AI competency needs to be embedded in digital competency frameworks, but managed as an adaptive layer responding to rapid technological and regulatory change

145. **The experience from the design and pilot process in Romania confirms that AI should not be treated as a standalone or parallel skills domain, but as an evolving capability embedded within the broader digital competency framework.** Across Outputs 1 and 2, AI-related tasks were consistently identified as extensions of existing digital practices – data use, content creation, problem solving, service design, and governance – rather than as isolated technical activities. This finding aligns with the evolution of European reference standards, notably DigComp 3.0, which integrates AI-related knowledge, skills and attitudes across multiple competency areas instead of creating a separate AI pillar. Embedding AI within the general digital framework ensures conceptual coherence, avoids fragmentation of skill models, and reflects how AI is actually used in administrative work.

146. **At the same time, the Romanian experience demonstrates that AI competencies require explicit articulation and regular updating within the framework to remain relevant in a fast-changing technological landscape.** The integration of AI-related descriptors drew not only on DigComp 3.0, but also on complementary sources such as UNESCO's AI and Digital Transformation Competencies for Civil Servants and the EU legal framework - in particular the EU AI Act. These inputs informed the inclusion of competencies related to AI literacy, responsible and ethical use, understanding of algorithmic decision-making, data bias, transparency, and human oversight. The lesson drawn is that AI competencies cannot be treated as static additions; they must be designed as an adaptive layer that can be recalibrated as AI technologies, use cases, and regulatory obligations evolve.

147. **The project further showed through the pilot process that effective AI capability building depends on differentiating the proficiency expected across various roles.** Basic AI literacy and responsible-use competencies are increasingly relevant for all civil servants and should be embedded at foundational proficiency levels. More advanced AI-related competencies – such as designing AI-enabled services, overseeing algorithmic systems, or managing compliance with AI governance requirements – are relevant only for specific roles and should be targeted accordingly. This reinforces the importance of using proficiency levels flexibly and avoiding blanket requirements for advanced AI skills. The key lesson is that administrations should future-proof their workforce by embedding AI coherently within general digital frameworks, while relying on adaptive governance, continuous review against DigComp updates, and targeted learning pathways to keep pace with the rapidly evolving AI landscape.

BOX 4: Operationalizing AI literacy in the public administration

Romania: Operationalizing AI literacy in the public administration

Under **Article 4 of the AI Act**, operationalizing AI literacy within Public Administration (PA) requires developing the skills, knowledge and understanding necessary for the informed deployment of AI systems. This includes fostering awareness of both the opportunities and risks associated with AI, as well as gaining awareness about the opportunities and risks of AI and possible harm it can cause (article 4 of the AI Act).

In the context of PA, AI literacy has different implications for management versus end-users. To assist managers and training providers in operationalizing these requirements effectively, several descriptors have been derived directly from Article 4. Namely, 9 specific descriptors link to **Competence 6.3 (AI Literacy in Public Administration)**, while in **Area 7**, there are 8 specifically tailored for managers.

Next Steps and Collaboration

To meet these challenges, the PA sector could invest in sharing of good practices. Formal EU-supported platforms, such as the Expert Group on Public Administration and Governance - Reform Support could serve as ideal venues for these critical discussions.

Concrete examples

For any users, at the very basic level, PA organizations should ensure a suffcient level of AI literacy that is proportionate to their technical knowledge, experience, education, and professional training.

Examples of descriptors:

- 6.3.01 (Basic) Aware that when using any AI systems in public administration, the user should be provided with a suffcient level of AI literacy.
- 6.3.03 (Basic) Recognize what AI is in general terms, making a basic distinction between what is and what is not an AI system.
- 6.3.09 (Intermediate) When using AI systems at in public administration tasks, aware of the risks of the AI system and basic steps to mitigate those risks, including how legal and ethical aspects can affect the individuals they are used on.
- 6.3.12 (Advanced) Distinguish examples of high-risk AI systems (e.g. according to legislation) in their field of public administration, their potential negative impacts and how the persons on whom the AI system is used can exercise their rights.

For managers:

- 7.2.04 (Basic) Provide strategic direction, oversight and training opportunities for the use of AI tools in public administration to integrate them into relevant parts of the team's processes and workflows while mitigating the risk of discriminatory outcomes from AI uses.
- 7.2.07 (intermediate) Enable and oversee the design and roll out of structured digital upskilling programs for the team (including training on AI systems where relevant), and support translation of acquired skills into updated job descriptions and workflows.
- 7.3.07 (Advanced) Contribute to the development of an institutional AI roadmap, aligned with AI Act requirements and Digital Decade objectives, while ensuring organizational cultural transformation and change management processes.

Lesson 6 - Framework impact depends on HR integration, not only on technical design

148. **One of the most consistent cross-output findings was that competency frameworks only generate workforce impact when embedded into core HR processes.** Output 3 mapped specific procedures connecting digital competencies to job analysis, recruitment standards, learning pathways, appraisal dialogues. The lesson aligns closely with World Bank, OECD[80] and SIGMA evaluations of competency-based civil service HRM reforms: frameworks must function as part of the HR system architecture, not as standalone policy instruments.

149. **The formal legal adoption of a framework, on its own, is insufficient and may even lead to formalistic "box-ticking" implementation if not supported by operational tools.** Meaningful integration requires standardized templates, workflow guides for HR units and line managers, methodological instructions for assessors, quality-assurance and appeals mechanisms, and digital infrastructure capable of storing competency evidence and linking it to training planning. Without these elements, managers lack practical means to apply the framework consistently, and digital competencies risk remaining symbolic labels in regulations rather than drivers of workforce development.

150. **In practical terms, Romania's experience illustrates that framework operationalization must be approached as a system-building exercise rather than a drafting exercise.** The essential tasks include aligning HR procedures and regulations with competency language, equipping HR units and managers with user guides and training, integrating competency data flows into HRMIS and TNA platforms, and sequencing rollout so that learning pathways precede accountability mechanisms. The lesson for Member States is that digital competency frameworks should be designed and implemented as integrated component of the HRM ecosystem.

Lesson 7 - Learning systems should lead reform sequencing

151. **Romania's proposed implementation logic underlines that training and TNA systems must precede high-stakes HR applications. O**utput 4 demonstrated how a DigComp-aligned TNA platform can function as the primary operational entry point for framework use: diagnosing skills gaps, routing staff to training pathways and aggregating workforce capability data for institutional planning.

152. **This approach also reflects the experience of relevant digital skills initiatives** such as Italy's Syllabus for Digital Skills for the public administration, or Spain's Digital Competencies of Public Employees: Reference Framework, both of which anchor framework impact in learning ecosystems. The project therefore reinforced a crucial sequencing lesson: linking digital competencies too early to appraisal scoring or promotion risks formalism and resistance; building learning capacity first enables sustainable uptake and credibility. Romania's large-scale operationalization of DigCompRO for citizens also proves that prioritizing contextual adaptation and learning are essential, as it places emphasis on blended delivery and a train-the-trainers cascade through public libraries (Box 5).

80. OECD (2017), Skills for a High Performing Civil Service, OECD Public Governance Reviews, OECD Publishing, Paris.
OECD (2024), Developing Skills for Digital Government: A review of good practices across OECD governments, Paris.

BOX 5: Romania: Operationalizing DigComp for citizens as a scalable model

Romania: Operationalizing DigComp for citizens as a scalable model

In Romania, the EU Digital Competence Framework for Citizens (DigComp 2.2 version) has been successfully adapted and implemented to build digital skills among adults at scale, particularly through public libraries (as the first stage)[81]. Key elements include:

Contextual adaptation

→ Adapting DigComp to Romanian realities, including everyday citizen needs, resulting in three flexible training streams: Citizen Life (public services and civic engagement), Personal Life (daily digital tools), and Professional Life (work-related skills). Learners can complete all streams or select pathways based on age, interests, or goals.

Blended delivery

→ A hybrid training model combining face-to-face sessions with online modules (via Moodle), supported by NRRP-funded equipment in local libraries and participants' own devices, ensuring accessibility across urban and rural areas.

Prioritized Train-the-Trainers approach (ToT)

→ Experienced librarians were selected as the initial cohort. Through a master trainer program, they were equipped to cascade knowledge, ultimately training over 700 librarians from county, municipal, city, and rural libraries. This maximized resource efficiency and made training available where citizens live.

Strategic, phased rollout

→ The initiative focused first on high-leverage groups (librarians as community anchors), which ensured sustainable adoption. Subsequent phases built on this foundation, enabling broader reach and long-term impact.

This approach can be considered a good practice regarding the power of targeted prioritization and cascading expertise in operationalizing digital competence frameworks without requiring overly detailed descriptors, allowing flexible, nationally relevant learning outcomes (as illustrated in related project outputs).

A comparable strategy could accelerate adoption of the proposed Digital Competence Framework for Public Administration, potentially by starting with priority roles in public services.

The EU Expert Group on Public Administration could also play a valuable role by establishing a dedicated subgroup on programs for key competences, including AI literacy. This would facilitate cross-member-state sharing of best practices.

Lesson 8 - General digital upskilling cannot substitute professional ICT capacity

153. **Across the design process it became evident that expanding general digital competencies, even at advanced proficiency levels, cannot substitute for the depth of expertise required to design, secure, operate, and sustain complex digital government systems.** Output 1 diagnostics and stakeholder consultations consistently confirmed critical skills gaps in advanced ICT domains - including digital system architecture, cybersecurity, application development, testing, and user-centred service design - that fall well beyond the scope of transversal digital upskilling. These findings led, under Output 2 (as a Connected report), to the development of a parallel framework of 24 specialised ICT professional roles, aligned with the e-CF and the ECSF, subsequently grouped into dedicated ICT job families to enable structured career pathways for technical specialists.

154. **The project therefore validated a dual-capacity model for digital government: general digital competencies help develop digital capability across the civil service and they need to be differentiated from specialised ICT roles and competencies.** Level C advanced descriptors under the general digital competency framework were intentionally calibrated to remain applicable for the general public administration roles, governance, and organisational coordination, without overlapping the technical depth demanded of ICT professionals. Without this structural separation, administrations

81. https://anbpr.org.ro/index.php/competente-digitale-de-baza-pentru-cetatenii-romani/.

risk misusing general competency frameworks to compensate for deficits in professional ICT staffing, reinforcing dependence on outsourcing, concentrating expertise in informal roles, and undermining institutional continuity. Romania's digital transformation gaps demonstrates that effective workforce reform requires coupling digital upskilling strategies with explicit ICT professionalisation pathways linked to classification systems, recruitment standards, training and certification, and career development, rather than attempting to stretch general competency models to cover specialist functions.

Lesson 9 - System reform benefits from phased, adaptive governance

155. **Finally, the project refined the understanding that digital competency reform is necessarily iterative and multi-year, requiring governance models that support continuous monitoring and updating.** The staged pathways developed under Output 3 recognized differences in HRM maturity, regulatory rigidity, and digital readiness across administrations, allowing each system to adopt proportionate integration timelines. At the same time, the experience showed that competency frameworks must remain "living instruments," with mechanisms in place to regularly review and update descriptors, proficiency expectations, and assessment tools in response to technological change, evolving service-delivery models, and new regulatory requirements, including those related to AI.

156. **This adaptive approach mirrors EU policy guidance emphasising experimentation and national tailoring rather than uniform implementation.** The lesson for Member States is that successful framework deployment depends less on speed of formal adoption and more on sustained governance capacity to adjust tools, processes and proficiency expectations over time.

5.2 EU-Level relevance and opportunities for future integration

157. **The Romanian General Digital Competence Framework for public administration employees was explicitly designed to remain compatible with the European skills ecosystem while extending existing models into public administration - specific application domains that requires its own occupational digital competency framework.** Its alignment with DigComp 3.0 ensures direct comparability with the individual digital skills standards currently underpinning EU training platforms, assessment instruments, and emerging micro-credential schemes. At the professional ICT level, the related role framework developed under Output 2 draws directly on the e-CF and ECSF, anchoring Romania's approach in the occupational taxonomies that support ESCO updates, EU Cybersecurity Skills Academy initiatives, public administration ICT professional profiles, and skills-based procurement and certification regimes across Member States. This dual anchoring positions the Romanian model not as a stand-alone national construct, but as a practical national implementation of Europe's shared digital skills architecture for the public sector.

158. **The model was deliberately designed to address current public administration and its occupational skill needs while remaining adaptable for future development and integration with other EU competence initiatives, such as JRC' work focused on Professional Interoperability Profiles (PIOP).** Romania's experience is particularly relevant for emerging EU workstreams linked to digitally enabled and interoperable public administrations, including efforts supporting the Interoperable Europe Act[82] and the implementation of the European Interoperability Framework (EIF)[83]. These initiatives increasingly recognize that interoperability depends not only on standards and technical infrastructures, but also on the availability of public servants with the competencies required to

82. https://interoperable-europe.ec.europa.eu/interoperable-europe/interoperable-europe-act.
83. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf.

design, govern and operate cross-institutional services and data ecosystems (Box 6). The proposed digital competency framework already embeds many of these capability domains at general level – such as cross-agency process coordination, digital service lifecycle management, data stewardship, AI governance, cybersecurity governance, and organisational transformation leadership. As such, it provides a structurally compatible foundation for future EU-level interoperability capability profiles. This compatibility allows national and EU frameworks to function as mutually reinforcing instruments rather than parallel systems.

BOX 6: Professional Interoperability Profiles (PIOP) developed by JRC can build upon the proposed general digital competency framework for the public administration

Professional Interoperability Profiles for civil service managers (PIOP) being developed by JRC can be structurally linked to the proposed general digital competency framework

Focussing on competence needs for mid-level managers (here, mainly Area 7 - Level B) the JRC carried out dedicated activities with DIGIT in support of the Interoperable Europe Act implementation.

The Interoperable Europe Act entered into force on 11 April 2024, marking a significant step towards strengthening interoperability in the public sector. The Act enables administrations to cooperate and ensure public services function seamlessly across territorial, sectoral, and organisational boundaries, while maintaining their sovereignty at all levels of government. (source: https://interoperable-europe.ec.europa.eu/interoperable-europe/interoperable-europe-act). Its implementation requires basic knowledge about the concept of interoperability and cross-border data exchange between public administration, but also some more advanced understanding of particular elements and measures of the Act, such as the interoperability assessments, the European Interoperability Framework, interoperability regulatory sandboxes, or the underlining governance structure (include the role of the Interoperable Europe Board).

Mid-level managers have been identified as critical players in the implementation of the Interoperable Europe Act, and thereby to help the EU and its member states to deliver interoperable trans-European digital public services to citizens and businesses across the entire EU.

To support mid-level managers in public sector institutions, bodies and agencies in taking up these tasks, this research of the JRC scoped and initiated the development of a professional interoperability profile (PIOP) for public servants - with a focus on middle management, and on the implementation of the Interoperable Europe Act.

This work benefited from the already established framework for citizen digital competences (DigComp) and aimed at the directly associations with potential training offerings (for example, provided by the Interoperable Europe Academy). Hence, the identified competences are complemented by intended learning outcomes. Here, learning outcomes refer to an approach that offers the strategic advantage of aligning to and embedding into existing EU initiatives such as the European Qualifications Framework (EQF) and the various uses of learning outcomes already observed in all Member States (see also European Centre for the Development of Vocational Training - CEDEFOP).

More specifically this work included the following:

- Identification of interoperability competences for public servants, based on the requirements to implement the Interoperable Europe Act.
- Specification of intended learning outcomes to align with the DigComp framework structure.
- Discussion, validation and revision the draft PIOP with relevant stakeholders.
- Pre-piloting exercise.
- Summary of the applied methodology and recommendations for the possible piloting of the PIOP.

As a result, a validated initial version of PIOP competences and learning outcomes are available, and recommendations for future actions and research are prepared. This includes a proposal for the further piloting of PIOP to help public sector organisations across the EU in implementing the Interoperable Europe Act (e.g. by user-centric development, the embedding with other functions and existing profiles, and addressing certification).

At the level of competences, requirements for interoperability were integrated into general digital competences, general management competences, leadership competences and interoperability specific competences. For general management competences it was, for example, underlined that stakeholder management competences need to include the Interoperable Europe Board, the Interoperable Europe Community, National competent authorities, their designated single points of contact, and interoperability coordinators for union entities. The interoperability specific competences include, for example, a requirement engineering competence, legal framework competence, procurement for interoperability competence, and others.

As far as learning outcomes are concerned, the identified competences were mapped (as intended learning outcomes) to DigComp. The approach combined a mapping the learning outcomes to existing DigComp competence, on the

one hand, with specifically themed modules outside of the original DigComp framework, on the other hand. A level of proficiency required for each identified area has been added accordingly. For example, for the competence "Managing information", the experts identified a need for advanced skills to be able to use a range of digital tools and methods to collect and process legal and official information. Then it comes to interoperability these tools and methods should, for example, include *the online form to perform interoperability assessments, guidelines for cross border Interoperability Assessments and Decision Tree for identifying and documenting binding requirements, Repository of IOPA reports, EU Better Regulation Guidelines and Toolbox*. As another example under the came category, PIOP includes an advanced skill need to *apply appropriate analysis of legal information to identity cross border interoperability barriers and other requirements of Interoperable Europe Act tasks*.

The initial work on PIOP complements the activities carried out in this TSI project in the sense that the identified needs of mid-level managers are further specified and the competences and desired learning outcomes for interoperability are more precisely articulated. This approach also illustrates how DigComp (and DigCompPA) could be used to develop more specific profiles that are required for implement EU (digital) policies.

159. **At the European level, the availability of nationally adapted yet structurally compatible competency models such as the proposed digital competency framework opens important opportunities for economies of scale in skills development.** Where Member States base their occupational frameworks on shared European taxonomies - notably DigComp, e-CF/ECSF and emerging EIF/JRC profiles — learning content, assessment instruments and certification pathways can be developed collaboratively instead of being duplicated nationally. This enables the creation of shared assets such as EU-level digital leadership curricula, interoperable micro-credentials, pooled online learning modules, simulation-based exercises and standardized assessment item banks, which can be localized with minimal transaction costs. Romania's experience demonstrates how public administration–specific competency descriptors can be articulated without sacrificing cross-country transferability, allowing the country to participate fully in present and future EU-level digital academies, cybersecurity capacity-building programs.

160. **Compatibility and the complementary nature of skills frameworks also facilitate the emergence of cross-national communities of practice.** Although such networks are not created by competency frameworks alone, shared skill vocabularies enable meaningful professional exchange by allowing roles, proficiency levels and learning pathways to be understood across national administrations. For Romanian officials, this creates concrete opportunities to engage in EU professional peer networks, exchange programmes, blended training cohorts and practitioner learning platforms. At EU level, it contributes to the longer-term development of a more cohesive European digital public-service profession, enhancing mutual recognition of skills and strengthening administrative cooperation.

161. **From a strategic perspective, the proposed framework demonstrates that Member States do not need to choose between European standardization and national customization:** the two can be combined through frameworks that apply common EU structures while embedding national legal requirements, HRM systems and service-delivery contexts. As further EU-driven digital capability profiles mature - particularly those connected to interoperability management, data-space governance, and AI regulation implementation - the Romanian framework offers an adaptable base for continued alignment, refinement and upward calibration. In this sense, the Romanian experience can be seen as the beginning not only of a national digital skills model for the public administration, but a transferable methodology for translating European skills architectures into policy measures. Moving forward, systematic alignment between national frameworks such as the proposed digital competency framework for the public administration and EU-level initiatives offers a pathway to reduce fragmentation in public sector upskilling efforts, increase the effectiveness of EU training investments, and reinforce the human capital foundations of Europe's digital transformation agenda. By using comparable and complementary models that are adapted rather than fully redesigned, Member States can more effectively share learning resources and ensure that investments in digital transformation are matched by efficient investments in the capabilities of the people responsible for delivering them.

Annexes

Annex 1: Alignment matrix with DigComp 3.0 (proficiency levels)

TABLE 11: Relationship between the four proficiency levels of DigComp 3.0, the eight levels of DigComp 2.2, along with an alternative 6-level mapping and the 3 levels in the digital competency framework for the public administration

DigComp proficiency levels		Digital competency framework for public administration: proficiency levels	Short description		Purpose
Basic	**1**	Level A	At basic level, individuals remember and implement simple tasks with guidance as needed.	*At the bottom of the Basic level, individuals require guidance to recognise and implement many or most simple tasks.*	To support personal, learning and/or working goals and participate in society.
	2			*At the top of the Basic level, individuals remember and implement simple tasks with little or no guidance.*	
Intermediate	**3**	Level B	At intermediate level, individuals identify and implement well-defined tasks and solve well-defined problems autonomously.	*At the bottom of the Intermediate level, individuals show some autonomy to identify and implement well-defined tasks and solve well-defined problems.*	To support personal, learning and/or working goals and participate autonomously in society.
	4			*At the top of the Intermediate level, individuals confidently and autonomously identify and implement well-defined tasks and solve well-defined problems.*	
Advanced	**5**	Level C	At advanced level, individuals assess and apply solutions to a variety of complex tasks autonomously and adapt to a variety of contexts to evaluate and execute tasks appropriately, guiding others if and as required.	*At the bottom of the Advanced level, individuals assess and apply solutions to a variety of well-defined tasks and engage with some complex tasks. They identify situations where approaches may need to be adapted, and guide others on well-defined tasks if and as required.*	To support personal, learning and/ or working goals, participate effectively in society, and manage or support others in achieving their goals.
	6			*At the top of the Advanced level, individuals work confidently on a variety of complex tasks, respond effectively to challenges in changing contexts, and lead or manage complex projects, guiding others on complex tasks if and as required.*	

DigComp proficiency levels		Digital competency framework for public administration: proficiency levels	Short description		Purpose
Highly advanced	**7**	Not covered*	At highly advanced level, individuals assess, evaluate and resolve highly complex or specialised problems to create new solutions or adapt existing ones, leading and guiding others if and as required.	*At the bottom of the Highly Advanced level, individuals assess highly complex or specialised problems and may contribute to new solutions or adapt existing ones, leading and guiding others if and as required.*	To support personal, learning and/or working goals, help others to participate effectively in society, lead or support others to achieve complex goals, and/or lead or contribute to improvements in or new solutions for highly complex problems.
	8	Not covered*		*At the top of the Highly Advanced level, individuals lead and guide others on the creation of solutions to highly complex or specialised problems.*	

*Note: DigComp defines proficiency progression spans from basic levels to highly advanced. By contrast, the proposed general digital competency framework was developed for the needs of the public administration and its proficiency levels are therefore calibrated to what is necessary and sufficient for effective performance in public administration roles and typically extend up to advanced levels, rather than to highly specialised individual expertise (based on the review performed under Output 1 of this project). This calibration does not preclude individual civil servants from pursuing further self-directed learning, developing higher levels of digital competency, or engaging in voluntary certification aligned with DigComp.

Annex 2: Overview of key legal and policy references that underpin the proposed model

TABLE 12: Legal and strategic justification for the proposed digital competencies

Competency area		Digital competency	Justification
Digital literacy in public administration	1.1	Searching and accessing data, information and digital content	→ EU Open Data Directive and Implementing Regulation on High-Value Datasets require civil servants to know how to search, access, and use publicly available datasets in machine-readable form.
	1.2	Evaluating data, information and digital content	→ The European Skills Agenda and Digital Decade emphasize evidence-based decision-making underpinned by data literacy. → OECD (2024 "Developing Skills for Digital Government") stresses skills for data-driven government, including validation of official sources (Eurostat, OECD, national statistics). → UNESCO (2022 Framework - Artificial Intelligence and Digital Transformation Competencies for Civil Servants) highlights "data use and governance" as a core competency domain for civil servants.
	1.3	Managing data, information and digital content	→ Interoperability Act and Law 242/2022 on Interoperability require civil servants to follow classification, metadata, and archiving rules. → The Data Act, and Data Governance Act foresee that public administrations must be able to collect, store, and process data.
Area 2. Digital Communication and Collaboration	2.1	Communicating, interacting and fostering citizen and business participation through digital technologies	→ Single Digital Gateway Regulation (SDGR) obliges administrations to ensure clear, inclusive, and accessible digital communication channels. → Web Accessibility Directive mandates that communications and digital services be usable by all, including persons with disabilities. → UNESCO (2024 Broadband report) emphasizes citizen-centric communication and inclusivity.
	2.2	Sharing and collaborating in digital teams in intra- and inter-institutional contexts	→ Interoperable Europe Act requires seamless cross-border data sharing and collaboration across institutions. → The Data Governance Act and Data Act explicitly require public administrations to facilitate secure access and reuse of data. → Open Data Directive promotes collaboration and reuse of public data.
	2.3	Ensuring digital integrity and accountability in public administration	→ The AI Act explicitly requires human oversight, accountability, and transparency in AI-enabled decisions. → Digital Services Act (DSA) requires public authorities to ensure safe and ethical digital interactions. → The Defence of Democracy package (2023)[84] promote the participation of citizens and civil society organisations in policy making → UNESCO (2022 Framework - Artificial Intelligence and Digital Transformation Competencies for Civil Servants) highlights trust, transparency, and ethical AI use as key digital attitudes.

Competency area		Digital competency	Justification
Area 3. Digital Content and Public Services	3.1	Developing, integrating and re-using digital content	→ Web Accessibility Directive and EN 301 549 standards mandate accessibility of digital content. → Digital Decade and ComPAct initiative stress interoperable and reusable public administration content. → UNESCO (2022 Framework - Artificial Intelligence and Digital Transformation Competencies for Civil Servants) calls for creativity, adaptability, and ethical AI use in content development.
	3.2	Delivering and contributing to digital public services	→ Single Digital Gateway and Once-Only Technical System (OOTS) require civil servants to design services that reduce administrative burden and ensure cross-border access. → eIDAS 2.0 and the EU Digital Identity Wallet obligate member states to build digital services around secure e-identification. → World Bank (GTMI 2022) and UNESCO emphasize citizen-centered service design and usability.
	3.3	Ensuring compliance with legal and regulatory frameworks and standards in digital environments	→ GDPR, Data Act, AI Act, NIS2 Directive, and Cyber Resilience Act impose direct obligations for compliance.
Area 4. Safe, Responsible, and Sustainable Use of Resources	4.1	Protecting devices and infrastructures	→ NIS2 Directive, Cybersecurity Act, and Cyber Resilience Act establish legal obligations for cybersecurity.
	4.2	Managing digital identities, and protecting personal data and privacy	→ GDPR and the Data Governance Act require secure storage, documentation, and traceability of personal data. → eIDAS 2.0 and eID require secure handling of digital identities and signatures. → UNESCO highlights the centrality of digital identity management to service delivery.
	4.3	Supporting healthy and sustainable digital practices	→ European Declaration on Digital Rights and Principles for the Digital Decade promotes sustainability, wellbeing, and inclusivity.
Area 5. Problem-Solving with Digital Technologies	5.1	Managing digital devices, including identifying and solving technical problems	→ OECD stresses that public servants must be able to use and troubleshoot digital tools for continuity of services. → World Bank's GovTech Maturity Index highlights operational continuity as a driver of maturity in government systems.
	5.2	Using automation tools in digital environments	→ EU AI Act encourages the safe use of automation while mitigating risks. → ComPAct initiative explicitly promotes workflow automation in public administrations. → OECD highlights computational thinking and automation as essential for public sector innovation.

84. https://commission.europa.eu/document/5d470456-641c-4248-951c-0ff1d52627fe_en.

Competency area		Digital competency	Justification
Area 6. Digital Transformation and AI Literacy	6.1	Contributing to digital transformation in public administration, driving innovation and improvement	→ EU Digital Decade, ComPAct initiative, OECD foresee that civil servants should actively support innovation, interoperability, and emerging technologies.
	6.2	Developing digital competence in the workplace	→ European Skills Agenda and Pact for Skills highlight continuous upskilling and reskilling, including for public sector staff.
	6.3	AI Literacy in public administration	→ AI Act explicitly requires AI systems providers and deployers ensure AI literacy for all staff (Art. 4). → UNESCO identifies AI literacy as a core competency domain, emphasizing risk awareness, ethics, and safe use.
Area 7. Digital leadership and governance in the public administration	7.1	Managing performance and operations through digital technologies	→ The Digital Decade requires public administrations to monitor progress against digitalization targets, using dashboards and indicators. → EU rules on Open Data and the Data Governance Act mandate transparency, reporting, and traceability of public sector data. → OECD's Framework for digital talent and skills in the public sector emphasizes managers' ability to use data analytics, KPIs, and digital monitoring systems to improve performance and efficiency. → World Bank's GovTech Maturity Index (2022) stresses the importance of data-driven management and automation for performance monitoring in digital governance.
	7.2	Leading team development in digital environments	→ The European Skills Agenda and Pact for Skills explicitly call for continuous learning ecosystems, including within public administrations. → The ComPAct initiative requires digital upskilling of civil servants, with managers responsible for aligning team skills with emerging needs (AI, cybersecurity, interoperability). → OECD (Framework for digital talent and skills in the public sector) highlights managers' role in talent pipelines, skills mapping, and fostering organizational learning cultures. → UNESCO's AI and Digital Transformation Competency Framework stresses adaptability, curiosity, and continuous learning as leadership attitudes.
	7.3	Driving and leading innovation and digital transformation	→ The Digital Decade and ComPAct initiatives require leaders to champion innovation, agile methodologies, and user-centered design in digital services. → The AI Act requires public sector institutions to establish governance for AI use, requiring leadership to coordinate adoption and scaling responsibly.
	7.4	Strengthening public services and ensuring responsible digital governance and cybersecurity	→ GDPR, NIS2 Directive, Cyber Resilience Act, and Interoperable Europe Act impose compliance obligations that require governance at managerial level. → The AI Act requires leadership to implement AI governance frameworks and accountability structures.
	7.5	Anticipatory and strategic thinking supporting public administration	→ The Digital Decade Policy Program and EU-level monitoring (DESI, country reports) require administrations to anticipate digital trends and prepare forward-looking strategies. → OECD stresses the need for strategic foresight and systems thinking in digital government, including use of scenario planning and predictive analytics.


WORLD BANK GROUP