

OUTPUT 4. REPORT WITH RECOMMENDATIONS ON UPDATING INA'S TRAINING NEEDS ASSESSMENT METHODOLOGY AND WITH PROPOSALS OF ELEMENTS FOR CURRICULUM

Technical Support Instrument

Supporting reforms in 27 Member States

**TSI COMPONENT “ROMANIA: DEVELOPING A
GENERAL DIGITAL COMPETENCE FRAMEWORK FOR
CIVIL SERVANTS”**

ACTIVITY 4

**SUPPORTING CAPACITY BUILDING PROGRAMS FOR THE IMPLEMENTATION
OF THE DIGITAL COMPETENCY FRAMEWORK, FACILITATE KNOWLEDGE
EXCHANGE EVENTS, AND PROPOSE KEY ELEMENTS OF CURRICULUM FOR A
SET OF LEARNING AND DEVELOPMENT PROGRAMS**

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

© 2025 The World Bank

1818 H Street NW, Washington DC 20433

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

Some rights reserved

The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for non-commercial purposes as long as full attribution to this work is given.

All queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@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).

The development of this report was led by Anca Butnaru, with a core team composed of Cristina Zamfir (Senior Public Sector Expert), Sorana Gheorghiade (Public Sector Analyst), Zohar Ianovici (Senior Public Sector and Digitalization Expert), Cezar Haj (Public Sector Expert and Senior Education Expert), Diana Iancu (Dean, Faculty of Public Administration, SNSPA), Magdalena Popescu (Senior Communication Expert), Cătălin Vrabie (Professor, Faculty of Public Administration, SNSPA) and George Mateescu (Senior Public Sector Expert).

Valuable inputs were also provided by Riina Vuorikari (Senior International Digital Competence Expert).

Fanny Weiner (Senior Public Sector Specialist) provided valuable insights as peer reviewer.

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 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 Panțiru (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 December 2025, 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).

Contents

Abbreviations	5
Glossary.....	6
Executive summary	9
1. Introduction: context and scope	14
2. The TNA process. Redesigning TNA for digital skills.....	18
2.1 The proposed general digital competency framework as the basis for TNA	18
2.2 Overview of the current TNA process in the Romanian public administration	20
2.3 Towards a targeted TNA process for digital competencies	25
3. The TNA platform: from assessment to learning decisions – international insights and lessons for Romania.....	29
3.1 Assessment methods applied on dedicated TNA platforms	29
3.2 Functional characteristics of digital skills (self-)assessment tools	36
4. Institutionalizing the digital-skills TNA process: design principles and implementation mechanisms	51
4.1 Define institutional ownership, mandates, and data governance	51
4.2 Select an implementation pathway for the digital-skills TNA platform	52
4.3 Design and test assessment methods and instruments based on the proposed digital competency framework for the public administration.....	53
4.4 Integrate learning pathways and recognition	57
4.5 Consider a gradual adoption strategy and monitor implementation	60
4.6 A proposed roadmap for implementation	62
Annexes	65
Annex 1 Examples of self-assessment questions using Likert scale, per competence level.....	65
Annex 2 Proposed format for assessment reports	67
Annex 3 Elements of curriculum proposed based on the proposed general digital competency framework for the public administration.....	71
A1. Digital literacy in public administration.....	71
A2. Digital communication and collaboration	78
A3. Digital content and digital public services	86
A4. Safe, responsible and sustainable use of resources	95
A5. Problem-solving through digital tools	102
A6. Digital transformation in public administration	106
A7. Digital leadership and governance in public administration	113
Annex 4 Example of knowledge-based TNA survey for the proposed general digital competency framework (levels A and B for digital competency areas 1-6).....	128

List of figures

Figure 1 Project intervention logic (as reflected by the project deliverables)	9
Figure 2 Theory of change – Digital skills assessment and learning are core to introducing the digital competency framework	15
Figure 3 TSI project intervention logic: Report corresponds to Activity 4	15
Figure 4 The proposed general digital competency framework for the Romanian public administration .	20
Figure 5 The TNA process at institutional level, per the legal framework – centered around the individual performance appraisal process.....	24
Figure 6 TNA process for digital competencies adapted to be deployed within current legal mandates ..	27
Figure 7 SNA AI strategy	39
Figure 8 An example for a Personal Digital Profile elaborated with the result of the IKANOS test	48
Figure 9 AgeDigital assessment platform ensures certification of the digital skills and connection to learning modules.....	49

List of tables

Table 1 Digital-skills assessment methods in public administrations: advantages, limitations, OECD/EU examples, and best HR uses (including hybrid approaches)	35
Table 2 Comparative overview of the two options for the TNA platform.....	52
Table 3 Recommended assessment methods for different use cases	54
Table 4 Key functionalities for the TNA platform	56
Table 5 Proposed minimum set of indicators for monitoring	61
Table 6 Roadmap for implementation - indicative	64

List of boxes

Box 1 Strengthening learning and cooperation through managerial and professional networks and coordination boards: case of Finland.....	28
Box 2 Ikanos as self-assessment platform.....	31
Box 3 Italy - SNA's Department of Digital and Ecological Transition (DiTED) and the Corso-Concorso executive pipeline	38
Box 4 Latvia's Digital Competency Framework and implementation model in the public sector	42
Box 5 Canada - Digital Competencies Self-Assessment (DCSA) – scope and methods applied	43
Box 6 The UK Government's Digital Competency Framework and TNA approach	46

Abbreviations

ADR	Authority for the Digitalization of Romania
AI	Artificial Intelligence
AI4SNA	Artificial Intelligence for SNA (Italy)
Accredia	Italy's national accreditation body
AgID	Agency for Digital Italy
CERT	Computer Emergency Response Team
CNCISCAP	National Committee for Coordinating the Implementation of the Strategy on Strengthening Public Administration
CNFPT	Centre National de la Fonction Publique Territoriale (France)
DCF	Digital Competency Framework
DDaT	Digital and Data Profession Capability Framework (UK)
DPIA	Data Protection Impact Assessment
DPP	Directorate for Short-term Training (INA)
DSKPA	Digital Skills and Knowledge for Public Administration (Italy)
DiTED	Department of Digital and Ecological Transition (Italy)
EC	European Commission
EIPA	European Institute of Public Administration
EU	European Union
FUN-MOOC	France Université Numérique MOOC platform
GDPR	General Data Protection Regulation
GSG	General Secretariat of the Government
HRIS	Human Resources Information Systems
HRM	Human Resources Management
IDcert	Italian digital skills certification platform
IKANOS	Basque Country's digital competence self-assessment tool
INA	National Institute of Administration
INAP	Instituto Nacional de Administración (Spain)
LMS	Learning Management System
MDPWA	Ministry of Development, Public Works and Administration
MLSS	Ministry of Labour and Social Solidarity
MOE	Ministry of Education
NACS	National Agency for Civil Servants
NRRP	National Recovery and Resilience Plan
OECD	Organisation for Economic Cooperation and Development
PIAO	Integrated Activity and Organization Plan (Italy)
PIX	Digital skills assessment platform (France/Belgium)
SNA	Scuola Nazionale dell'Amministrazione (Italy)
SSO	Single Sign-On
TNA	Training Needs Assessment
TSI	Technical Support Instrument
WCAG	The Web Content Accessibility Guidelines

Glossary

Acronym	Meaning	Definition
A/B test	Version testing	A controlled experiment where you compare two versions of something - A (current/baseline) vs. B (changed variant) - to see which performs better on a chosen metric.
AI	Artificial Intelligence	Computer systems that perform tasks requiring human intelligence; includes generative AI used for drafting, summarizing, etc.
AI Act	Artificial Intelligence Act	EU regulation categorizing AI risk and setting obligations; used for governance/roadmaps.
API	Application Programming Interface	Interface for systems/data exchange used in interoperability/scale-up.
AV	Antivirus	Security software protecting devices; checked in device self-audits.
Backlog	An ordered list of pending work - ideas, requests, fixes, or tasks that are not started yet but may be delivered in the future.	
BCP/DR	Business Continuity Plan / Disaster Recovery	Plans to maintain/restore services during/after incidents.
BI	Business Intelligence	Tools and methods to analyze operational data and create dashboards.
CC (licensing)	Creative Commons	A family of content licenses (e.g., CC BY, CC BY-SA, CC0) that specify how others may use, share, and adapt works with conditions like attribution or share-alike.
CRM	Customer Relationship Management	System for managing interactions with citizens/businesses; used in workload/capacity planning.
CSV	Comma-Separated Values	Open, interoperable tabular data format used for sharing/publishing datasets.
Data Act	European Data Act	EU law on fair access/use of data, incl. portability and B2G sharing.
DB	Database	Structured data stores used by information systems and analytics.
DGA	Data Governance Act	EU regulation enabling trusted data sharing and stewardship.
DL	Deep Learning	Subfield of ML using multi-layer neural networks.
DMS	Document Management System	Institutional system for storing, versioning, and controlling documents.
DNS	Domain Name System	Internet naming system; appears in troubleshooting (adapter/DNS reset).
DNSC	Direcția Națională de Securitate Cibernetică	Romania's National Directorate for Cyber Security; referenced for incident coordination/guidance.
DPIA	Data Protection Impact Assessment	GDPR tool to assess and mitigate high-risk personal-data processing.
DSA	Digital Services Act	EU regulation on online platforms/content governance; considered for compliance.
eDelivery	Ending official documents or data electronically with proof so the sender and recipient are authenticated, the content's integrity is protected, and there's an audit trail.	
EDR	Endpoint Detection and Response	Security tooling on devices to detect/respond to threats.
eID	Electronic Identity	Digital identification and authentication used in public services.
EN 301 549	European Norm 301 549	EU standard specifying accessibility requirements for ICT products and services.
ERP	Enterprise Resource Planning	Core back-office system integrating finance, HR, etc.; used in analytics/forecasting topics.
FAQ	Frequently Asked Questions	User-support format for clear guidance in services and communications.

Gantt	A timeline view of a project that shows tasks as horizontal bars from their start date to end date, plus dependencies between tasks.	
GDPR	General Data Protection Regulation	EU data-protection law governing personal data processing, rights, and obligations in PA.
HTML	HyperText Markup Language	The standard programming language for structuring content on the web.
HW/SW	Hardware/Software	
INS	Institutul Național de Statistică	National Institute of Statistics, referenced for data-sharing.
IoT	Internet of Things	Networked sensors/devices; covered in emerging-tech governance.
IP (legal)	Intellectual Property	Legal rights over creations of the mind - protecting use and distribution.
ISO 27001	ISO/IEC 27001	International standard for information security management systems.
ISO 42001	ISO/IEC 42001	International standard for AI management systems and governance.
Kanban	Lightweight method for managing work as a flow by visualizing tasks on a board, limit work in progress (WIP), and continuously improve based on real data (cycle time, throughput).	
KPI	Key Performance Indicator	Quantitative measure used to track performance and outcomes.
LLM	Large Language Model	AI model trained on large text corpora; used for generative tasks.
MFA	Multi-Factor Authentication	Login method requiring two or more verification factors.
ML	Machine Learning	Statistical/algorithmic methods enabling systems to learn patterns from data.
NGO	Non-Governmental Organization	A non-profit, independent organization that operates outside direct government control to pursue a public or social mission.
NIS / NIS2	Network and Information Security Directive (recast)	EU cybersecurity directives setting requirements for essential/important entities.
NLG	Natural Language Generation	Automation that turns data into written summaries (auto-reports).
OKR	Objectives and Key Results	Goal-setting framework linking objectives to measurable results.
OWASP	Open Worldwide Application Security Project	Community and guidelines for web/app security best practices.
PA	Public Administration	Government institutions and their staff; the main context for all competencies and learning outcomes.
PDF/A	PDF for Archiving	ISO-standardized PDF version designed for long-term preservation.
PII	Personally Identifiable Information	Data that can identify a person; handling/sharing rules are emphasized.
PNI	Platforma Națională de Interoperabilitate	National Interoperability Platform referenced for data-sharing/governance.
PoC	Proof of Concept	A small, time-boxed experiment to show that an idea or technology is feasible and delivers enough value to justify a bigger investment.
Q&A	Questions & Answers	Simple format page/session/section where people ask questions and someone provides answers - live or written.
README	Short for „Start here”	A document that explains what a project (software, managerial, etc.) is, how to use it, and where to find things. It's the first file people read when they open a repository or shared folder - typically named „Readme”.

RFP	Request for Proposals	Procurement document used to solicit vendor solutions with required clauses.
ROeID	Romanian electronic ID	National eID solution used by citizens to access digital public services.
ROI	Return on Investment	Metric to evaluate financial/benefit returns of initiatives.
Sandbox	A safe, isolated environment where you can experiment, test, or learn without risking real systems or data.	
SDG	Single Digital Gateway	EU initiative/portal enabling cross-border online access to public services and information.
SFTP	Secure File Transfer Protocol	Encrypted file-transfer method for inter-institutional exchanges.
SLA	Service Level Agreement	Target commitments (e.g., response or processing times) used in service operations.
SMS	Short Message Service	Text messaging channel used for notifications and inclusive support.
SOP	Standard Operating Procedure	Step-by-step documented workflow; used for knowledge transfer and consistency.
UCD	User-Centered Design	Designing services/tools around user needs with iterative testing.
URL	Uniform Resource Locator	Web “address” that tells a browser where a resource is and how to get it.
VDI	Virtual Desktop Infrastructure	Remote desktop environment provided by the institution.
VPN	Virtual Private Network	Secure remote connection to institutional networks.
WCAG	Web Content Accessibility Guidelines	International guidelines for making digital content accessible; referenced for documents, portals, and services.
WIP	Work In Progress	

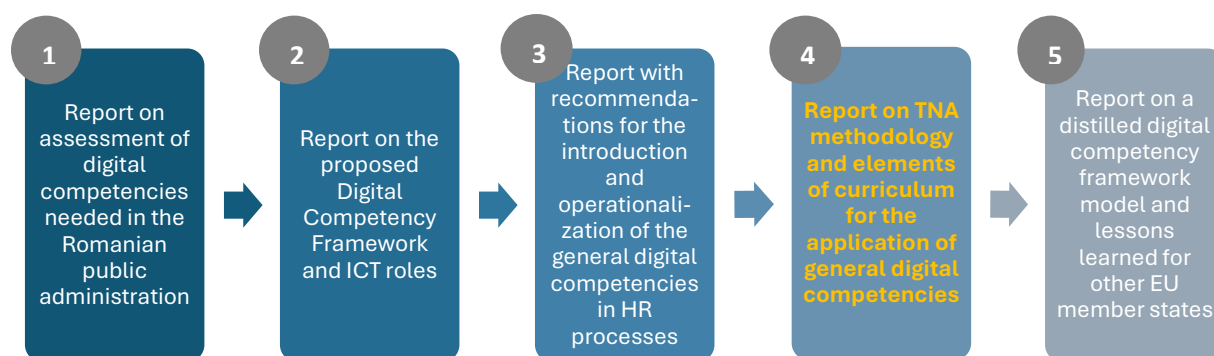
Executive summary

Romania's digital transformation depends on a civil service equipped with clearly defined and measurable digital skills. The development of a general digital competency framework provides the foundation for standardizing digital capabilities across the public administration, distinguishing baseline skills required of all civil servants from advanced competencies needed in specialized roles. However, the value of the framework depends on its practical use within HRM systems, particularly through systematic assessment of skills and targeted workforce development.

To support this objective, the World Bank supports the National Agency for Civil Servants (NACS), The National Authority for Digitalization of Romania (ADR) and the National Institute of Administration (INA) to strengthen the digital capacity of Romania's civil service through a Technical Support Instrument (TSI) project on Developing a General Digital Competency Framework for the Romanian public administration. The project is implemented in close partnership and collaboration with the European Commission. Earlier project outputs established the analytical base (Output 1) and designed the framework itself (Output 2), defining competencies, descriptors, and proficiency levels aligned to DigComp 3.0 and DigCompRO (GEO 27/2025). Output 3 addressed legal anchoring and recommendations on HR process integration.

This report corresponds to Output 4 / Activity 4 and focuses on operationalizing the framework through a Training Needs Assessment (TNA). It proposes a revised methodology that transforms the framework into a practical instrument for evidence-based workforce development. Digital skills assessment becomes the core mechanism for identifying competency gaps across institutions, prioritizing training investments, and aligning learning interventions with Romania's digital transformation objectives and NRRP commitments.

Figure 1 Project intervention logic (as reflected by the project deliverables)



The report focuses on providing targeted recommendations on the training system to support system capacitation instead of premature system-wide application of digital competencies. Consistent with recommendations from Outputs 2 and 3, implementation is staged: digital competencies are initially embedded in recruitment and training, not yet in performance management, promotion, or mobility, to mitigate compliance risks and ensure that competencies drive real capability development rather than formalistic reporting.

The report establishes a structured approach to linking digital competency needs to learning responses. It proposes methods to:

- identify digital skills gaps at institutional and individual levels;

- prioritize training needs based on competency deficiencies;
- align curricula and learning outcomes to the framework’s descriptors and proficiency levels; and
- establish feedback loops that continuously update training portfolios and competency definitions.

International experience informs the operational approach proposed in this report. The analysis reviews public-sector digital assessment platforms and self-assessment tools, highlighting how digital platforms improve consistency, workforce planning, and data-driven targeting of training interventions. These examples guide recommendations for a Romanian digital skills (self-)assessment platform tailored to INA’s mandate and HRM realities.

The analytical work follows two complementary dimensions

- First, the report reviews and redesigns INA’s existing TNA methodology, identifying limitations in capturing digital competencies and proposing updates aligned with the new framework.
- Second, it assesses platform functionalities and governance models used internationally to support scalable assessment and analytics, translating key lessons into design requirements for Romania’s institutional and digital roadmap.

The work builds on the Bank’s earlier 2022 RAS support to INA on training needs assessments. That analysis informed national training strategies and identified priority staff segments. This report extends that work by integrating competency-based digital assessment, replacing perception-based or attendance-driven training models with an evidence-based system grounded in demonstrated skills.

The scope is limited to general digital competencies across the civil service, excluding specialized ICT roles, which require distinct technical training and oversight mechanisms. The report recognizes that the assessment and upskilling of ICT professionals should be coordinated separately, under the leadership of ADR, to align with national digitalization strategies and evolving technology standards, while remaining coherent with NACS- and INA-led HRM reforms.

Methodologically, the report draws on desk research, process mapping, international benchmarking, and targeted interviews with digital skills and TNA authorities in selected EU and OECD countries. Consultations with Romanian HR and IT working groups ensured that recommendations reflect operational capacities and system readiness. Additional collaboration with universities and training providers (including ECDL) supported the development of preliminary curriculum elements and assessment questionnaires aligned with the competency framework.

The report is structured around three core analytical components:

- Redesign of the TNA process for digital competencies (Chapter 2);
- Use of digital assessment platforms to convert evaluation into actionable learning decisions (Chapter 3); and
- Institutionalization of digital TNA, including governance arrangements, implementation pathways, and a phased adoption roadmap (Chapter 4).

An adapted TNA approach is needed for digital competencies in a system in which training needs identification is formalistic and appraisal-driven

The report proposes redesigning Romania’s TNA system for civil servants so that digital skills are identified and managed using the proposed general digital competency framework. The framework becomes the common language for what “digital competence” means in the civil service and the reference

for describing, measuring, and planning digital upskilling across seven competency areas, six of which apply to all staff and one to managers. International examples (Basque Country's IKANOS, Latvia, others) show how such frameworks can underpin TNA tools, training catalogues, and certification schemes in a consistent way.

The current TNA system is legally well-defined but still largely formalistic and appraisal-driven. Training needs are mostly derived from annual performance evaluations, consolidated administratively by HR units, and centralized by NACS for INA and other providers. This process focuses on “filling in forms,” is weakly connected to strategic priorities, and does not use competencies or robust validation/certification mechanisms. Digital training priorities therefore tend to follow ad hoc demands and available courses rather than evidence on actual digital skill gaps, and institutional roles (NACS, INA, ADR) are not yet fully aligned around a coherent digital-skills governance model.

To address these gaps, the report proposes a dedicated, platform-based TNA stream for digital competencies, which sits alongside - but not inside - the annual appraisal cycle. All civil servants would complete a baseline (self-)assessment against the full digital framework at the start of a multi-year cycle, followed by lighter annual updates focusing on priority and fast-evolving areas such as AI, data governance, and cybersecurity (assessed every year for all staff). A digital platform managed by INA would generate individualized learning recommendations, institutional and system-level dashboards, and aggregated reports for NACS and ADR, feeding directly into training design, budgeting, and national reporting. Managers are expected to shift from passive approvers to active talent developers, supported by guidance and communities of practice.

Overall, the redesigned TNA process aims to move Romania from a “managed but formalistic” TNA model to a strategic, evidence-based digital capability system. It connects competency-based assessment, foresight on future digital needs, and structured data flows into one integrated process, enabling targeted training, informed HR planning, and iterative updates to job profiles, curricula, and the digital competency framework itself.

For data-driven TNA for digital skills, a digital skills assessment platform is essential

A digital TNA platform is the backbone of a modern approach to assessing and developing digital skills across government. International experience shows that such platforms act as a single gateway that links assessment, analytics, learning recommendations, and certification. They allow administrations to move from fragmented, perception-based needs reporting to evidence-based workforce diagnostics that support targeted training investment and alignment with digital-transformation objectives. By using common competency standards (usually linked to DigComp), platforms ensure comparability across institutions and job families.

The most robust public-sector systems use hybrid assessment models, combining self-assessment with knowledge and task-based testing tailored to different role profiles. Examples such as France's PIX, the Basque Country's IKANOS/BAIT model, and Italy's “Deep Skills” initiative illustrate how layered diagnostics can produce both system-wide insights and valid individual profiles. Role-specific frameworks, such as the UK's Digital, Data and Technology (DDaT) Capability Framework, show how generic civil-service diagnostics can be complemented by deeper validation for ICT professionals, enabling differentiated learning and career pathways.

Strong institutional ownership and governance are critical to platform sustainability. High-performing models assign clear leadership to a central public institution, often supported by training academies and

digital agencies, ensuring continuity of funding, standards, and policy alignment. France's PIX consortium, Italy's coordination between the Department for Public Administration, SNA and Formez PA, Finland's dual ownership through eOppiva and the VAHTI network, and Spain's INAP-Red.es partnership demonstrate how shared governance structures link assessment tools directly to national digital strategies and civil-service reform agendas. Platforms are not isolated IT products but integral components of broader capability-building systems.

The scope of digital TNA platforms typically extends across the entire civil service and integrates assessment, learning, and reporting functions. In countries such as Latvia and Canada, platforms enable standardized diagnostics against common frameworks, while also linking results directly to learning pathways and portfolio-level training planning. In some settings, notably the UK, assessment outcomes are used more strongly to inform professional frameworks and even financial incentives for digital specialists, underscoring that TNA platforms can serve both developmental and workforce-management functions when appropriately designed.

Assessment results should translate directly into learning actions to add value. Effective platforms route users automatically to curated learning pathways delivered through national training catalogs, online platforms, or modular programs. Examples from France, Italy, and Canada show how assessment outcomes feed into practices ranging from basic IT literacy modules to advanced academies on data, cybersecurity, cloud services, or service design. This integration ensures that diagnostics do not remain descriptive but become the entry point to continuous professional development aligned with institutional priorities.

Certification, feedback, and reporting mechanisms sustain participation and enable strategic decision-making. Platforms commonly provide personalized digital-skills profiles, visual dashboards of strengths and gaps, and micro-credentials or formal certificates recognizing learning achievements. Digital badges support recognition of small learning steps, while certificates validate more substantial competence gains. Institutional dashboards allow leadership and HR units to monitor participation rates, aggregate skill levels, track progress over time, and assess training impact. International practice consistently keeps certification feedback developmental rather than punitive, avoiding any direct link between TNA results and individual performance appraisal.

Across all reviewed countries, digital TNA platforms are deliberately separated from performance management. Assessments are used for diagnostics, learning guidance, and workforce planning, not for scoring employees or influencing annual ratings. This separation is essential to encourage accurate self-reporting, broad participation, and trust in the system. Linking assessments to formal appraisal outcomes is widely seen as a deterrent that undermines the quality of data and the credibility of the process.

For Romania, the international evidence supports the creation of a single, integrated TNA platform anchored in the proposed general digital competency framework. The platform should combine scalable self-assessment with objective testing options, route results into tailored learning pathways, and issue recognized micro-credentials or certificates. INA should lead learning design and platform operation, ADR should oversee advanced ICT and data-governance pathways, and NACS should ensure methodological coherence and integration with HR processes such as recruitment planning and workforce analytics. Under this model, the TNA platform becomes not simply a digital questionnaire but a continuous learning engine linking skills diagnostics, training investment, certification, and Romania's wider digital-government transformation agenda.

For effective delivery, it is important to consolidate INA's institutional mandate on digital skills TNA and ensure a phased implementation

Finally, institutional ownership is crucial for sustainable consolidation. For this, the TNA platform development and TNA process coordination for digital competencies should be placed clearly with INA, which should be formally designated as Product Owner of the platform, with a multi-year budget and dedicated staff. NACS would ensure alignment with the wider competency-based HRM reform, aggregation standards, and future updates of the digital competency framework for HR purposes. ADR would focus on updating digital-skills priorities (e.g. cybersecurity, AI), ensuring that TNA results inform training and policy, and running a separate TNA/upskilling stream for specialized ICT roles. A joint governance structure (INA–NACS–ADR–GSG) should oversee the product roadmap, adoption targets and validation of expected digital levels by role.

To turn diagnostics into development, the platform must be tightly integrated with learning and recognition. INA and ADR should create a structured training catalogue tagged to the digital competency framework (competence area, level, modality, duration, assessment), combining INA courses, university offers and EU resources (e.g. Interoperable Europe Academy). Role-aware learning paths should be auto-generated after each assessment, mixing mandatory “floor-raising” modules (such as an annual cybersecurity hygiene course with simulated phishing) with elective deepening options. Micro-credentials and digital badges are encouraged as a recognition and motivation tool, initially kept separate from formal appraisal, but designed so they can later support career development and talent mapping once the system matures. Curriculum elements in Annex 3 provide the bridge between the framework and concrete content, with training organized by thematic learning areas rather than one-module-per-competence, reflecting the fact that digital tasks rely on clusters of interdependent skills.

Implementation should be gradual and iterative. The report proposes piloting the platform and instruments, refining items, dashboards and user journeys based on results, and documenting practical “how-to” guides for later replication. Institutions should nominate focal points and run time-bound campaigns (e.g. cyber month, AI awareness) to drive completion. A monitoring framework with a minimum set of indicators (participation, completion, gap-closure, score improvement, remediation, advanced-skills enrolment, persistent gaps, badge uptake, satisfaction, and certification rates) should track both equity and impact, disaggregated by region, institution, role and gender.

A five-phase roadmap is proposed for the operationalization of the platform driven digital skills TNA process. Phase 1 focuses on governance setup and deciding between the two possible delivery models. Phase 2 covers detailed design and prototyping (functional and technical specifications, initial item bank, basic wireframes). Phase 3 develops and pilots the full platform with several thousand users in a small number of institutions. Phase 4 extends access to all ministries and agencies, embeds the TNA into the regular HR cycle, integrates with INA's LMS and catalogues, and issues annual individual and institutional reports. Phase 5 institutionalizes continuous improvement and progressive integration with EU-level digital academies and certification frameworks. Together, these measures would make the digital-skills TNA a permanent, trusted instrument of Romania's competency-based HRM and digital-government reform.

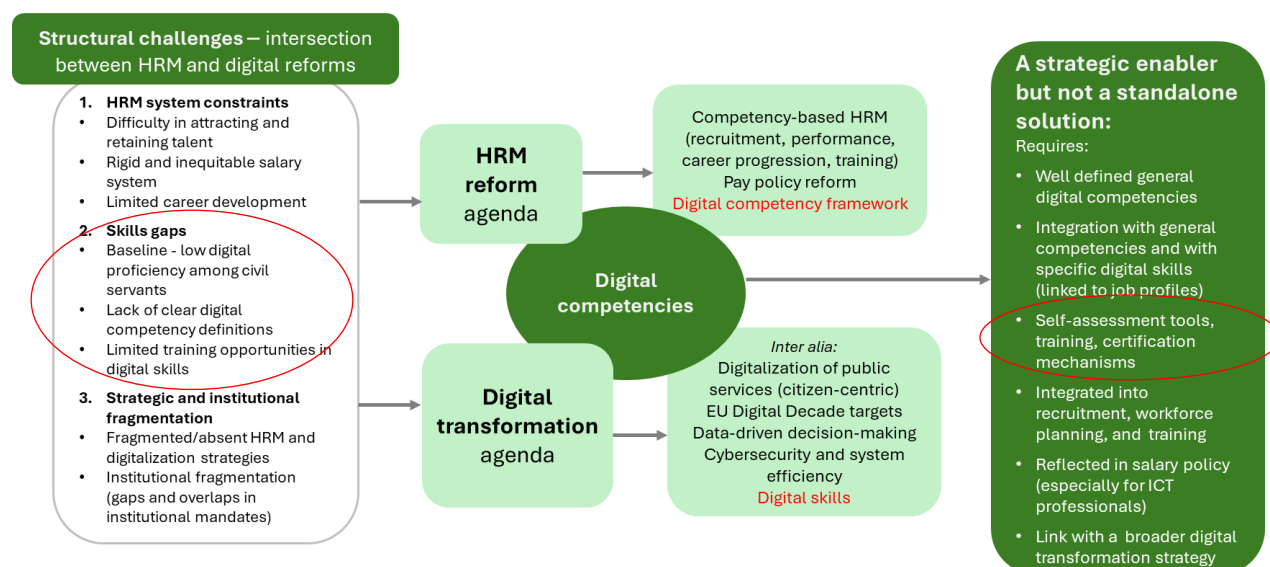
Operational annexes included in this report provide practical instruments: sample self-assessment items aligned with competency levels; standardized reporting templates for individual and institutional assessments; indicative elements of learning curriculum mapped to the general digital competency framework; and a structured, knowledge-based TNA questionnaire to support early pilots.

1. Introduction: context and scope

1. **The development of a general digital competency framework for the Romanian public administration offers a critical foundation for digital transformation reform efforts.** Public servants need to work in new, digitally enabled ways, using data effectively, collaborating across institutions, and managing digital risks. A general digital competency framework for the public administration offers a structured model for defining and measuring digital skills across the civil service. It also provides the foundation for differentiating between baseline skills required for all public servants and advanced competencies needed for specialized roles. However, its success will depend on its integration into key HRM tools and processes, particularly those focused on assessing training needs and guiding workforce development.
2. **Building on these premises, the World Bank, in close collaboration with the European Commission, is supporting the Government of Romania through a Technical Support Instrument (TSI) project in developing a general digital competency framework.** The project is implemented jointly with the National Agency of Civil Servants (NACS), the Authority for the Digitalization of Romania (ADR), and the National Institute for Administration (INA). The project's overarching objective is to strengthen the capacity of Romania's civil service to support digital transformation by developing and operationalizing a general digital competency framework.
3. **Earlier outputs of the project established the analytical and conceptual foundation for this framework.** **Output 1** provided the evidence base, including an assessment of international practices, a review of the national HRM and digital policy context, a job analysis of key civil service roles, and a foresight exercise to anticipate emerging competency needs. These elements ensured that the framework reflects both current realities and future requirements of public administration. **Output 2** proposes the design of the digital competency framework, including detailed competency descriptors and complexity levels. **Output 3** proposes the approach for legal adoption and the methodology for operationalization.
4. **Recommendations on digital skills assessment for the civil service constitute a key operational element of the theory of change included in Output 1¹.** Consequently, the scope of the present report is meant to cover the elements that would ensure that the general digital competency framework becomes a practical instrument for evidence-based HRM. By systematically assessing current digital skill levels across institutions, the assessment generates the data needed to identify competency gaps and prioritize training interventions. This directly supports the broader objective of aligning workforce development with Romania's digital transformation priorities. As digital competencies are at the intersection between HRM and digital transformation reform priorities, reform interventions need to focus specifically on the upskilling of the public administration (as shown in the theory of change in Figure 2). In doing so, the assessment of digital skills needs to anchor the framework within the HRM system, enabling a strategic approach to building a digitally capable public administration workforce.

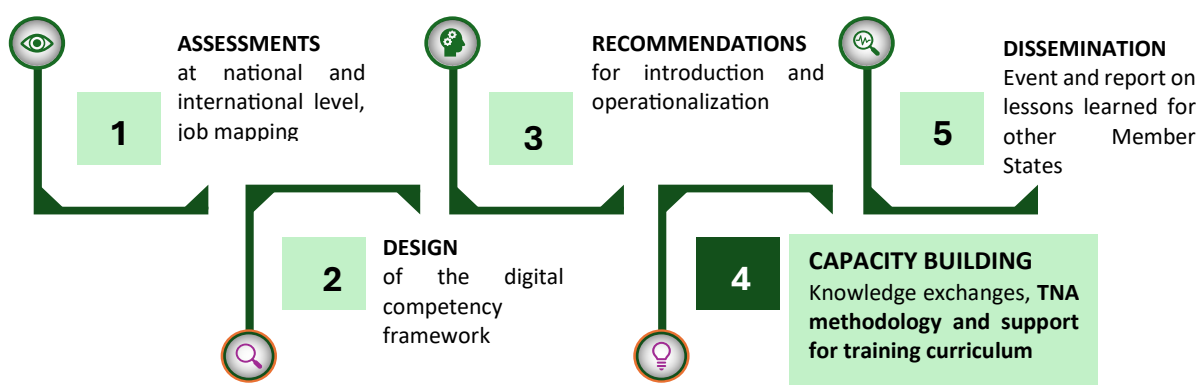
¹ World Bank, Output 1 - *Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service, Taking into Account Relevant Policies at the National and European Union Levels*. Developed under the TSI project "Romania: Developing a General Digital Competence Framework for Civil Servants". Available at: <https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745>.

Figure 2 Theory of change – Digital skills assessment and learning are core to introducing the digital competency framework



5. This report constitutes Output 4 and builds upon previous work by proposing a framework for Training Needs Assessment (TNA) that translates the digital competency framework into a practical instrument for workforce development. This report supports the operationalization of the framework by proposing an updated framework for assessing digital skills training needs. It corresponds to Activity 4 of the TSI project by supporting the INA in strengthening its TNA methodology to align with the newly developed digital competency framework. Activity 4 also included support for capacity development through knowledge exchanges, with the relevant findings from the two study tours organized in January-February 2025 already captured in dedicated study visits reports that accompanied the delivery of Output 1.

Figure 3 TSI project intervention logic: Report corresponds to Activity 4



6. The focus on TNA and development of learning instruments is essential for the operationalization of the digital competency framework proposed under Output 2, while avoiding the risks associated with premature, full-scale implementation across all HR processes. In Outputs 2 and 3, the Bank recommended introducing general digital competencies only in recruitment and training, rather than extending them immediately to performance management, promotion, or mobility. This phased approach helps prevent digital competencies from becoming a purely formal or compliance-driven exercise, ensuring instead that they are meaningfully embedded in HR practices.

7. **This report aims to provide a structured approach for linking digital competency needs and learning interventions.** It presents insights and includes recommendations aimed to:
- identify digital competency gaps across institutions;
 - determine and prioritize training needs;
 - align learning objectives and training curricula with the defined competency descriptors and proficiency levels; and
 - establish feedback loops to update both training programs and competencies over time.
8. **In parallel, the report dives into relevant international examples of digital assessment/self-assessment tools used in public administrations.** Several EU and OECD countries have deployed digital platforms that allow public employees to evaluate their own digital skills and identify training needs aligned with national or European competency standards. Notable examples - such as Italy's *Syllabus*, Canada's *Digital Competencies Self-Assessment* - illustrate the potential of such tools to enhance individual learning, institutional planning, and system-wide capacity-building.
9. **A dedicated analysis is included on how assessment/self-assessment platforms can support the application of the proposed TNA methodology.** This component responds to INA's need for practical, scalable tools that facilitate consistent and structured identification of digital competency gaps. By assessing the functionality, design, and implementation of peer platforms, the report offers clear recommendations for developing a self-assessment solution tailored to the Romanian context.
10. **The report follows two main analytical layers, focusing both on process structure and platform design for digital skills assessment.** First, it analyzes the existing TNA methodology and identifies limitations and opportunities for improvement, particularly in relation to digital skills. Second, it conducts a comparative review of digital skills self-assessment platforms in other countries, drawing lessons that can inform Romania's institutional and technological roadmap.
11. **The report also builds upon previous analyses and recommendations on TNA developed by the Bank for INA in 2022².** Under this previous Reimbursable Advisory Services (RAS), the Bank analyzed the training needs of Romanian public administration staff, identifying priority areas and target groups to support national strategic objectives. The findings were meant to guide the national training strategy and the updating of INA's training portfolio. The Bank also proposed a model and methodology for conducting TNA within the public administration and included a survey on citizen perceptions of staff competencies. In addition, support was also provided to distill lessons from relevant international TNA practices relevant for Romania.
12. **The objective of this report is to support Romania's transition to a user-centered, data-driven approach to digital skills development in the civil service.** An improved TNA methodology, supported by an accessible (self-) assessment tool, can enable the systematic identification of skills gaps, better align training with actual workforce needs, and support strategic workforce planning. These efforts directly contribute to broader reform objectives under the National Recovery and Resilience Plan (NRRP) and Romania's alignment with EU Digital Decade targets.

² Recommendations developed by the Bank under the Reimbursable Advisory Services Agreement on Strengthening the INA's Capacities to Improve the Training Policy Framework in the Romanian Public Administration (P169456) *Output 1 – Report identifying enabling conditions for Training, Deliverable 1.1 Report on training needs assessment for public administration staff*. Available at: <https://ina.gov.ro/wp-content/uploads/2023/03/INA-RAS-Output-1.1-TNA-report-Copy.pdf>.

13. **In terms of scope, this report focuses on TNA processes and tools for the operationalization of the general digital competency framework for the public administration and not on the specialized IT roles.** However, it is important to note that IT roles require a distinct and more technical process TNA and upskilling. Given the specificity and rapid evolution of digital technologies, such a process should be coordinated by a dedicated entity with expertise in digital transformation – such as the Authority for Digitalization of Romania (ADR). This entity would be responsible for systematically identifying skills gaps across IT functions, aligning them with emerging digital standards and government technology priorities, and facilitating access to relevant training and certification programs. A dedicated coordination mechanism led by a digitalization-focused institution would ensure consistency between institutional IT workforce planning, national digitalization strategies, and the broader competency-based HRM reforms coordinated by NACS and INA.
14. **Methodologically, the report was developed based on a mixed-method approach combining desk research, process mapping and targeted interviews.** The focus of the report is on the TNA process structured around INA's mandate, to ensure that the future implementation is rooted in the existing institutional ecosystem for TNA and training for civil servants. It draws on previous analyses of TNA practices conducted under earlier project phases and examines INA's existing methodology in relation to digital competency identification. The analytical process included a review of international experiences and good practices, complemented by five targeted interviews with TNA authorities and institutions responsible for digital skills assessment in selected EU and OECD countries³. In addition, consultations were held with members of the HR and IT working groups involved in designing Romania's digital Competency Framework for the civil service, who emphasized the importance of aligning assessment tools with training and capacity-building priorities. This evidence-based and consultative approach ensures that the report's findings and recommendations are both contextually grounded and informed by relevant international models.
15. **The development of this report also relied on consultations with university representatives and private sector relevant training providers.** INA is already engaged in a close collaboration with universities and this delivery model constitutes a solid foundation for building the future delivery mechanisms for digital upskilling of public administration staff. The development of the elements of curriculum, as well as the preliminary TNA questionnaire included in this report was ensured in collaboration with university professors specialized in public administration and digitalization. Furthermore, these elements were also subject to consultations with key training providers (such as ECDL).
16. **The report is structured in four chapters and includes four annexes:**
- Chapter 2 examines the redesign of the TNA process for digital skills, highlighting how a competency-based approach and the new general digital competency framework can strengthen the identification of skill gaps across Romania's public administration.
 - Chapter 3 explores how digital TNA platforms can transform assessments into actionable learning decisions. It reviews assessment methods supported by dedicated IT platforms and outlines key functional characteristics of effective digital (self-)assessment tools.
 - Chapter 4 focuses on institutionalizing the digital-skills TNA process, presenting the design principles, governance arrangements, and implementation mechanisms required to ensure sustainability. It discusses institutional ownership, implementation pathways, assessment design, integration of learning pathways, and the proposed roadmap for gradual adoption.

³ From Italy, Spain, Latvia, UK and Portugal.

- Annex 1 includes sample self-assessment items aligned with the General Digital Competency Framework, illustrating how each competence level can be evaluated using a standardized Likert-scale approach.
- Annex 2 includes the recommended structure, layout, and content of digital-skills assessment reports, with examples of key indicators, charts, and summaries for both individual and institutional results.
- Annex 3 proposes suggested elements for future curriculum, learning outcomes, and indicative topics derived from the national digital competency framework to support targeted training interventions.
- Annex 4 proposes a structured TNA knowledge-based questionnaire for competency areas 1-6 for proficiency levels A and B (which are applicable to the majority of civil service jobs).

2. The TNA process. Redesigning TNA for digital skills

2.1 The proposed general digital competency framework as the basis for TNA

17. **A general competency framework already serves as a key reference for the civil service HRM system, informing recruitment and training.** Its further operationalization benefitted from financing from the NRRP, particularly through Milestone 419 – Operational Competence Frameworks in the Central Public Administration. Within this reform, NACS is responsible for implementing a competency-based approach across the public administration, linking career management, selection, and performance management to measurable competencies. A draft legislative act was foreseen under Milestone 419 and was developed with technical assistance to expand the integration of the general competency framework into core HRM processes, targeting also the performance management system, including the TNA cycle⁴. This will ensure that competencies become the common denominator across HR functions, moving from fragmented administrative practices to a coherent, capability-based system. The legislative proposal draws on the design model developed under the earlier SIPOCA 136 project⁵, and its adoption will mark the effective operationalization of the framework at central-government level, followed by phased implementation across the wider civil service.
18. **INA has already begun integrating the general competency areas into its training curricula, reflecting the general competencies into course learning outcomes.** For example, INA's training programs for senior and managerial civil servants are increasingly aligned with the general competency framework adopted under the Administrative Code. While the structure of the programs does not strictly mirror the grouping of the general competencies for managers, the course content and learning outcomes reflect broadly the substance of the competency framework model.
19. **However, the institutional TNA process remains largely decoupled from the competency-based approach, as described in the next section of this report.** The identification of skill gaps through the

⁴ Reform 3 under NRRP is presented at: <https://www.anfp.gov.ro/en/projects/projects-in-implementation-menu/nrrp-projects/projects-in-implementation-list/operationalization-of-central-public-administration-competence-frameworks>.

⁵ Supported by the World Bank under the HRM RAS.

annual TNA cycle is not yet aligned to the competency framework or supported by shared tools. This limits the ability of institutions to generate comparable data and to link staff development plans directly to competency profiles.

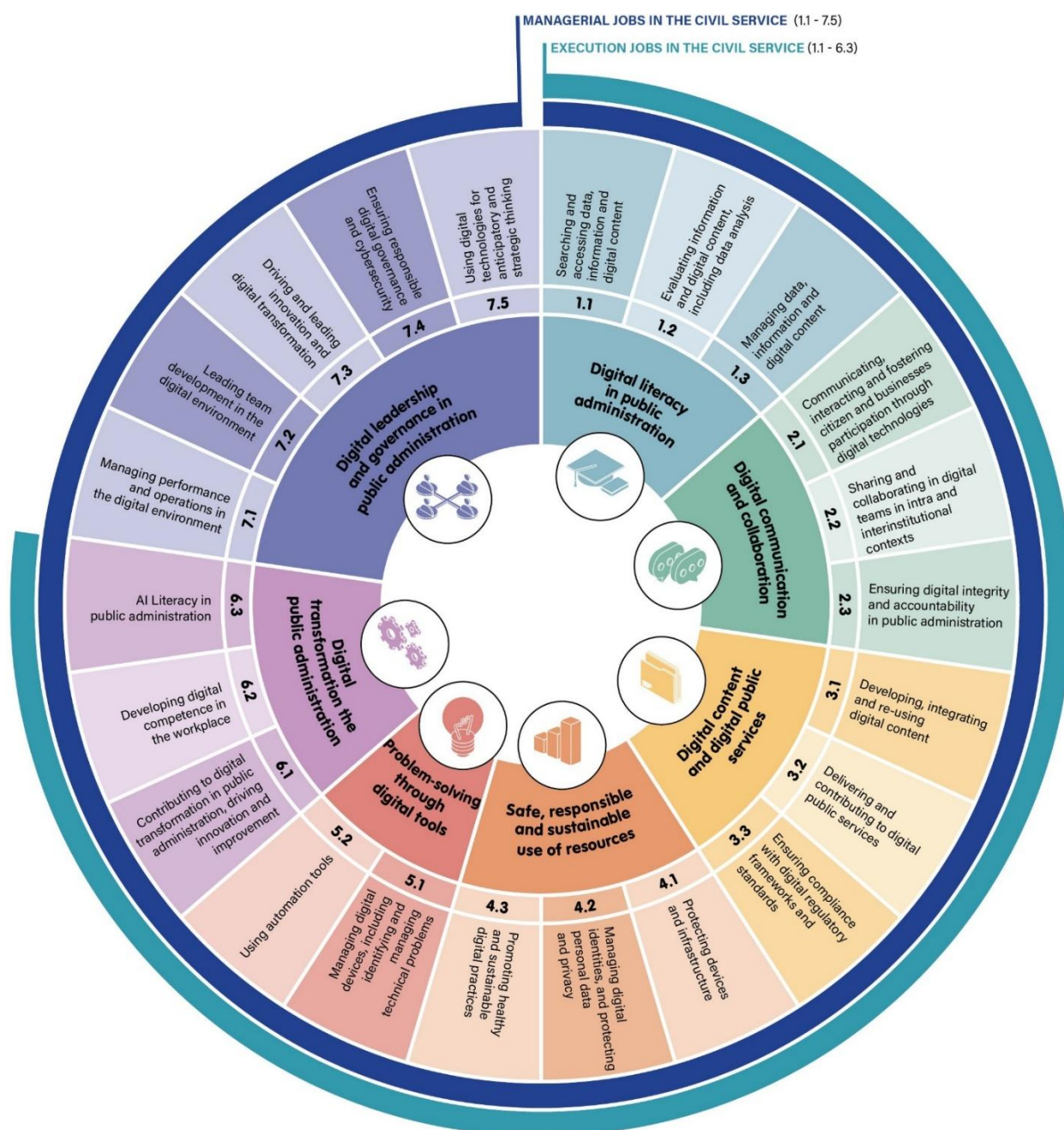
20. **Moving beyond the general competency framework already in place, digital competencies necessitate a consistent shared language for what “digital competence” means in the public administration.** DigComp already offers a shared language and conceptual model for digital competence, helping policymakers in EU Member states to advance their digital skills agenda for public servants. A detailed overview of DigComp 2.2 is included in Output 1 developed under the TSI project. Member States draw on DigComp to design TNA platforms, training catalogs, and, in some cases, certification pathways⁶. This uptake reflects DigComp’s role in harmonizing digital skill standards across the EU, ensuring that public employees and citizens share a common understanding of the competences needed in a digital society.
21. **Spain’s Basque Country operationalized DigComp through IKANOS, producing tailored competence profiles for government roles.** IKANOS⁷ uses DigComp as the conceptual backbone and generates public-sector-relevant competence maps and personalized development roadmaps⁸; it is designed for large-scale use and has been deployed across public administrations as well as other sectors. Details on the implementation of the IKANOS framework in TNA and learning are included in chapter 3 of this report and are also available in the review of international experience conducted as part of Output 1 under the TSI project.
22. **Latvia is also a recent relevant example of how DigComp can be embedded into their civil service frameworks to create a standardized, government-wide approach to digital competence.** In this case, DigComp serves as a harmonized vocabulary for describing and measuring digital skills across policy design, operational processes, and service delivery. More details on the Latvian case study are included in Chapter 3 of this report. This approach preserves comparability across governments while recognizing the varied digital capability needs of different roles.
23. **The general digital competency framework developed under Output 2 of this TSI project establishes the reference standard for conducting TNA and planning targeted training interventions.** The framework is closely aligned with DigComp 2.2 and builds upon the foundation of DigCompRO. The framework includes seven competency areas, out of which six apply to all civil servants and the seventh one is devoted to managerial positions. Across these areas, competencies closely mirror the DigComp logic, but with important additions and updates that are relevant for the public administration personnel. A brief overview of the model is reflected in **Eroare! Fără sursă de referință..**

⁶ Awareness of the DigComp framework among the CEPIS community - CEPIS
<https://cepis.org/digcomp-report-2021/>

⁷ IKANOS official webpage <https://ikanos.eus/en/digital-competences/>

⁸ Refer to Output 1 of the TSI for further details: Report on the assessment of the digital competencies needed in the Romanian civil service. World Bank.

Figure 4 The proposed general digital competency framework for the Romanian public administration



2.2 Overview of the current TNA process in the Romanian public administration

24. This section provides an overview of the current TNA process in the Romanian public administration, based on previous analyses conducted by the Bank. As such, it does not include an in-depth evaluation of the TNA system, but rather highlights its key features, advantages and challenges, to

lay the basis for defining a specific TNA process model for digital skills, without completely decoupling it from existing institutional mandates and current HRM characteristics.

25. **Given that institutional roles for HRM and digitalization were already analyzed in Output 1, this report makes only specific references to relevant responsibilities for training and TNA.** Output 1 developed under the TSI project includes a dedicated section covering strategic and institutional aspects related to the development and implementation of digital competencies in the Romanian public administration, at the intersection between HRM and digital transformation.
26. **An evaluation conducted by the Bank in 2022⁹ classified the Romanian TNA system as having many elements of the “managed” phase of development (phase 3 out of 4), based on its objectives and level of HRM integration, but it is still generally a formalistic exercise.** The maturity model for TNA outlines four progressive stages that reflect how systematically and strategically organizations approach training. The classification criteria across these stages include the degree of standardization, stakeholder involvement, institutional integration, resource allocation, and evaluation focus, moving from fragmented and reactive approaches to a coherent, outcome-driven system. In the *Initial* stage, training needs are identified ad hoc and inconsistently, often by external experts, with little internal capacity or evaluation. The *Repeatable* stage introduces standardized and regularly applied methods, managed by L&D specialists, though still focused mainly on inputs such as budgets and training days. The *Managed* stage integrates L&D into broader HR processes, with line managers participating and competency frameworks guiding training alignment; evaluation expands to outputs and performance indicators. Finally, the *Strategic* stage positions L&D as a core enabler of organizational reform and future readiness, supported by governance structures, digital tools, and outcome-focused evaluation.
27. **The legal framework in place describes training rights and obligations and process steps linked to the performance appraisal process.** The Administrative Code provides for the right and obligation for public servants to continually improve their skills and professional training¹⁰. These provisions are mirrored by the obligation that public authorities and institutions have to ensure that each civil servant attends at least a professional training and development program once every two years. The TNA process is conducted annually; it is explicitly formally linked to the staff annual appraisal system. GD No. 1066/2008 states that the evaluation report on the individual professional performance must include the areas in which the civil servant needs additional professional training¹¹. The civil servants in management positions identify and report training needs of the subordinated civil servants, as part of the performance appraisal process highlighting priority areas and the criteria used for identifying those areas¹². Civil servants have the right to be consulted by their immediate superiors when their proposed individual training needs and programs are determined. Public authorities and institutions also have an obligation to produce annual professional development plans for contractual staff. They must also provide budget funds for supporting the estimated costs of the professional training and development

⁹ 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>.

¹⁰ Article 458(1) of GEO no. 57/2019 on the Administrative Code. More specifically, according to Article 398(3) of GEO no. 57/2019 on the Administrative Code, high-level civil servants have the obligation to attend professional development courses, usually every year.

¹¹ Article 16(1) of GD No 1066/2008 (this provision mirrors Article 485(9) of the Administrative Code which states that, as part of evaluating the individual professional performance of civil servants, requirements regarding the professional training of civil servants are set out).

¹² Article 17(1) of GD No 1066/2008.

programs¹³. However, there are no legal provisions that detail the process of producing and approving the annual professional development plans for contractual staff.

28. **Formal responsibilities for identifying training needs, developing annual training plans and monitoring implementation are also established within the HR units in the public authorities and institutions.** The civil servants, designated by the head of the public authority/institution to implement the rules regarding the professional training of civil servants,¹⁴ centralize the reports on the training needs of the civil servants as derived from the performance appraisal process and develop proposals for a professional development plan. The annual professional development plan for civil servants must be based on the priority areas for training programs set out, in the case of civil servants, by order of the NACS President¹⁵ or, in the case of high-level civil servants, by Government Decision¹⁶. The proposed plan and budgetary allocations are subject to consultation with the joint committee (“comisia paritară”)¹⁷. These proposals are submitted to the head of their respective public authority/institution¹⁸.
29. **NACS centralizes the training needs of civil servants as submitted by public institutions and prepares an annual report.** The annual report presents the results of the TNA process, which mainly consists in centralizing training needs included by managers in individual performance appraisal reports¹⁹. Priority areas for training programs addressed to civil servants must be set out by order of the NACS²⁰.
30. **Training needs are then made available to the INA and to other professional training/development providers.** In doing so, the INA and other training providers are expected to tailor their programs to suit the training needs of civil servants.
31. **INA is the authority responsible for the professionalization of the central and local public administration staff²¹, but its role in TNA is not sufficiently leveraged in the current HRM system.** INA ensures specialized training for high level and managerial civil service positions, as well as a broad range of non-exclusive professional training and development programs for civil servants, contractual staff, local elected officials, public managers, and other public administration personnel. However, INA’s training portfolio is constrained by the current mandate of the NACS which only covers civil servants. INA develops its programs based on training needs centralized by NACS, meaning that data on contractual staff training needs remain unavailable. This creates a systemic gap: INA is legally mandated to train contractual personnel but lacks an institutional mechanism to receive and process their training needs. Details on these current roles and applicable legal framework are already analyzed in the Bank’s report on the TNA system from 2022²².

¹³ Article 551(1) of GEO no. 57/2019 on the Administrative Code.

¹⁴ Article 15 of GD No. 1066/2008

¹⁵ Article 11 of GD No. 1066/2008.

¹⁶ Article 12(1) of GD No. 1066/2008.

¹⁷ Article 17(3) of GD No. 1066/2008.

¹⁸ Article 17(2) of GD No. 1066/2008.

¹⁹ The 2025 report on the professional training of civil servants is available at: https://www.anfp.gov.ro/media/johbo1mc/raport-formare-2025_final.pdf.

²⁰ According to Article 11 of GD No. 1066/2008 and Article 401 of GEO 57/2019 on the Administrative Code.

²¹ Article 2(1) of GO No. 23/2016.

²² 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>.

32. **To compensate for this legal gap, INA conducts a distinct and parallel training needs analysis exercise to inform its training programs for the following year.** The Directorate for Short-term Training (DPP) of INA and its five territorial centers send a questionnaire annually to local and central public administration institutions to collect staff perceptions about training needs for a pre-defined list of training programs²³.
33. **Another relevant entity is ADR, which is responsible for fostering digital talent and skills within the Romanian public sector, but it doesn't have a de jure role in TNA, not even for the specialized IT roles in the public administration.** In their recent report Digital Government Review of Romania²⁴, OECD had noted that ADR's responsibility to develop digital talent and skills in the Romanian public sector is encompassed by the legal role of the NACS as overarching institution in charge of national civil service policy, recruitment, and talent development in the Romanian government. In this context, Output 1 of this TSI project recommends to update the governance system for HRM and digital upskilling²⁵, to ensure that NACS is capacitated for oversight and coordination on the competency-based HRM reform agenda across the civil service, ensuring that digital skills are part of the broader reform framework; that INA is capacitated to lead the development of general digital competencies in the public administration and that ADR is capacitated to lead and deliver the operationalization of specialized IT roles in the central public administration, including their upskilling initiatives.
34. **The current process for training needs is rather formalistic and weakly connected to strategic priorities, although the participation in TNA reporting has improved.** Strategic training priorities set by the NACS in the area of digital skills are based on inputs from institutions, but these are not systematically aligned with broader policy frameworks. Most managers and HR staff define training needs based on short-term or individual preferences rather than institutional or strategic objectives. The result is a fragmented system where individual, institutional, and national priorities are poorly correlated. Nonetheless, there are signs of improved participation in recent data collection efforts. The overall institutional response rate reached 32.7 percent in 2025²⁶, up by about seven percentage points from the previous year. Central public administration bodies (72.1 percent) and county councils (95.1 percent) were almost fully represented, while towns and municipalities also achieved a solid 70.5 percent response rate. However, commune-level authorities remain underrepresented, with a 26.9 percent response rate, which lowers the representativeness of the TNA results at the national level. However, this still marks a major improvement compared to 2019, when only about 4 percent of public institutions that employ general civil servants had submitted training needs to the NACS, as required by the applicable legal framework.²⁷
35. **To conclude, TNA is still approached more as an administrative task linked to the annual performance appraisal, rather than as a strategic management tool, as noted by the Bank in 2022.** NACS and INA depend on data reported by institutions, however, no public body conducts systematic, forward-looking TNA at the individual, institutional, and system levels²⁸. HR departments provide administrative

²³ Ibidem.

²⁴ OECD (2023), Digital Government Review of Romania: Towards a Digitally Mature Government, OECD Digital Government Studies, OECD Publishing, Paris, <https://doi.org/10.1787/68361e0d-en>

²⁵ Recommendations included in Outputs 2 and 3 under the TSI project.

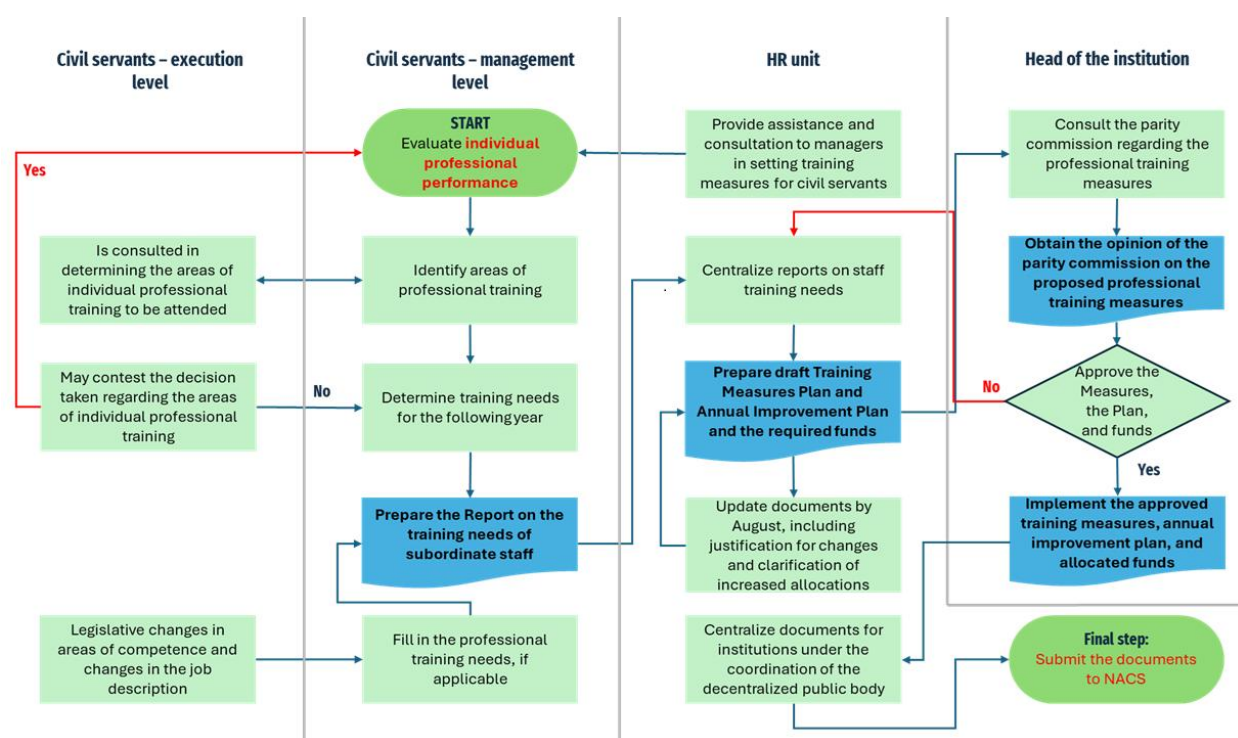
²⁶ See NACS, Report on the professional training of civil servants, 2025. The results of the centralization process, 2025. Available at: https://www.anfp.gov.ro/media/johbo1mc/raport-formare-2025_final.pdf

²⁷ See NACS, Report on the professional training of civil servants, 2019.

²⁸ 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

rather than methodological support, and few institutions measure the impact of training. Therefore, the TNA process in Romania's public administration continues to be approached primarily as an administrative extension of the annual individual performance appraisal. As illustrated in Figure 5, the institutional TNA process is initiated and largely driven by individual-level evaluations conducted by managers, with limited connection to broader organizational or sectoral priorities. The process relies heavily on each manager's capacity to identify and justify training needs, without structured analytical or competency-based instruments to guide decisions. HR units mainly consolidate the reports received and provide procedural rather than methodological support, while the role of institutional leadership is confined to approving plans and budget allocations. Consequently, the process functions as a bottom-up administrative workflow centered on individual appraisals, not as an integrated mechanism for aligning workforce development with institutional strategies or future skill requirements.

Figure 5 The TNA process at institutional level, per the legal framework – centered around the individual performance appraisal process



Source: Authors' elaboration

36. Furthermore, the absence of structured validation and certification mechanisms for acquired skills undermines the credibility, comparability, and portability of digital-skills assessments in Romania's public administration. These gaps are particularly challenging in the digital domain, where rapid technological change requires clear standards and recognized credentials. In practice, managers lack benchmarks for judging proficiency, HR cannot aggregate relevant data across institutions, and staff have few recognized credentials to signal attainment or support mobility. For digital competencies, current arrangements for recognition/validation/certification of digital skills lead to considerable

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>.

challenges and hamper mobility, recruitment and promotion systems, as signaled by HR experts during the consultation phases for the design of the general digital competency framework. A dedicated validation and certification system would be needed to set relevant skill standards, accredit training providers accordingly, and maintain a credential registry that HR systems can use for verification, as recommended in Output 3 under the TSI project.

37. **In this context, the current TNA process is not structured, nor does it rely on adequate tools to allow the identification of digital skills needed in the public administration.** As a result, digital training priorities are rarely derived from data on actual skill needs, but from ad hoc preferences or available course offers. This disconnect prevents institutions from systematically building the digital competencies required for interoperability, data-driven decision-making, and the implementation of Romania's broader digital-government agenda.

2.3 Towards a targeted TNA process for digital competencies

38. **A dedicated, stand-alone TNA stream for digital skills should sit alongside - rather than inside - the annual appraisal cycle.** A linkage between these processes should exist, by recording in the appraisal file the learning path resulting from the digital-skills TNA, but the TNA should not be turned into a rating instrument. This preserves a single record while keeping diagnosis (TNA) and judgement (appraisal) functionally distinct, which is the precondition for unbiased, future-oriented skills planning.
39. **The process needs to be structured around the right tools, mainly centered around an assessment platform, to ensure evidence.** In a recent assessment²⁹, OECD underlined that systematic assessments of digital skills among civil servants are still uncommon, with most institutions relying on qualitative inputs from staff and managers about their perceived training needs. These fragmented and perception-based approaches provide useful insights but lack the consistency and comparability required for evidence-based workforce planning. To achieve a more reliable and scalable understanding of public-sector digital capabilities, the OECD recommendations were structured around the role of self-assessment tools and performance-based tests aligned with recognized frameworks such as DigComp. International experience illustrates the value of this approach. A platform-based approach to TNA for digital skills enables diagnostics at scale. Relevant characteristics of such platforms are extensively analyzed in Chapter 3 of this report.
40. **Future needs should also be covered in today's TNA.** Each yearly cycle should collect insights from foresight and strategy - such as for example the Interoperable Europe agenda, data-driven government priorities, AI oversight, and cybersecurity requirements, so the TNA does not merely catalogue current deficits but anticipates role shifts. Such a foresight exercise was already conducted and is reflected in Output 1³⁰ developed under the TSI project.
41. **The frequency and scope of the TNA process should be legally regulated and adapted as part of a multi-annual digital capability development plan.** The process should combine a comprehensive

²⁹ OECD, Burtscher, M., S. Piano and B. Welby (2024), "Developing skills for digital government: A review of good practices across OECD governments", *OECD Social, Employment and Migration Working Papers*, No. 303, OECD Publishing, Paris, <https://doi.org/10.1787/f4dab2e9-en>.

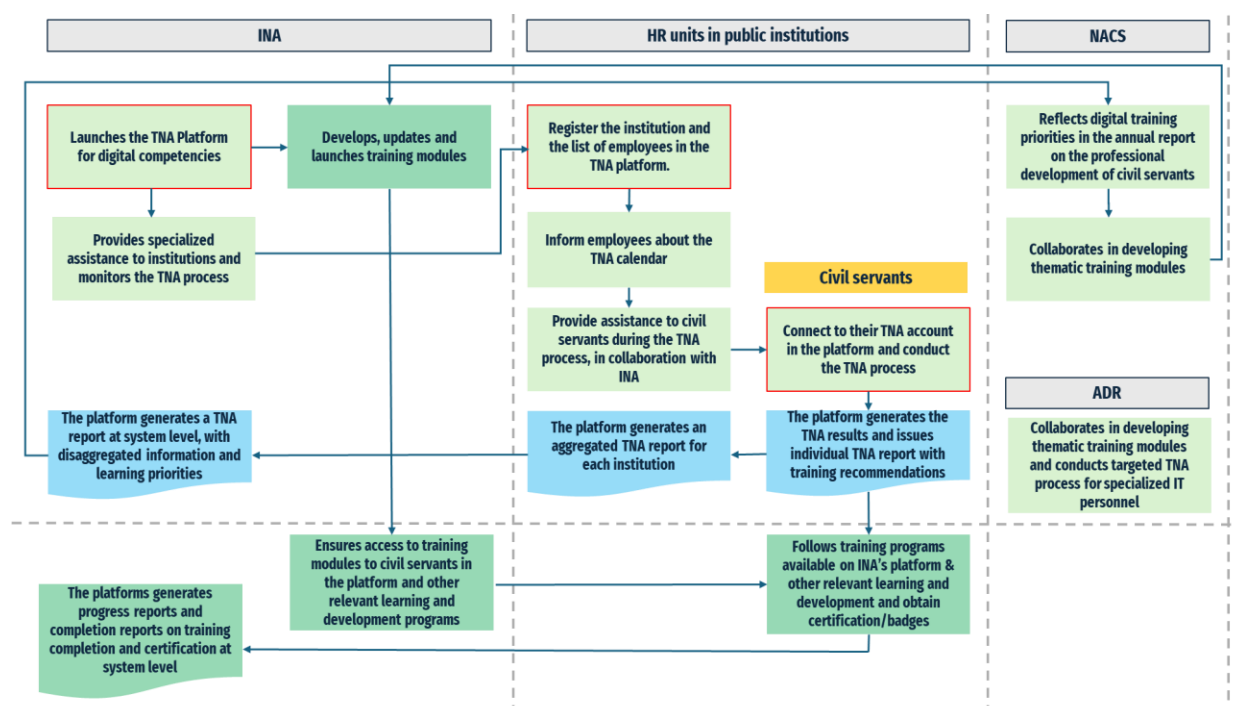
³⁰ World Bank, Output 1 - *Report on the Assessment of the Digital Competencies Needed in the Romanian Civil Service, Taking into Account Relevant Policies at the National and European Union Levels*. Developed under the TSI project "Romania: Developing a General Digital Competence Framework for Civil Servants". Available at: <https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745>.

baseline assessment with targeted annual updates, underpinned by clear legal and methodological provisions. At the beginning of each multi-year cycle, all civil servants should complete a baseline (self-) assessment covering the full general digital competency framework. This initial exercise would establish a reference point for capability levels across the various competency areas, forming the basis for individual learning plans and institutional workforce planning.

42. **In subsequent years, the annual self-assessment should focus on priority and fast-evolving competencies, as determined by each institution in line with strategic and technological developments.** Areas such as digital transformation, artificial intelligence, and data governance should be reassessed regularly to track progress and identify emerging needs. Importantly, cybersecurity should be treated as a core priority competency, assessed every year across all roles, regardless of job function or grade. Cyber awareness, information security, and safe digital practices are fundamental to the resilience of public institutions and must be monitored continuously, not cyclically.
43. **Each assessment should lead to tailored development recommendations that feed into individual learning plans.** Once the performance management system is aligned with the competency-based HRM reform developments, and the system is fully capacitated to run periodic digital skills TNA using a dedicated platform and to ensure digital upskilling through relevant training modules, the results of the digital skills TNA process could also feed into the performance discussions. Institutions could adapt the focus of their annual TNA cycle based on updated risk assessments, technological changes, or policy priorities, ensuring both relevance and flexibility.
44. **Data flow and reporting should be simple and decision oriented.** Institutions should have access to timely information, ideally through dashboards that (i) benchmark their staff against national baselines, (ii) surface gaps by types of jobs, and (iii) translate gaps into costed training plans. Nationally, the lead body should issue an annual portfolio report that rolls up needs by ministry/role cluster and publishes binding guidance for the next budget cycle (e.g., mandatory modules, priority cohorts). Spain's structured, framework-led approach shows how competency models can underpin portfolio-level guidance and procurement of training at scale.
45. **A new platform-based TNA process is expected to introduce a digital, integrated, and data-driven model that simplifies how training needs for digital competencies are identified, analyzed, and addressed** across Romania's public administration, ensuring coordinated action between INA, NACS, ADR, HR units, and civil servants. Figure 6 presents the proposed process through the INA digital platform. The process starts with INA launching and managing the platform, developing and updating digital-skills training modules, and providing technical assistance to institutions. HR units in public institutions register their institutions and staff on the platform, inform employees about the TNA calendar, and support them during the process. Civil servants then log into their individual accounts to complete the TNA (self-) assessment, after which the platform automatically generates individual, institutional and system-level TNA reports. These aggregated reports identify learning priorities, direct individuals towards existing learning programs and also guide the design of training modules. NACS integrates the digital-skills training needs into the annual professional development report and collaborates with INA to develop thematic modules. ADR also collaborates in this process³¹.

³¹ As this report focuses on the general civil service, it does not cover the role of ADR in managing targeted TNA and development of the specialized ICT personnel. Output 2 – the connected report on proposed ICT roles includes details on the role of ADR in developing the ICT workforce for the public sector.

Figure 6 TNA process for digital competencies adapted to be deployed within current legal mandates



46. **The proposed TNA process for digital competencies aligns broadly with the existing legal framework governing professional training and TNA in Romania's public administration, while addressing its current operational limitations.** The Administrative Code (GEO 57/2019) and GD no. 1066/2008 establish the legal basis for identifying and planning civil servants' training needs, linking them to the annual performance appraisal and mandating institutions to prepare annual professional development plans. The INA digital TNA platform simplifies and modernizes this process for digital competencies by transforming it into a structured, evidence-based system that automates data collection, links (self-)assessment and institutional aggregation, and directly connects civil servants, HR units, and national authorities (NACS, INA, ADR) through a single interface. This ensures real-time visibility of training needs, generates consistent reports at institutional and system levels, and integrates results into learning pathways and certification. In doing so, the platform operationalizes the existing legal mandates rather than replacing them, streamlining compliance, reducing reporting burdens, and enabling Romania's TNA system to evolve from a "managed" to a "strategic" stage of maturity, consistent with competency-based HRM and digital-government reform goals.
47. **Managers' capability should also be enhanced to make them an active part in the TNA wider ecosystem for public sector digital capability.** Practice-oriented manager training and communities of practice can play an important role in developing managerial capabilities for enhancing digital skills across the civil service. This combination turns managers from passive approvers into active talent developers and makes the TNA a living process rather than a yearly formality. OECD guidance on developing digital government skills supports the shift from course-centric to capability-centric practices, underlining the need to align support across an entire learning system, that includes formal and informal training methods, including through communities of practice, networks of experts. These can serve a dual role: coordination enhancement and learning, as it is for example the case in Finland for the VAHTI network on cybersecurity (Box 1).

Box 1 Strengthening learning and cooperation through managerial and professional networks and coordination boards: case of Finland³²

Finland's Digital and Population Data Services Agency (DVV) coordinates the VAHTI network, a long-standing collaborative platform that develops and sustains digital and cybersecurity capability across the Finnish public sector. VAHTI brings together the management and experts responsible for cyber and digital security from more than 40 public organizations. It operates through a Digital Security Management Board and three permanent working groups focusing on (i) risk management, business continuity, and preparedness; (ii) cyber and digital security development; and (iii) data-protection advancement.

The VAHTI structure is explicitly designed as a learning network. Members co-produce practical guidelines, policy recommendations, and training materials; organize peer-learning sessions and topical debates; and share real-time situational insights on digital security challenges. Participation is open and transparent, following the Chatham House Rule, which encourages open knowledge exchange and collective reflection. Over time, VAHTI has evolved from a coordination forum into a community of practice that supports continuous capability development - helping institutions identify emerging skills needs, align training priorities, and strengthen leadership for digital security. Its model illustrates how inter-institutional learning ecosystems can complement formal training and make digital-competence development a continuous, collaborative process across government.

48. **Finally, the TNA process should also be used to close the loop and feed results into process and framework updates.** Aggregated findings should signal where to launch targeted academies (e.g., data stewards, AI product owners), adjust job descriptions, and prioritize micro-credentials with recognized standards. Over time, the system should shift from core module development and ad-hoc course buying to strategic capability building, evidenced by better alignment with digital-government benchmarks and relevant EU level digital-government maturity indicators. That is how a decoupled, tool-enabled, foresight-informed TNA becomes the engine for a digitally competent, interoperable, citizen-centered Romanian public administration.

³² Information available at: <https://dvv.fi/en/vahti-network>.

3. The TNA platform: from assessment to learning decisions – international insights and lessons for Romania

50. **A digital TNA platform is the backbone of a modern, government-wide approach to skills assessment.** In mature digital training ecosystems, digital TNA platforms provide a single entry point where public institutions can assess, analyze, and act on digital-skills data using common standards. The platforms connect self-assessments, knowledge tests, and task-based exercises with HR and learning systems, turning raw data into actionable insights. More than a technical tool, a digital TNA platform is an enabler of strategic capability building, helping public institutions align digital-skills development with national digital-transformation goals. By centralizing information and automating analysis, the platform reduces duplication, increases comparability, and supports targeted investment in learning.
51. **This chapter focuses on the key functionalities that make digital TNA platforms effective tools for government-wide digital skills assessment and planning of learning interventions.** It explains how these platforms combine assessment, data management, and learning functions to create a coherent ecosystem for evidence-based upskilling. The chapter defines the scope and purpose of a digital TNA platform and its role in ensuring systematic, comparable measurement of digital skills. It also examines the core functional architecture, including user management, analytics, interoperability with HR and learning systems, and data-governance mechanisms, that enable large-scale implementation. Functionalities are analyzed based on relevant international experiences.

3.1 Assessment methods applied on dedicated TNA platforms

52. **Digital TNA systems rely on a mix of assessment methods - self-assessments, knowledge-based tests, task and performance evaluations, and emerging AI-assisted tools - each capturing a different facet of digital competence.** As will be detailed below - no single method is sufficient. Most governments combine approaches so that cost, objectivity, validity, and coverage are balanced against the intended use (baseline mapping, assurance of minimum standards, or validation for critical positions). Each method provides distinct types of evidence and serves specific policy purposes within the overall assessment framework:
- Self-assessments offer rapid, large-scale insights into perceived skill levels and support diagnostic mapping for learning pathways;
 - Knowledge-based tests provide standardized benchmarks that allow consistent comparison across institutions and job roles;
 - Task- and performance-based assessments evidence what staff can actually do in operational or higher-stakes roles; and
 - Emerging AI-assisted conversational tools introduce adaptive and formative testing that adjusts to the learner's profile and provides immediate feedback.
53. **Many governments operationalize this mix through integrated digital TNA platforms that aggregate various instruments.** Digital TNA platforms launched and operated by various governments worldwide bring self-assessment, knowledge checks, and task-based exercises into one service. They usually map results to a national or DigComp-similar compatible schema. Furthermore, they generate role-aware learning paths and provide privacy-safe dashboards for ministries and central agencies. The next subsections summarize each assessment method, its strengths, limitations, and best-fit use cases, and illustrate how governments embed these methods within integrated TNA platforms to support evidence-based workforce planning and targeted upskilling.

Self-assessments

54. **Self-assessment instruments are the most widely used entry point for measuring digital competence in public administration.** They rely on individuals reporting their own perceived level of knowledge, confidence, or frequency of performing specific digital tasks. Typically administered online through structured questionnaires, they use predefined scales, such as Likert-type or multiple-choice formats, to capture responses across a consistent set of descriptors. This design allows results to be aggregated and compared at institutional or national level. Because these tools require only basic digital access and minimal infrastructure, they are well suited for large-scale deployment across multiple public authorities.
55. **The main advantage of self-assessment lies in their scalability, affordability, and diagnostic value.** They can be implemented quickly, cover a broad spectrum of competencies, from foundational digital literacy to advanced skills such as data analytics, AI literacy, or cybersecurity, and provide a first-level overview of workforce readiness. At the individual level, they encourage reflection and self-awareness, which supports intrinsic motivation for learning and helps employees identify areas for improvement³³. At the organizational level, aggregated results create a baseline of perceived capability that can inform institutional training strategies, workforce planning, and investment decisions.
56. **However, self-assessment data should be interpreted with caution.** Numerous studies have shown that respondents often misjudge their actual skill levels³⁴, due either to overconfidence or to underestimation, depending on prior exposure, role expectations, or demographic factors (e.g., gender, education, professional culture). Comparative studies find that discrepancies between self-reported and actual performance are particularly pronounced in complex domains such as problem-solving and cybersecurity³⁵. These instruments therefore capture perceived competence rather than demonstrated performance.
57. **The results are most reliable when self-assessments are complemented by more objective approaches, such as knowledge-based testing or performance tasks** that validate and calibrate the findings. When integrated into a digital TNA platform, self-assessments serve as the first diagnostic layer in a broader measurement ecosystem, providing rapid, system-wide insights while anchoring more targeted assessments for specific occupational groups or priority skill areas. Self-assessment tools are the most widely used starting point for mapping digital skills.
58. **For instance, the Basque Country's IKANOS³⁶ tool is used for digital self-diagnosis, producing individualized roadmaps that support long-term development.**

³³ ITU, *Digital Skills Assessment Guidebook*, 2020. Available at: https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.04-2020-PDF-E.pdf.

³⁴ Litt, E. (2013). Measuring users' Internet skills: A review of past assessments and a look toward the future. *New Media & Society*, 15(4), 612–630. <https://doi.org/10.1177/1461444813475424>.

³⁵ Marzan, M.-D., Stamate, A., & Spuru, L. (2024). *Digital Competence Among Older Adults: Is Self-Assessment Reliable?* *Cureus*, 16(11), e73543. <https://doi.org/10.7759/cureus.73543>

³⁶ Information in this section was collected during the study visit organized by TAIEX with Bank support under the TSI project. Relevant information was also collected from the following websites:

- <https://test.ikanos.eus/index.php/566697?newtest=Y&lang=es>
- <https://ikanos.eus/wp-content/uploads/2018/03/Perfil.Profesional.ikanos.Administrativo.pdf>
- <https://ikanos.eus/recursos/documentos-pdp-2/>
- <https://www.ikanos.eus/wp-content/uploads/2018/03/Perfil.personal.ikanos.pdf>

Box 2 Ikanos as self-assessment platform³⁷

Ikanos is a regional digital-competency initiative of the Basque Government (Spain), aligned with the DigComp model.

Key features:

- Includes an online self-assessment test for individuals and organizations, allowing users to rate their own digital skills across multiple dimensions.
- Offers a personalized digital-skills profile report, including visual overview of strengths and weaknesses and a recommended learning path.
- Designed for large-scale deployment (used by tens of thousands of learners in the Basque region) and supports benchmarking and organizational diagnostics.

Relevance for TNA platforms:

Ikanos demonstrates how a self-assessment tool, rooted in a common competency framework (DigComp), can serve as a foundational layer in a broader TNA ecosystem. It shows how government can use assessment data for workforce planning, training-pathway design, and organizational diagnostics.

59. **In practice, self-assessment is most useful for rapid TNA and for creating individual learning pathways.** For evaluating digital skills level in the public sector, self-assessment works well for onboarding diagnostics, annual skills surveys, and portfolio planning at the ministry level. Its potential value in raising awareness and generating actionable data for human resources management (HRM), without imposing heavy costs on administration.

Knowledge-based assessments

60. **Knowledge-based testing offers a scalable and objective way to benchmark digital competencies, though it risks emphasizing theoretical knowledge over practical competence.** These assessments, often delivered through multiple-choice or standardized tests, are effective for establishing baseline knowledge across large administrations. They can be standardized, easily scored, and deployed at relatively low cost³⁸, which makes them attractive for governments seeking to ensure comparability across institutions.
61. **Knowledge-based tests also have clear methodological limits.** They tend to measure what individuals know about technology rather than what they can do with it. As research notes, many instruments focus on recognition of technical features, such as identifying a specific action button in an image of a digital tool, rather than assessing whether the user can apply that knowledge to complete a

-
- <https://op.europa.eu/en/publication-detail/-/publication/de6190cb-c4b2-11ea-b3a4-01aa75ed71a1/language-en>
 - <https://op.europa.eu/en/publication-detail/-/publication/7a30c607-2304-11eb-b57e-01aa75ed71a1/language-en>

³⁷ As described in 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. World Bank Group. <https://documentsinternal.worldbank.org/Search/40030465>

³⁸ ITU, *Digital Skills Assessment Guidebook*, 2020. Available at: https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.04-2020-PDF-E.pdf.

real-world task, like attaching and sending a document³⁹. This creates a performance gap between declarative knowledge and functional competence.

62. **When used as part of a mixed-method TNA approach, knowledge-based assessments help validating or calibrating self-assessment results** and identifying areas where additional training or practical testing is required. Properly designed and periodically updated, they provide a cost-effective means of maintaining consistent digital-skill benchmarks across large public workforces.
63. **The focus of a knowledge-based assessment depends more on design choices and not necessarily on the maturity of the digital platform that delivers it.** Even basic platforms can host sophisticated, context-relevant questions, while advanced platforms may still rely on simple recall tests if not well designed. The key determinant of quality is whether the assessment goes beyond identifying tool-specific knowledge to test conceptual and procedural understanding - for example, whether a respondent knows *why* certain digital actions are required and *when* to apply them in a work process. To ensure validity and avoid overemphasis on rote recall, knowledge-based assessments should therefore be combined with task, or performance-based components that demonstrate applied capability in realistic administrative contexts.
64. **To ensure validity, such tests should be complemented by task- or performance-based components that capture applied capability.** Knowledge-based assessments remain a valuable part of a mixed-method approach when the goal is to measure foundational understanding, establish common benchmarks, or verify certain levels of digital proficiency across a large workforce.

Task- and performance-based assessments

65. **Task-based and performance-based assessments both evaluate what individuals can do with digital tools, yet they differ in depth, scope, and purpose.** Task-based assessments focus on the completion of specific, well-defined digital actions, such as formatting a document, sharing a file, or applying a formula in a spreadsheet. They are typically automated, scalable, and objective, making them suitable for large-scale measurement and diagnostic use. Their design allows governments to test thousands of users under standardized conditions, generating comparable data on functional proficiency. These assessments provide valuable insights into practical tool use but usually test actions in isolation, without assessing broader reasoning or problem-solving processes.
66. **Performance-based assessments, by contrast, evaluate the ability to apply digital skills in authentic, multi-step situations that mirror real work contexts, which make them more complex to develop and administer.** Rather than testing discrete actions, they assess how individuals integrate knowledge, tools, and judgement to achieve a goal, for example, preparing a data-driven report, managing an online process, or responding to a simulated cybersecurity incident. This approach provides a more valid picture of applied competence, particularly for advanced or high-stakes positions, though it is costlier and more complex to administer.
67. **Task-based assessments are a reliable method for measuring digital competence, as they go beyond self-reported skills or theoretical knowledge.** They provide direct evidence of the workforce's abilities. For example, The *PIX* platform, managed by the French Ministry of Education and DINUM, has a dedicated track for public administration (*PIX Fonction publique*)⁴⁰. It uses interactive, task and

³⁹ Sparks, J. R., Katz, I. R. & Beile, P. M. (2016). Assessing digital information literacy in higher education: A review of existing frameworks and assessments with recommendations for next-generation assessment. ETS Research Report Series, 2016(2), 1–33. <https://doi.org/10.1002/ets2.12118>.

⁴⁰ <https://www.campus.numerique.gouv.fr/pix-fonction-publique-d%C3%A9tat/>.

performance-based exercises, such as managing documents, evaluating information sources, or applying cybersecurity practices, to assess actual capability.

68. **Designing such assessments requires specialized infrastructure, trained evaluators, and significant investment, making them more resource-intensive than other approaches.** Such tests are also more time-intensive to conduct.⁴¹ Their context-specific nature also complicates standardization, making it difficult to compare results across ministries or countries. Reviews confirm that while task-based methods offer the highest validity, they are the hardest to scale and benchmark systematically⁴². For this reason, task-based assessments can be applied selectively, targeting selected digital competencies.

Hybrid assessment: knowledge- and task-based

69. **The most effective digital-skills assessments combine knowledge-based and task-based components within a single testing framework.** Knowledge-based items establish a consistent and comparable measure of conceptual understanding, testing whether individuals know *what* to do and *why* it matters, while task-based items verify whether they can actually *do it* using digital tools. When integrated, these methods balance validity, scalability, and cost-effectiveness.
70. **International experience, for example France's PIX, shows that this layered approach produces more reliable and actionable results than either method alone.** It enables governments to capture both declarative and procedural knowledge, supporting the design of training pathways that develop not only awareness but also practical proficiency. The PIX platform integrates both knowledge-based and task-based assessment. Knowledge-based questions check conceptual understanding of digital principles and tool functions, for example, identifying a secure password or recognizing trustworthy online information. As users progress, the platform presents task-based exercises that require performing concrete digital actions in simulated environments, such as formatting documents, managing shared files, or applying data-protection settings⁴³. This mix of question types ensures that PIX measures not only what users know but also how they apply that knowledge in practice. The combination of conceptual and applied testing underpins the reliability of PIX's certification system and allows institutions, including public administrations, to map digital skills with both breadth and depth.

Conversational (Chatbot-based) assessments

71. **Chatbot-based assessments are an emerging method that uses conversational agents to evaluate competences through interactive dialogue.** Unlike traditional questionnaires, chatbots can adapt questions dynamically, probe reasoning, and provide real-time feedback, making assessments more engaging and accessible. Pilot studies in higher education show that conversational assessments can improve test-taking effort, reduce anxiety, and provide richer evidence of understanding compared

⁴¹ ITU, *Digital Skills Assessment Guidebook*, 2020. Available at: https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.04-2020-PDF-E.pdf.

⁴² Van Laar, E., van Deursen, A. J. A. M., Helsper, E. J., & Schneider, L. S. (2025). *Developing Performance Tests to Measure Digital Skills: Lessons Learned From a Cross-National Perspective*.

⁴³ Examples of practical questions are included in this presentation: https://unevoc.unesco.org/yem/materials/pix/The_Pix_Platform.pdf.

to static formats⁴⁴. These features suggest potential for public administrations seeking scalable yet user-friendly digital skills diagnostics.

72. **Application of this method to digital skills frameworks seems feasible, but evidence remains at the pilot stage.** A Swiss initiative in Bern University has created DigiBot, which uses the European DigComp framework to test if digital competencies can be evaluated using a chatbot format, enabling individuals to complete a personalized self-assessment through natural language dialogue⁴⁵. A similar initiative that aims to build a dedicated LLM that draws on the UK's *Digital, Data and Technology* (DDAT) competency framework and can assess individual's digital skills seems to be currently underway⁴⁶. These pilots highlight feasibility for civil service contexts, particularly in onboarding and continuous training.
73. **Using AI chatbots still raises concerns over validity, reliability, and regulatory compliance.** While chatbot-based assessments may capture richer responses, their measurement accuracy has yet to be validated systematically against task-based or proctored benchmarks. Studies warn that results can vary depending on design quality, conversation flow, and rubric alignment⁴⁷. In employment settings, EU regulation also raises compliance considerations: under the EU AI Act, AI systems used for worker assessment fall under "high-risk" classification, requiring transparency, human oversight, and risk management procedures.⁴⁸

Role-specific assessment models

74. **Several countries combine approaches, tailoring assessment methods to workforce needs and role types.** In Italy, the INPS "Deep Skills" initiative demonstrated how adaptive and gamified assessments can drive large-scale participation while maintaining analytical value. The project engaged a broad cross-section of INPS employees through an adaptive online assessment structured in three levels of increasing difficulty. The test combined practical, job-relevant skill questions with gamified, real-life "riddles" that had no single correct answer. This approach reduced anxiety and encouraged participation. This balance of relevance, adaptability, and engagement resulted in high completion rates and credible diagnostic data. Based on the results, INPS identified over 2,300 "digital champions" - staff members tasked with promoting digital literacy and coaching colleagues within their units⁴⁹. The initiative illustrates how well-designed hybrid assessments can generate both organizational insight and sustained momentum for digital upskilling across the public sector.

⁴⁴ Yıldırım-Erbaşı, S. N., Bulut, O., Demmans Epp, C., & Cui, Y. (2025). *Advancing Higher Education Students' Assessment Experiences with Conversational Agents*. Educational Technology Research & Development, Educational Technology Research and Development DOI:10.1007/s11423-025-10472-3.

⁴⁵ SocietyByte / Bern University of Applied Sciences (2025). DigiBot: A Personalized Generative AI Tool for Assessing Digital Competences through Self-Assessment. More information available at: <https://www.societybyte.swiss/en/2025/04/16/digibot-a-personalized-generative-ai-tool-for-assessing-digital-competences-through-self-assessment/>.

⁴⁶ As noted during interviews conducted by the Bank team with the team in UK, as part of the research phase for this report.

⁴⁷ Yıldırım-Erbaşı, S. N., Bulut, O., Demmans Epp, C., & Cui, Y. (2025). *Advancing Higher Education Students' Assessment Experiences with Conversational Agents*. Educational Technology Research & Development, DOI:10.1007/s11423-025-10472-3.

⁴⁸ European Commission (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689). Official Journal of the European Union, European Union (2024). See Annex III, 4(b) and Articles 8–15.

⁴⁹ Burtscher M., Piano S, Welby B., *Developing skills for digital government: A review of good practices across OECD governments*, 2024, DOI:10.1787/f4dab2e9-en.

75. **Also, it is important to adapt TNA methods to role specificity, to ensure that ICT professionals are not assessed through generic approaches intended for the wider civil service.** Usually, digital professionals undergo more rigorous validation aligned with job requirements. For example, The UK's *DDaT Capability Framework* sets out detailed role profiles and career pathways for digital specialists, linking them to a mix of assessment methods targeted to the specific profiles that are continuously updated (every 3 months)⁵⁰.
76. **No single method provides a complete view of capability; most administrations adopt a *hybrid mix tailored to purpose and role*.** As summarized in Table 1, self-assessment instruments enable scalable diagnostics and routing to learning; knowledge-based tests provide standardized benchmarks (including for mandatory courses); task- and performance-based assessments evidence practical competence for higher-stakes roles; and conversational tools are useful for formative diagnostics. Opting for hybrid approach that combines several assessment methods allows governments to balance cost, objectivity, validity, and coverage.

Table 1 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 TNA and awareness Good for baseline 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

⁵⁰ Information available at: <https://ddat-capability-framework.service.gov.uk/roadmap>.

Conversational (Chatbot-based) assessment	Engaging UX for enhanced uptake	Validity/reliability not on par with task tests; prompt -	Early experiments - Switzerland	Formative diagnostics (onboarding, pulse checks)
	Adaptive probing to accurate identification of competency level	sensitivity/ "hallucinations";	"DigiBot" university pilot	
	real-time feedback to managers and employees	Unsuitable for high-stakes certification	Early DDaT-aligned prototypes (pilot stage)	Can complement, not replace, other methods.
	low marginal cost at scale			

77. **Systematic assessments of digital skills among civil servants are still uncommon⁵¹, but a growing number of governments are adopting integrated online TNA platforms that combine multiple assessment instruments within a single environment.** These platforms typically bring together self-assessment, knowledge-based testing, and, in some cases, task- or performance-based exercises, linked to relevant competency frameworks. Results are automatically analyzed and translated into personalized learning pathways or institutional training recommendations. Such integrated approaches support large-scale participation, standardization, and continuous monitoring of digital capability development. The core characteristics of effective TNA platforms are important as they determine the robustness and policy relevance of the TNA process. Such core characteristics are explored in the next section of this report.

3.2 Functional characteristics of digital skills (self-)assessment tools

78. **A growing number of governments have adopted platform-based approaches to assess and improve the digital skills of public employees.** These platforms serve as critical enablers for aligning public administration capabilities with national digital transformation agendas. By offering self-assessment modules, diagnostic tools, and links to targeted training content, they help civil servants benchmark their digital competencies, identify gaps, and access personalized development pathways. At the institutional level, such platforms offer public sector employers strategic insights into workforce readiness, allowing for better planning, capacity-building, and resource allocation.
79. **This section examines the functionalities, strategic design, implementation, and institutional integration of platform-based digital skills assessment tools in the public administration.** Its objective is to support the operationalization of Romania's digital competency framework by identifying governance, methodological, and capacity-building practices that enable effective uptake. While the platforms reviewed include a variety of technical functionalities, these were not analyzed in detail, as they fall outside the scope of this report. To inform Romania's efforts to design a digital skills self-assessment platform for civil servants, the section draws on examples from countries such as Latvia, Canada, Spain, and France, as well as supranational tools supported by the European Commission. These platforms were selected for their relevance to the public sector, their demonstrated alignment with competency frameworks such as DigComp, and their integration with HR and training systems.
80. **The review is structured around four core characteristics relevant for successful implementation and sustainability: (i) TNA ownership and administration, (ii) assessment methodology and scope, (iii)**

⁵¹ Burtscher M., Piano S, Welby B., *Developing skills for digital government: A review of good practices across OECD governments*, 2024, DOI:10.1787/f4dab2e9-en.

integration with training provision, and (iv) certification, feedback and reporting mechanisms. These dimensions reflect both operational and institutional design considerations that are essential for ensuring that digital skills assessments are not merely diagnostic, but also developmental and strategically embedded into broader human resource management (HRM) processes.

81. **This structured approach allows for a more nuanced understanding of what makes a TNA platform effective, scalable, and institutionally anchored.** Rather than promoting a single model, the analysis highlights features and functions that have proven successful in different governance contexts, with an emphasis on transferability to Romania's institutional framework and ongoing HRM reform agenda. The goal is to identify not only what works, but what fits best within the Romanian public administration's evolving digital competency and workforce development ecosystem.
82. **As a foundation, effective TNA platforms depend on their institutional anchoring within broader HRM systems and digital transformation strategies.** Usually, these platforms are not standalone diagnostic tools, but are purposefully integrated into public sector reform agendas aimed at building digital capacity and modernizing service delivery. In Spain, the forthcoming *AgeDigital* platform, developed by the Instituto Nacional de Administración (INAP) ensures competency-based assessment but also certification, as well as training impact dashboards aligned with national digitalization targets under *Digital Spain 2026*⁵². In Italy, the *Syllabus* and *DSKPA* platforms are part of a coordinated vision involving the Department for Public Administration, Scuola Nazionale dell'Amministrazione (SNA), and Formez PA, structured under the national *Three-Year Plan for IT in Public Administration*⁵³, with clear alignment to the DigComp framework and the broader "Promoting Change" competency for civil service executives. Latvia's digital skills ecosystem is similarly embedded in public administration reform, with the State Chancellery leading the integration of the competency framework into selection, appraisal, and development processes, supported by EU funds and linked to national digital transformation guidelines (State Chancellery, 2024⁵⁴). In Canada, the Canada School of Public Service (CSPS) Digital Academy's self-assessment tools and capability frameworks are guided by the *Government of Canada Digital Standard*⁵⁵, ensuring that training pathways are aligned with evolving institutional priorities for agile, inclusive, and user-centered service delivery. The Digital Academy supports the strategic upskilling for a digital-first public administration⁵⁶. These cases demonstrate that anchoring TNA platforms within strategic frameworks enhances their relevance, sustainability, and impact, ensuring that digital upskilling efforts are not episodic but embedded in long-term institutional development.

i. Platform ownership and administration

83. **A successful digital skills assessment platform requires clear institutional ownership and robust administrative support.** The sustainability of large-scale digital-skills platforms depends strongly on their ownership and governance arrangements, which ensure policy continuity, strategic alignment, and coordination across multiple stakeholders. The PIX platform offers a robust model in this regard. In France, PIX is managed by a Groupement d'Intérêt Public (GIP Pix), a public interest consortium bringing together the Ministry of National Education and Youth, the Ministry of Higher Education and Research, and DINUM

⁵² Information made available during the study visit organized under the TSI project. Details on the Spanish case study are also available in Output 1 developed under the TSI project.

⁵³ <https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2024-2026/index.html>

⁵⁴ Based on information gathered during interviews conducted in 2025.

⁵⁵ <https://digitalgovernmenthub.org/examples/government-of-canada-digital-standards/>.

⁵⁶ https://www.cspc-efpc.gc.ca/about_us/business_lines/digitalacademy-eng.

(the Interministerial Directorate for Digital Affairs⁵⁷). This multi-stakeholder governance guarantees stable funding, interoperability with education and public-sector systems, and consistent policy direction aligned with the national digital-skills agenda. In Belgium, PIX has been adopted by the Fédération Wallonie-Bruxelles with the technical support of ETNIC, the regional public IT agency, under cooperation agreements with GIP Pix⁵⁸. This arrangement preserves a single technical and methodological standard while allowing contextual adaptation at the regional level. The combination of ownership and decentralized deployment under formal public governance ensures that PIX remains an open, scalable, and sustainable infrastructure for digital-skills development across multiple sectors, including education, employment, and public administration. In contrast, Canada's CSPA Digital Academy platform is centrally governed by the Canada School of Public Service⁵⁹, which provides a unified capability framework and digital-learning ecosystem, while allowing departments to tailor content and delivery to their specific workforce needs.

84. **Italy's approach to digital-skills assessment and training in the public administration demonstrates the importance of clear institutional ownership and inter-agency coordination.** The country's digital-transformation and upskilling agenda is led by the Department for Public Administration (Dipartimento della Funzione Pubblica - DFP), which provides strategic direction and policy oversight, while implementation is shared with the Scuola Nazionale dell'Amministrazione (SNA) and Formez PA. Italy's approach is anchored in two complementary instruments: the Syllabus, which provides a national digital-competency framework and online training catalogue⁶⁰, and DSKPA⁶¹, a diagnostic and capacity-building platform coordinated by Formez PA and supported by EIPA. Together, they form an integrated system that combines skills definition, assessment, and training delivery, ensuring alignment with DigComp and the national Three-Year Plan for IT in Public Administration. The SNA, as the national school of government, anchors the system's sustainability by integrating competency-based training for middle and senior civil-service managers. This shared-governance model illustrates how a clearly defined division of responsibilities - policy ownership by the DFP, implementation by specialized training bodies, and alignment with EU standards - can secure long-term institutional commitment and coherence for national TNA platforms⁶².

Box 3 Italy - SNA's Department of Digital and Ecological Transition (DiTED) and the Corso-Concorso executive pipeline⁶³

Italy's Scuola Nazionale dell'Amministrazione (SNA) is integrating digital and sustainability skills into executive formation through a dedicated department (DiTED). DiTED designs specialized courses in cybersecurity, AI in public administration, digital skills for service innovation, and sustainability management. It works with universities, public institutions, NGOs, and research organizations to keep content aligned with national priorities and EU digitalization objectives.

Executive selection and training are delivered via the Corso-Concorso, a competitive, year-long pathway that combines selection and professional formation. Candidates pass an entry competition, then complete eight months of general training with examinations and rankings that determine their preferred assignment across central administrations (Presidency of the Council, ministries, agencies, major non-economic public bodies). The final four months comprise specialized training and an

⁵⁷ <https://www.numerique.gouv.fr/numerique-etat/dinum/>.

⁵⁸ Information available at: <https://pix.org/fr-be/>.

⁵⁹ Canada's Canada School of Public Service is the central government body responsible for governing and delivering learning services, including its digital platforms, to federal public service employees.

⁶⁰ <https://www.syllabus.gov.it/portale/web/syllabus/offerta-formativa>.

⁶¹ <https://www.eipa.eu/epsa/digital-skills-and-knowledge-for-public-administration/>.

⁶² A detailed presentation of the Italian case study is included in Output 1 under the TSI project.

⁶³

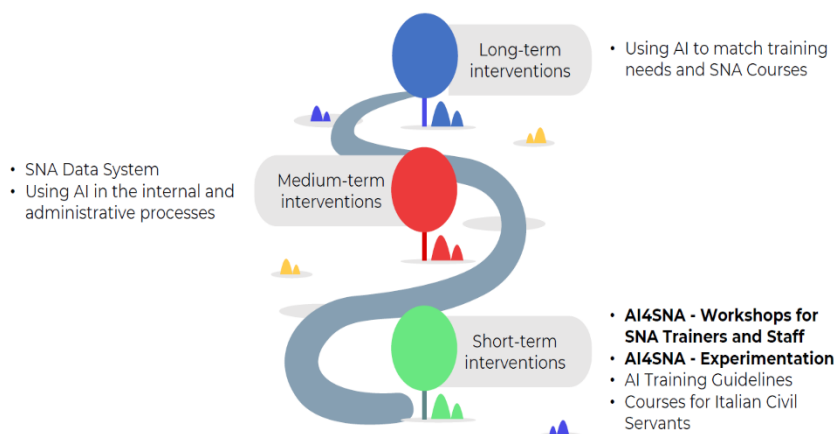
internship - sometimes including a placement at the European Commission - culminating in final assessments certifying managerial readiness. Eligibility typically requires a university degree and five years of civil-service experience, or an equivalent academic specialization.

A dedicated competency framework underpins the *Corso-Concorso*, with digital competence embedded under the broader “Promoting Change” area. The framework uses three proficiency levels (1–3), emphasizes fostering a digital mindset, and currently does not isolate digital competencies for managers as a stand-alone domain.

Delivery remains predominantly in-person, with gradual modernization of formats and expanded access via digital platforms, and evaluation focuses on outputs rather than impact. The emphasis on face-to-face learning reflects the leadership-development model, while ongoing efforts aim to broaden reach; monitoring prioritizes completion and placement results over longer-term outcomes.

85. **SNA demonstrates strong institutional leadership in embedding AI into public sector training.** As the institutional owner of Italy’s executive-level public service training, SNA has initiated the AI4SNA program to pilot the use of AI in training design, delivery, and content development⁶⁴. The initiative is implemented by the Department for Digital and Ecological Transition (DiTED), in collaboration with AgID and aligned with Italy’s National AI Strategy (2024–2026), ensuring coherence with national digital priorities. SNA’s ownership extends beyond training content to include strategic governance of AI integration, positioning it as a central actor in scaling digital innovation across the civil service. By institutionalizing the use of AI within its platform and organizational structure, SNA ensures that emerging technologies are not only explored but systematically incorporated into public sector learning systems.

Figure 7 SNA AI strategy



86. **Effective ownership of national TNA platforms requires distinguishing between general public-administration training and specialized ICT-professional development.** Many countries separate these streams institutionally: general digital-skills training is coordinated by civil-service training bodies, while technical or cybersecurity training is overseen by specialized digital-governance agencies. Finland and Spain illustrate this dual-governance approach.
87. **In Finland, platform ownership is clearly divided between institutions responsible for general civil-service development and those managing specialized digital and cybersecurity competencies.** The Ministry of Finance owns and governs eOppiva, the common digital learning platform for all public

⁶⁴ <https://sna.gov.it/home/attivita/ricerca/progetti-di-ricerca/progetti-in-corso/ia-e-formazione-sna/>.

employees, developed and maintained in cooperation with HAUS Development Centre Ltd (HAUS), which is a limited liability company wholly owned by the state, whose mission is to provide general personnel training services for the entire state administration⁶⁵. eOppiva provides a wide catalogue of civil-service learning modules, including both general management and digital-skills training, and serves as the national platform for continuous professional development. Its governance under the Ministry of Finance ensures strategic consistency, while the use of a shared public platform fosters scalability, cost efficiency, and interoperability with other HR systems. In parallel, the Digital and Population Data Services Agency (DVV) ensures distinct more targeted training and coordination on specialized digital topics. This agency is responsible for the digitalization of society, secures the availability of data, and provides services for citizen's life events⁶⁶. DVV coordinates the VAHTI network, which develops cybersecurity and digital-security competencies across government. VAHTI's mandate includes setting common standards, coordinating sectoral training programmes, and supporting information-security management in public institutions. This dual-ownership structure - eOppiva for broad workforce upskilling and VAHTI for technical and cybersecurity domains - allows Finland to combine inclusiveness with depth, ensuring that both general and specialised roles benefit from targeted, institutionalised digital capability-building.

88. **Spain presents a coordinated model anchored in centralized policy leadership and shared implementation.** The Instituto Nacional de Administración Pública (INAP) holds the national mandate for civil-service training and manages the Marco de Competencias Digitales del Empleado Público, a comprehensive competency framework aligned with DigComp. The framework defines the digital knowledge, skills, and attitudes expected of all public employees and serves as the reference for curriculum design and future certification processes. INAP is now operationalizing this framework through its online learning and assessment environment, the INAP Campus, which includes a dedicated section on digital competencies⁶⁷. The new Agedigital interface⁶⁸ recently introduced on INAP's official portal provides a self-diagnosis tool and structured learning itineraries that allow civil servants to assess their digital-skills levels and access tailored learning plans. This platform consolidates training, assessment, and certification within one environment under INAP's ownership, ensuring that digital-skills development remains integrated with broader HR and professional-development systems for the public sector. In parallel, Red.es, the technical body specialized in digitalization, also has a key role to play. Red/es is a public corporate entity (entidad pública empresarial) attached to the Ministry for Digital Transformation and Public Function, through the State Secretariat for Digitalization and Artificial Intelligence (SEDIA)⁶⁹. Red.es delivers digital-skills and training programmes for citizens, SMEs, and the public sector (Competencias Digitales para el Empleo Público initiatives under España Digital 2026⁷⁰). This model demonstrates that platform ownership can be both centralized and collaborative, combining strategic control with distributed technical responsibility.

→ For Romania, these lessons highlight that a sustainable digital-skills assessment platform and TNA system depends on coordinated ownership and collaboration between institutions that already have legal mandate for training, HRM and digitalization. INA is mandated to serve as the central operational and learning and development center, designing the TNA methodology, delivering the general digital skills assessment, developing and delivering learning content, and ensuring that results feed directly into training programs. ADR has a critical role guaranteeing alignment with broader digital transformation

⁶⁵ <https://vm.fi/en/education-and-training-services>.

⁶⁶ <https://dvv.fi/en/digital-and-population-data-services-agency>.

⁶⁷ <https://campus.inap.es/v3/>.

⁶⁸ <https://www.inap.es/es/agedigital>.

⁶⁹ <https://www.red.es/es>.

⁷⁰ <https://www.red.es/es/iniciativas/proyectos/formacion-en-competencias-digitales>.

strategies, but also in managing and delivering specialized training and potentially managing the HR system for professional IT roles in the public administration. NACS needs to strengthen its oversight and HRM coordination role, promoting collaboration between HR and digital-skills systems and helping embed digital competences in recruitment and workforce-planning processes.

ii. Scope and assessment methods deployed on the platform

89. **The scope of a TNA platform is important because it determines the effectiveness, relevance, and strategic impact of the assessment process across individual and institutional levels.** A broad and well-defined scope ensures that the platform captures training needs that are not just technical or role-specific but also aligned with organizational transformation objectives, such as digitalization, inclusion, or service quality improvements. This enables the institution to link training investments directly to policy or reform outcomes.
90. **The scope of a TNA platform is shaped not only by the range of competencies assessed but also by why and when it is deployed within public administration systems, and also which processes the platform feeds into** - TNA, workforce planning, recruitment, or certification, since this determines the platform's impact on policy design and resource allocation.
91. **In most international cases examined, the primary purpose of TNA platforms is to inform the targeted upskilling and the development of targeted learning programs,** as well as to support the strategic planning of training provision, and enable evidence-based decision-making on workforce development. For instance, the establishment of Latvia's Digital Academy is part of a broader public administration reform⁷¹ underpinned by state and EU funding aimed at strengthening the digital skills of public servants⁷² at both state and municipal levels. This initiative is aligned with national policy priorities including Latvia's broader strategies to modernize public administration through digital transformation while it also draws on EU structural and cohesion funds as its financial basis. In Latvia, as in other relevant examples, the primary purpose of the TNA is to feed into learning management decisions.
92. **The typical scope of TNA platforms is to cover standardized comparable assessment, training and certification across the public administration workforce.** For example, in Latvia the scope of the platform extends across all civil service categories and integrates every stage of the capability-development process: assessment, learning, certification.⁷³ More details on this example are included in Box 4.
93. **While some platforms focus solely on providing individualized feedback, where digital skills assessments are designed primarily as developmental tools, others have adopted more integrated approaches.** For example, the United Kingdom has begun to embed digital skills assessments more systematically into HRM and pay frameworks. Although assessments are currently decentralized, with each department developing its own methodology, larger and more mature departments have established robust internal processes. The Government Digital and Data Profession Capability Framework⁷⁴ provides cross-government role and skill definitions, fostering alignment. Importantly,

⁷¹ <https://eprasmes.lv/wp-content/uploads/2022/02/Latvijas-lzglitiba-atstibas-pamatnostadnes-2021-2027.pdf>

⁷² <https://www.esfondi.lv/en/about-eu-funds/>

⁷³ Source: Consultations with the Government's Digital Academy, School of Public Administration, Latvia – interviews conducted under the TSI project as part of the research phase.

⁷⁴ <https://ddat-capability-framework.service.gov.uk/>

assessment outcomes are directly tied to pay allowances for digital professionals, creating tangible incentives for both individuals and departments.

Box 4 Latvia's Digital Competency Framework and implementation model in the public sector⁷⁵

Latvia's Digital Skills Training Needs Assessment platform represents a comprehensive, government-wide approach to developing and managing digital competencies across the civil service. Designed to align national priorities with international standards, the platform integrates assessment, learning, and reporting within a single system. It provides a structured mechanism for identifying skill gaps, guiding targeted training, and monitoring impact at both individual and organizational levels, thereby strengthening the digital capacity of public administration.

Ownership & administration: Governance anchors the platform in HR processes while allocating technical ownership by domain. The State Chancellery integrates the framework into selection, development, and appraisal; line ministries steward role-specific competencies (e.g., Defence for cybersecurity). EU funds support implementation through a partner network, with technical development outsourced for speed. The initiative targets ~63,000 employees.

Assessment methodologies & scope: The dedicated TNA platform aggregates assessment, learning, and reporting in one. The model is rooted in international practice and tailored to national priorities: it combines a competency framework, role mapping, a self-assessment tool, and an upgraded LMS to generate role-aware learning paths and portfolio-level analytics.

The competency framework is DigComp-aligned and translated for civil-service use. Six domains (e.g., data, cybersecurity, AI, and transversal skills) comprise 20+ competencies, each described at four proficiency levels with behavioral indicators - applicable to all staff, not only IT roles. Role profiles cover core digital roles (e.g., Data Strategy Director), enabling roles, and universal "user" roles, linking expectations to targeted training.

Integration with training provision: The platform centers on self-assessment and personalized development, with certificates available but emphasis on skills acquisition. Users complete an online self-diagnosis across the six domains and receive recommended courses; forthcoming releases aim to add deeper role-based guidance (e.g., "Level 3 Change Management" for project managers).

Feedback & reporting mechanisms: Impact is monitored through a structured five-level methodology (reaction, learning, behavior, organizational results, public value). Pilots across 10 projects - from webinars to behavior-change interventions - feed evidence into course design and investment choices (e.g., a cybersecurity course assessed for short-term knowledge gain, mid-term behavior change, and long-term resilience).

System-level measurement and transparency accompany rollout. A nationwide digital-skills survey establishes a 2025 baseline (to be repeated annually), and an open-access handbook/toolkit on training impact assessment is available to public and private users. Tools, methods, and results are published online to support reuse and accountability.

94. **The assessment method applied on the platform determines the effectiveness of the TNA process.** From an outside perspective, it also defines the platform's credibility and user engagement. High-performing platforms use adaptive, interactive tools to measure proficiency across various digital domains. Pix, notably, incorporates over 2,900 questions, up to seven levels of proficiency, and features

⁷⁵ Source: Consultations with the Government's Digital Academy, School of Public Administration, Latvia – interviews conducted under the TSI project as part of the research phase.

an adaptive testing engine that adjusts user inputs, thus creating a nuanced and individualized assessment experience. The methodology blends multiple-choice, Likert scales, and scenario-based simulations, which is crucial for engagement and accurate skill mapping. Canada's Digital Competencies Self-Assessment (DCSA)⁷⁶ offers a more reflective approach, rooted in the "Six Digital Competencies for Public Servants," focusing on confidence levels and familiarity rather than technical expertise, which are more appropriate for policy or administrative roles transitioning to digital-first environments.

95. **Canada's TNA platform employs multiple mechanisms to inform the design and delivery of its learning programs for federal public servants.** The CSPS Digital Academy, established by the Canada School of Public Service (CSPS) in 2018, operates with a broad and strategic scope aimed at equipping federal public servants with the essential knowledge, skills, and mindsets required for effective service in the digital era. The Academy's mandate extends beyond traditional training, encompassing the development and delivery of comprehensive learning programs that address the evolving needs of Canada's public sector workforce. This scope is closely aligned with the objectives of the Beyond2020 initiative⁷⁷, which seeks to foster an agile, inclusive, and well-equipped public service, and is guided by Canada's Digital Standards. The digital TNA and learning platform covered large-scale initiatives such as the 2023 Employee-Identified Learning Needs Survey⁷⁸, which collected system-wide data on current and anticipated learning priorities to support evidence-based planning and resource allocation. In parallel, the CSPS collaborates with Statistics Canada on a voluntary Skills Inventory project⁷⁹, enabling departments to analyze workforce capabilities and training gaps for strategic HR management. The CSPS Digital Academy further complements these efforts through its Digital Readiness Self-Assessment⁸⁰, which allows public servants to evaluate their alignment with the Government of Canada's Digital Standards and receive targeted learning recommendations. Collectively, these tools serve as critical enablers of demand-driven learning, supporting both organizational capacity building and individual development planning across the federal public service.

Box 5 Canada - Digital Competencies Self-Assessment (DCSA) – scope and methods applied

Canada operates an online, voluntary Digital Competencies Self-Assessment (DCSA) aligned to the Government of Canada's Digital Competencies Framework. The tool presents statements (and occasional scenarios) across core domains - information and data literacy, communication and collaboration, digital content creation, safety/security, and problem-solving - and asks users to rate their proficiency on an ordered scale. The focus is formative: helping public servants reflect on their capabilities in relation to government-defined expectations.

Ownership & administration: Canada School of Public Service (CSPS) develops and operates the self-assessments and learning offer for federal public servants. (wiki.gccollab.ca)

Results are delivered as a confidential profile mapped to proficiency levels, with links to learning resources. Individual reports highlight strengths and gaps from foundational to advanced.

For data skills specifically, the Government of Canada's Data Competency Framework defines three levels -*Foundational, Intermediate, Advanced* - allowing institutions to tailor expectations by role or project and to align recruitment, learning pathways, and workforce planning with operational needs.

⁷⁶ <https://www.canada.ca/en/treasury-board-secretariat/topics/professional-development/>

⁷⁷ <https://www.canada.ca/en/privy-council/topics/blueprint-2020-public-service-renewal.html>

⁷⁸ https://publications.gc.ca/collections/collection_2023/efpc-csp/SC103-56-2023-eng.pdf.

⁷⁹ <https://www.statcan.gc.ca/en/>

⁸⁰ https://wiki.gccollab.ca/CSPS_Digital_Academy/Digital_Readiness.

Assessment methodologies & scope: Self-assessment against Government of Canada Digital Standards and a Digital Competencies model; reflective, confidence-based items; also targeted “Digital Readiness” checks.

Integration with training provision: Direct linkage to learning pathways (e.g., Discover series, ethics, cloud, cyber) surfaced post-assessment. (CSPS pages describe routing to relevant resources.)

Feedback & reporting mechanisms: Individual summaries and organization-level insights via surveys/inventories; formal system-wide HR dashboards are evolving rather than fully centralized.

The platform tool is most effective for guiding individual learning and for giving organizations a broad view of skills needs, while high-stakes validation would require additional methods (not only self-assessment).

Source: Authors’ elaboration, based on the information publicly disclosed by the Government of Canada.

→ To sum up, interviews and relevant documentation available indicate that relevant digital TNA platforms are generally used for assessment, learning and planning purposes, not for individual performance evaluation. Across the reviewed countries assessments serve primarily as developmental and diagnostic tools. They help identify skills gaps, inform training design, and guide institutional learning strategies based on aggregated data. Evaluation usually relies on self-assessment, knowledge-based and task-based methods. Assessment results remain confidential and are not linked to appraisal or promotion. Officials interviewed from other EU countries noted that connecting TNA outcomes to performance ratings would risk discouraging participation and reduce the accuracy of self-assessment. Most governments therefore keep a clear distinction between TNA as a capability-development instrument and performance-management systems.

For Romania, this distinction is essential. The future TNA platform should explicitly state that its role is formative, not punitive, focusing on evidence-based learning needs. This will help build trust, ensure high participation, and position the platform as a key enabler of continuous digital upskilling across the civil service.

iii. Integration with training provision

96. **An essential feature of effective digital competency platforms is the seamless integration of assessment and self-assessment tools with training provision.** Rather than serving as stand-alone diagnostics, these tools function as entry points into structured learning pathways that support continuous professional development. By linking assessment results directly to relevant learning content, whether through internal training catalogs, public online courses, or modular programs, institutions can ensure that upskilling efforts are both targeted and scalable.
97. **Country examples from Belgium, France, Italy and Canada illustrate different models for embedding training pathways into digital skills platforms, reinforcing the platforms' developmental value.** Italy has launched targeted initiatives to bridge the digital divide across regions. Digitalization and innovation in Italy are unitarily led by Digital Transition Managers (DTM) appointed for each institution. The DTMs are supported and coordinated by AgID, and their roles and required competencies are regulated by law. AgID promotes tools and initiatives to encourage updating of skills and capacity-building

of DTMs, including collaboration platform ReTeDigitale⁸¹, labs, and the development and use of common resources, all of which mapped directly to SNA (Scuola Nazionale dell'Amministrazione) and Formez PA offerings. These pathways are modular and adaptive, accommodating both foundational skills and advanced training in AI, cybersecurity, or e-procurement. The platform not only recommends courses but facilitates enrollment and tracks progress, making it a core component of the professional development cycle.

98. **The Pix platform⁸² also ensures a strong alignment between diagnostic assessment and institutional learning.** While Pix itself does not deliver training, it provides personalized training recommendations based on assessment results, directing users to public digital learning providers such as FUN-MOOC (France Université Numérique)⁸³.
99. **In France, the CNFPT⁸⁴ has integrated DigComp-based assessment tools into its digital training strategy for local government employees.** These tools identify individual and organizational training needs, which then inform the design and adaptation of CNFPT's training catalogues⁸⁵. CNFPT offers a wide range of digital learning modules, ranging from basic IT use to cybersecurity, data protection, and digital public service delivery. Based on assessment outcomes, users are directed to specific training activities either through in-person sessions or via the CNFPT's e-learning platform, which includes short courses, interactive modules, and practical exercises. This integration ensures that diagnostic data feeds directly into capacity-building programs, enabling local governments to align their workforce development efforts with evolving digital competency requirements.
100. **Canada's CSPS Digital Academy offers a range of thematic and role-relevant learning pathways⁸⁶ grounded in assessment diagnostics.** For example, the *Discover Series*⁸⁷ provides foundational learning streams such as *Discover Digital*, *Discover Data*, *Discover Agile*, *Cyber Security*, and *Discover Cloud*, with content delivered via self-paced and instructor-led modalities. For those interested in ethics and policy dimensions, *Data Ethics 101*⁸⁸ offers practical guidelines for transparency, fairness, inclusivity, and responsible use of data. For employees seeking leadership in modern government, the CSPS Digital Accelerator⁸⁹ provides applied, experiential learning involving real projects, peer learning, and experimentation with human-centered and iterative methods.⁹⁰ Modules are also structured thematically, into learning pathways, like the one on Digital, Data and Service Design⁹¹. These programs show how assessments are tied to concrete learning offerings that correspond to detected learning needs and institutional priorities.
101. **For specialized ICT roles, effective alignment between TNA and training pathways typically relies on structured digital-profession frameworks, as exemplified by the Digital, Data and Technology (DDaT)**

⁸¹ <https://www.retedigitale.gov.it/it/home>.

⁸² Interreg Europe. (n.d.). *Digital skills assessment tool: Pix*. <https://www.interregeurope.eu/good-practices/digital-skills-assessment-tool-pix-0>

⁸³ <https://www.fun-mooc.fr/fr/etablissements/fun/>

⁸⁴ https://www.fun-mooc.fr/en/organizations/centre-national-de-la-fonction-publique-territoriale-cnft/?page_courses=3

⁸⁵ CNFPT. (2023). *Offre de formation en compétences numériques*. <https://www.cnfpt.fr> (accessed September 2025) - <https://www.cnfpt.fr/se-former/decouvrir-offres-thematiques/transition-numerique/national>.

⁸⁶ <https://www.canada.ca/en/government/system/digital-government/>

⁸⁷ <https://catalogue.cspc-efpc.gc.ca/product?catalog>

⁸⁸ <https://www.cspc-efpc.gc.ca/tools/articles/data-ethics-101>

⁸⁹ <https://www.cspc-efpc.gc.ca/catalogue/programs/digital-accelerator-eng.aspx>

⁹⁰ <https://www.cspc-efpc.gc.ca/digital-data/digital-ps>

⁹¹ <https://www.cspc-efpc.gc.ca/digital-data/index-eng.aspx>.

Capability Framework in the UK (see Box 6). For example, in Scotland the Scottish Digital Academy provides a concrete illustration of how DDaT frameworks can translate directly into structured, role-based training offers. The Academy operates under the Scottish Government's digital-skills strategy and delivers modular learning aligned with the Digital, Data and Technology (DDaT) Capability Framework. One example is the Data and Analytics Learning Pathway,⁹² which supports public-sector employees in developing skills across four progressive proficiency levels. Learning modules correspond to different levels of responsibility and technical depth: for example, the Driving Value from Data course, hosted by The Data Lab, helps public-sector employees understand data as a strategic asset and apply it to decision-making. The Data Masterclass supports senior leaders in embedding data-driven approaches in organizational culture. Technical pathways include the Microsoft Azure Architect Design course, which combines digital and live learning to build cloud-architecture capabilities, and the Data Science Accelerator, an intensive development program for public-sector analysts to apply data science to real policy challenges⁹³. Employees can also act as mentors in the Accelerator program, reinforcing a culture of peer learning and professional collaboration. By explicitly mapping learning outcomes to capability levels defined in the DDaT framework, Scotland demonstrates how digital-skills assessments and frameworks can be operationalized through a formal, government-wide training system that combines standardized competence models with tailored learning experiences.

Box 6 The UK Government's Digital Competency Framework and TNA approach

The United Kingdom's Digital, Data and Technology (DDaT) Capability Framework provides a structured, government-wide approach to defining, developing, and managing digital skills across the civil service. The framework establishes clear role definitions, proficiency levels, and competency standards to guide recruitment, pay, and professional development. By promoting both technical depth and cross-functional agility, the DDaT framework supports the creation of a modern, adaptable public workforce equipped to deliver digital transformation effectively.

Ownership & administration: The UK Government has developed a structured and evolving DDaT Capability Framework designed to support strategic workforce planning, role definition, and digital skills development across departments. The framework is governed centrally by the Government Digital Service, but implementation is managed at the departmental level, allowing adaptation to specific institutional contexts.

Assessment methodologies & scope: Departments use the DDaT framework as a guide to design assessment and recruitment processes that reflect their operational needs. While the framework provides a unified structure for defining roles and expected capabilities, assessment remains decentralized across departments. Tools and methods vary. Efforts are underway to develop a standardized, potentially AI-driven assessment instrument to ensure consistency across government. This tool is expected to include features such as name-blind statistics, CV matching, and adaptive testing, supporting data-driven decisions in workforce management.

Integration with training provision: The DDaT framework connects assessment outcomes with learning and development opportunities, creating clear pathways for skill acquisition and career growth⁹⁴. Although many of these processes remain manual, plans are progressing to integrate assessment systems with enterprise resource planning platforms. This integration would enable automated

⁹² <https://digitalacademy.gov.scot/courses/data-and-analytics-pathway/>.

⁹³ Ibidem.

⁹⁴ <https://prospectus.governmentcampus.co.uk/04-professions/government-digital-and-data-profession/>.

learning recommendations and real-time career tracking, aligning employee development more closely with organizational needs.

Feedback & reporting mechanisms: Assessment outcomes are used to guide professional growth, but they are not applied for performance evaluation. Continuous feedback mechanisms are being developed to strengthen the alignment between skills, learning, and institutional performance. Challenges such as staff resistance to digital change persist, but demonstrable results and transparent reporting continue to build confidence in the system and support its gradual standardization across departments.

Source: Authors' elaboration, based on consultations with Capability and Workforce Division, Department for Science, Innovation and Technology, UK Government

→ **Digital-skills assessment platforms are most effective when they connect diagnostics directly to learning and certification. For Romania, the future TNA platform should serve as a single gateway linking self-assessment, adaptive training, and recognized certification, all anchored in the proposed digital competency framework for the public administration.** Using DigComp as a reference will ensure consistency with EU standards and allow the platform to draw on training content and learning resources developed under European initiatives. INA should lead on learning design and delivery, ADR should focus on advanced ICT and data-governance pathways, and NACS should ensure methodological coherence and integration with HRM systems. Together, these institutions can make the TNA platform a continuous learning engine that links digital-skill needs with training investments, certification, and Romania's wider digital transformation agenda.

iv. Certification, feedback and reporting mechanisms

102. **Certification, dynamic feedback and actionable reporting are critical to maintaining user engagement and informing individual learning and institutional strategy. Effective systems include certification and recognition through badges⁹⁵.** Digital certificates and digital badges are two types of credentials used to recognize learning achievements, each suited to different types of accomplishments. Digital certificates are typically issued for achievements that require significant time and formal assessment, such as completing a long course (over 40 hours)⁹⁶ or earning a professional certification, and are valued in situations where employers or formal bodies need proof of substantial, rigorously tested skills. Digital badges, on the other hand, are used for shorter, often informal learning experiences, such as completing a brief online module or acquiring a specific skill through a short course (e.g., 2 hours). Badges are commonly awarded for micro-achievements within longer programs, involve less formal evaluation, and are designed to be easily shared and accumulated as part of lifelong learning pathways. For example, the Enterprise Skilling and Strategy (ESS) team within the Treasury Board Secretariat (TBS) is piloting the use of digital badges to recognize digital skills achievements across the Government of Canada.⁹⁷

⁹⁵ Information from <https://www.accreditable.com/platform>.

⁹⁶ Kluzer S., Centeno C. and O'Keeffe, W., DigComp at Work, EUR 30166 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-22558-4, doi:10.2760/17763, JRC120376. Available at: https://ikanos.eus/wp-content/uploads/bp-attachments/10426/digcomp_at_work_090720_1.pdf.

⁹⁷ https://wiki.gccollab.ca/Digital_Talent/Digital_Badges.

103. **The Basque Country’s IKANOS Self-Assessment Test⁹⁸ (SAT) is a user-friendly online assessment tool designed to provide users with a personal digital profile based on DigComp 2.2.** It is designed to be accessible and can be taken in 25 minutes on any device with a web browser. Upon completion, users receive a personalized report⁹⁹ in PDF format that outlines their digital competence profile (see Figure 8 below). This report graphically displays achievements and areas for improvement across various digital skills. The IKANOS SAT has proven effective for various user groups, including citizens, professionals, teachers and students.

Figure 8 An example for a Personal Digital Profile elaborated with the result of the IKANOS test¹⁰⁰



104. **The BAIT system, an evolution of the IT Txartela certification in the Basque region, is underpinned by a robust, evidence-based reporting.** This mechanism is activated by the adaptive testing structure¹⁰¹, which collects real-time data on user performance and generates a detailed, certification for each participant reporting their demonstrated skills against the DigComp framework.

105. **Although primarily oriented toward educational stakeholders, the Italian digital skills certification scheme is a working example of how micro-credentials, especially in digital skills, can be institutionalized, credentialed, and used as recognized evidence of competence.** The EDSC DigComp certification¹⁰² (via CertiSkill / Intertek Italia) issues certificates aligned with DigComp 2.2. The process allows individuals to take a single exam covering multiple proficiency levels; upon passing, they receive a certificate in PDF and Open Badge format, and are registered in the national Accredia¹⁰³ registry. Because the certification is accredited by Accredia (Italy’s national accreditation body), it has legitimacy and portability. **More information on certification mechanisms in selected EU countries and recommendations on recognition/certification of digital skills are included in Output 3 developed under the TSI project.**

⁹⁸ <https://ikanos.eus/en/ikanos-model/audit/ikanos-test/>
⁹⁹ <https://ikanos.eus/en/ikanos-model/audit/perfil-digital-personal/>
¹⁰⁰ Ibidem.
¹⁰¹ <https://www.bait.eus/Bait/home/certificamos>.
¹⁰² <https://certiskill.eu/certificazioni/digcomp-2-2-en/>
¹⁰³ <https://www.accredia.it/>

106. **In Canada, platforms like the CSPS Digital Academy produce individual growth summaries.** The platform provides course takers with feedback on their digital skills through a combination of post-course evaluations, interactive assessments, and platform analytics. Additionally, CSPS collects user feedback through course evaluations and surveys, which help refine content and delivery, ensuring that learning experiences are responsive and tailored. This feedback loop is supported by the platform's tracking of completion rates, quiz scores, and engagement metrics, allowing both learners and administrators to monitor progress and adjust learning pathways accordingly.
107. **New initiatives are under way to better integrate digital competencies into HR processes.** Spain's INAP plays a leading role in aligning digital skills development with human resource management processes. The AgeDigital platform is currently under construction. Designed as a centralized digital competency management system, AgeDigital will assess public servants' digital skills, recommend tailored training programs, and generate post-training evaluations. The aims to provide individual feedback, institutional reporting, and system-wide impact analysis. A key innovation is the inclusion of impact dashboards and conversational AI to support user engagement and decision-making. Furthermore, the platform will maintain a centralized registry of certifications linked to competency accreditation, which is expected to inform career progression and support the development of a new performance evaluation model. By integrating with HR and economic management tools¹⁰⁴, AgeDigital will enable better talent planning, track the economic returns of training investments, and reinforce INAP's broader strategy to embed digital competencies into the Spanish public administration's transformation agenda.

Figure 9 AgeDigital assessment platform ensures certification of the digital skills and connection to learning modules¹⁰⁵



108. **Pix is also a reference for feedback and reporting mechanisms.** The Pix Orga dashboard allows organizations to assess employee competencies, track progress, and refine training strategies. The platform combines interactive self-assessments with organizational dashboards (Pix Orga) that allow HR units and managers to monitor results, identify skill gaps, and adjust training plans. Based on these

¹⁰⁴ HR and economic management tools refer to digital systems or platforms that support the planning, operation, monitoring, and optimization of human resources and financial resources across government. These tools are often integrated into larger enterprise resource planning systems and are key to aligning staff development with institutional goals and budgets.

¹⁰⁵ <https://www.inap.es/es/agedigital>

diagnostics, institutions can plan targeted training and recognize progress through Pix Certification, officially aligned with the DigComp framework and recognized in France and across Europe¹⁰⁶.

→ **For Romania, the integration of certification, feedback and reporting mechanisms within the future TNA platform will be essential to ensure both user engagement and institutional learning.** The platform should provide each civil servant with a personalized digital-skills profile, similar to models like Pix or IKANOS, summarizing assessed competencies, strengths, and learning priorities. Micro-credentials, issued as digital certificates or badges for completing targeted modules or workshops, would allow staff to showcase their evolving skills transparently and progress through adaptive learning pathways.

At the institutional level, aggregated dashboards should enable INA, ADR, and NACS to monitor participation, identify emerging training needs, and assess the impact of digital-skills programs. Feedback loops should remain developmental, not evaluative, ensuring that individual data is used to guide learning pathways rather than performance appraisal. INA should oversee the generation and interpretation of learning analytics for training design, ADR should contribute to monitoring advanced digital skills, while NACS should ensure methodological consistency and using feedback for potential updates of the digital competency framework model. Establishing such reporting and feedback architecture would create an evidence-driven TNA system.

¹⁰⁶ <https://pro.pix.org/en/public-sector>.

4. Institutionalizing the digital-skills TNA process: design principles and implementation mechanisms

109. **Building on the TNA process already proposed in Chapter 2 and the review of platform characteristics in Chapter 3, this chapter outlines how Romania can institutionalize a government-wide digital-skills TNA process.** The aim is to establish a standardized, data-driven approach supported by a dedicated digital platform that informs targeted learning, workforce planning, and capability development across the public administration. The chapter summarizes the key features required for such a system, covering ownership and governance, scope and assessment methods, integration with training and certification, and feedback and reporting mechanisms. Together, these elements provide a roadmap for embedding the TNA process into Romania's broader HRM and digital transformation frameworks.

4.1 Define institutional ownership, mandates, and data governance

110. **A well-defined institutional framework is essential for the success and sustainability of any government-wide digital skills initiative.** In the context of digital skills training for Romania's civil service, fragmented mandates and overlapping responsibilities have historically led to gaps in implementation, inconsistent standards, and missed opportunities for strategic alignment. By establishing explicit institutional ownership, the government can ensure that digital skills development is systematically anchored in national priorities, supported by adequate resources, and coordinated across all relevant agencies.
111. **INA is best positioned to act as the Product Owner for the digital skills TNA platform.** INA holds the legal mandate for civil service training in Romania. As the institution responsible for professional development across the public administration, INA is best positioned to act as the Product Owner for the digital skills future TNA platform. This legal foundation provides INA with the authority to lead the design, implementation, and ongoing management of the platform, ensuring continuity and avoiding project orphaning. A Government Decision should formally designate INA as the Product Owner, with a multi-year budget line and staffing to support platform operations.
112. **While INA should have the primary role, effective digital skills development requires close collaboration with NACS and ADR:**
- **NACS:** Responsible for civil-service competency alignment and national aggregation/reporting standards. NACS should be consulted on the interpretation and updating of the digital competency framework and HR policy use, ensuring that the TNA platform aligns with broader civil service reform agenda.
 - **ADR:** Responsible for targeted review of the digital competency framework, ensuring it is updated based on evidence and that system level TNA results are correlated to relevant updated training interventions, especially in priority areas (cybersecurity, AI etc.). ADR should also be responsible for deploying a dedicated process for TNA and professional development for the specialized ICT roles.
113. **To prepare for operationalization, a formal governance structure including INA, NACS, ADR, and the GSG could be established to approve the product roadmap and adoption targets.** Clear operational procedures should be set for consultation with line ministries and agencies, who would validate expected digital-skill levels by role within their organizational structures and contribute to refining occupational standards. Such a governance model would secure institutional ownership, promote cross-agency

accountability, and ensure that the TNA platform evolves as a shared public resource driving continuous digital capability development.

4.2 Select an implementation pathway for the digital-skills TNA platform

114. **Choose a single pathway - either extend INA's current platforms or stand up a dedicated assessment service - and document the rationale.** INA should lead a structured choice between two viable options, informed by clear criteria and accompanied by non-negotiable policy guardrails:

- **Option A - Extend INA's existing platforms.** Build the assessment capability into INA's current Learning Management System (LMS)/ portal by adding (i) a self-assessment and knowledge-check module aligned to the national digital skills TNA schema, (ii) a role/standards registry to fit the organizational needs of the TNA (iii) a learning-path generator to match the skills gaps with suitable training options and (iv) aggregated dashboards for the use of department managers/ HR representatives. The main advantages of this option are faster time-to-value, lower incremental cost, single user experience, reuse of identity and hosting on the existing INA platform. On the downside, this option presents potential constraints for advanced task-based simulations; higher risk of vendor lock-in for future extensions. **Best when:** generating a national baseline is the priority and task-based assessments remain targeted in following stages.
- **Option B - Build or procure a dedicated assessment platform.** Deploy a stand-alone, API-first service purpose-built for self-, knowledge-, and task-based testing, with a clean data model and analytics layer; integrate with INA's LMS and NACS reporting. The main advantages of this option are: scalable for high-assurance, task-based growth; more elaborated analytics and potentially easier evolution to micro-credentials and proctoring. In contrast, this option involves higher upfront cost; longer time to launch and will require stronger product/vendor management. **Best when:** Romania intends to scale task-based assessments from Year 2 onward.

Table 2 Comparative overview of the two options for the TNA platform

Dimension	Option A - Extend INA's portal	Option B - Dedicated assessment platform
Description	Add DigComp-aligned self-assessment, role registry, learning-path generator, and dashboards within INA's existing Learning Management System.	Build or procure a stand-alone, API-first platform for self-, knowledge-, and task-based assessments, integrated with INA's LMS and NACS reporting.
Pros	Faster implementation (≤12 months to national baseline) Lower incremental cost Unified user experience Reuses existing identity and hosting systems	Scalable for high-assurance, task-based growth Cleaner analytics and data structures Easier evolution to micro-credentials and proctoring Greater flexibility for future innovation
Cons	Limited ability to support advanced task-based simulations Higher risk of vendor lock-in for future extensions	Higher upfront costs Longer time to launch Requires stronger product and vendor management
Best Use Case	When speed is the priority and Romania seeks a rapid national baseline within 12 months; task-based assessments can remain limited in Year 1.	When Romania aims to scale advanced task-based assessments across multiple job

		families and requires a future-proof platform.
Decision Criteria	Depth/assurance needed now vs. later Integration with SSO/LMS/HRIS Analytics requirements Total cost of ownership (3 years) Vendor lock-in risk Change management burden	Same criteria as Option A, but weighted more heavily toward scalability, flexibility, and long-term analytics needs.
Policy Guardrails	Conduct a Data Protection Impact Assessment (DPIA) Enforce that TNA results are not used in performance appraisal or pay decisions Ensure confidentiality of individual results Apply minimum cell sizes in dashboards to avoid re-identification	

115. **In Romania, establishing clear policy guardrails will be essential to ensure trust, fairness, and compliance in the rollout of a digital-skills TNA platform for the civil service.** First, a Data Protection Impact Assessment (DPIA) should be conducted before implementation to evaluate potential privacy risks, given that the platform will process sensitive personal and behavioral data related to civil servants' digital competence levels. This assessment, aligned with GDPR requirements, should define data-handling protocols, access rights, and retention periods.
116. **Equally important is the adoption of the principle “TNA ≠ performance appraisal”, which must be explicitly stated in the platform’s governance framework.** This means that assessment results should be used exclusively to guide learning pathways, institutional training design, and strategic workforce planning, not to determine salary adjustments, promotions, or disciplinary actions. Such a safeguard is essential to encourage honest self-assessment, protect user confidence, and ensure broad participation.
117. **To reinforce confidentiality, individual-level data must remain private and test results accessible only to the assessed employee and authorized administrators within INA, NACS and the employer institutions.** Aggregated analytics should be anonymized and published using minimum cell-size thresholds in dashboards and reports to prevent any risk of re-identification, particularly in smaller institutions. These safeguards would not only ensure compliance with GDPR and national legislation but also establish a culture of trust-based participation, a prerequisite for embedding digital-skills assessment as a continuous, developmental process rather than a control mechanism.

4.3 Design and test assessment methods and instruments based on the proposed digital competency framework for the public administration

118. **The proposed digital competency framework for the public administration developed under the TSI project should become the backbone of the TNA platform. This model is aligned with the DigComp 2.2 and DigComp RO.** The proposed competency framework is intended to be inclusive and adaptable, allowing institutions to opt for more advanced levels of complexity where operational needs require. This approach ensures consistency and comparability across the public sector, while providing flexibility for institutions that wish to address specific digital skill requirements. By focusing on a unified framework, Romania can support scalable digital upskilling and avoid fragmentation, ensuring that all public administration staff benefit from a coherent and comprehensive model.

119. **Adopt a tiered assessment model that scales to the whole service while allowing depth for mandatory skills and higher-stakes roles.** Begin with a short self-assessment for all staff, then layer knowledge checks where policy/standards literacy matters (e.g., cybersecurity, data protection, accessibility) and deploy task-based simulations for competencies where it is relevant to test demonstrated performance (e.g., cybersecurity, data/analytics, service design).
120. **Ensure psychometric quality, accessibility, and fairness before national rollout.** Items should be piloted with diverse user groups and tested for difficulty and discrimination; wording and scoring must avoid bias; interfaces should comply with WCAG 2.1¹⁰⁷ (keyboard-only flows, alt text, plain language, Romanian-first). The Web Content Accessibility Guidelines (WCAG) are an international standard that ensures digital content is accessible to people with disabilities, covering aspects like screen-reader compatibility, color contrast, and keyboard navigation. Release candidates should pass a documented quality gate prior to production.
121. **Set up an item bank and blueprint to govern coverage and refresh.** INA should maintain an initial catalogue of at least 200 items tagged by competence area, level, item type (self/knowledge/task), language, and expected difficulty, alongside a blueprint that specifies coverage targets¹⁰⁸. A scheduled annual refresh should add new items, retire outdated ones, and recalibrate difficulty where pilots indicate drift.
122. **A credible platform combines methods matched to purpose - self-assessment, knowledge checks for compliance literacy, and task-based tests for applied competence.** As summarized in Table 2, self-assessments are best for rapid, low-cost diagnostics and routing to learning; knowledge-based tests (MCQ/short answer/scenarios) establish standardized benchmarks where policy and standards matter (e.g., cybersecurity, GDPR, accessibility); and task-based simulations demonstrate what staff can actually do.

Table 3 Recommended assessment methods for different use cases

Item Type	Description	Use Case
Self-assessment test	Likert-scale or confidence-based statement where users judge their skill level.	Mass baseline, reflection, routing to courses
Knowledge-based tests	Multiple-choice, short-answer, or scenario-based test of factual knowledge.	Compliance knowledge (cyber, GDPR, accessibility)
Task-based tests	Simulation or practical exercise demonstrating ability to perform a digital task.	Proving applied competence

123. **The platform should also allow short, modular assessments with adaptive routing and strong delivery controls, minimizing burden while preserving measurement quality.** Each assessment should be generated from a structured blueprint that defines coverage by competence area and proficiency level, and includes item tags (domain, level, format, expected difficulty) and exposure rules (randomization, parallel forms) to ensure comparability across institutions. Modular testing allows the evaluation of

¹⁰⁷ <https://www.w3.org/TR/WCAG21/>

¹⁰⁸ The test bank for DigComp self-assessment for citizens includes 82 items. Information available at: Vuorikari, R., Pokropek A., Castaño Muño, J., Enhancing digital skills assessment: introducing compact tools for measuring digital competence. <https://doi.org/10.1007/s10758-025-09825-x>.

distinct competence areas without overburdening participants, while adaptive routing adjusts question difficulty in real time based on user responses, maintaining precision and engagement:

- **Modular testing is highly recommended, as it allows the assessment of digital skills to be organized into short, targeted units, each focused on a given thematic grouping of competences.** Instead of requiring civil servants to complete one long and complex test, the approach divides the assessment into manageable modules, such as data management, digital communication, or cybersecurity, aligned with the digital competency framework. This structure makes testing more flexible, enabling institutions to select only the modules relevant to particular roles or functions. It also improves accuracy and user experience by reducing fatigue and allowing adaptive sequencing, where difficulty and content adjust based on previous responses. Internationally, platforms such as Pix in France apply modular testing to efficiently evaluate digital competences while maintaining comparability across institutions.
- **Adaptive testing should also be considered.** Adaptive testing ensures that every person taking the test gets questions that match their ability, making the results trustworthy and fair. Because the test adapts as the person answers, it uses fewer questions to get a reliable measure, so people spend less time testing but still get accurate results. This approach helps both advanced and beginner users focus only on what truly matters to assess their skills, making the testing process quicker and less tiring.

124. **The future digital-skills TNA platform for Romania's civil service should apply a tiered testing structure combining three complementary methods to balance coverage, precision, and usability:**

- **Self-assessment (all staff):** allows all staff to rate their confidence in different skills using simple questions that adjust based on their answers, with the whole process taking about 20–30 minutes. This part isn't about passing or failing; it's meant to help staff see where they stand compared to what their job requires. Simple branching logic can streamline completion (e.g., skipping follow-up items when responses are consistent). Civil servants should be able to complete or repeat the self-assessment at any time to reflect new learning, role changes, or evolving responsibilities. This approach encourages a culture of continuous development and allows individuals to monitor their own progress. See **Annex 1** for an example for a limited set of self-assessment questions and instructions on how to apply the TNA.
- **Knowledge checks (relevant concepts/rules/standards):** use mixed formats (MCQ, short answer, brief scenarios), randomized item order, and parallel forms to limit coaching effects. Reference scores to role baselines (criterion-referenced). Such tests verify understanding of core concepts and rules (e.g., GDPR, cybersecurity hygiene, data ethics). This step is especially important to demonstrate compliance and conceptual literacy. It also helps validate the self-assessment results. A proposed knowledge-based TNA questionnaire is included in **Annex 4**, developed in collaboration with university professors specialized in ICT and public administration.
- **Task-based micro-simulations (for selected competencies):** short simulations capturing evidence through action logs (e.g., steps taken, files produced). These methods can be used for the most important competencies that require periodic refresher training, even in broader groups. For example, governments increasingly use digital simulations for incident response training or major process changes across different teams, not just for high-stake or specialized staff. The key is matching the use of simulations to the cost, impact, and need for evidence-based skill demonstration, to ensure evidence for periodic upskilling in areas where hands-on ability truly matters.

125. **The platform should provide confidential, actionable feedback to each civil servant.** Every participant should receive an individual “digital passport” showing (i) current level by competence area versus the expected level for their role, (ii) specific gaps, and (iii) an auto-generated learning path tied to approved courses. Recognition (e.g., badges/micro-credentials) should align to a national schema. A proposed feedback report template is provided in **Annex 2**. The individual overall results and the recommended learning modules should also be visible to the institution and to INA.

126. **The system should equip institutions with aggregated, privacy-safe analytics.** Human resources departments and central agencies should be empowered to access relevant TNA data regarding staff at/above role baseline, heatmaps by competence area, trends by unit/sector. These insights should feed workforce planning and annual training programs. These reporting dashboards should allow interested governmental bodies to plan civil-service, sectoral and institutional-wide development interventions and strategies.

Table 4 presents the key functionalities that should be considered during the design and testing phase of the TNA platform.

Table 4 Key functionalities for the TNA platform

Functional area	What it should do	End-user features	Admin/HR features	Data captured & outputs	Transparency & KPIs	Integration safeguards
Account & role setup	Identify who is assessed and for which role/profile.	Single sign-on; select role/unit; short onboarding.	Bulk user import; role catalog; cohort creation.	User ID, role, unit, seniority, consent.	% onboarded; active users by institution.	SSO with gov ID; RBAC; GDPR consent logs.
Self-assessment (Likert)	Rapid baseline against the national digital CF.	10–15 min questionnaire; progress bar; save & resume.	Editable item bank; routing by role; A/B test items.	Raw item responses; sub-scores by comp	Completion rate; median score by domain/role.	Item versioning; accessibility (WCAG).
Knowledge checks	Objective benchmark on core topics (e.g., cyber).	Short quizzes; immediate feedback.	Question pools; randomization; pass marks.	Scores; pass/fail; attempt history.	Pass rates; retake rates; time-to-pass.	Proctoring options (if needed).
Task/ mini-simulations (optional pilots)	Evidence of “can-do” skills for selected roles.	Scenario tasks; sandbox exercises.	Assign to target roles; scoring rubrics.	Scenario scores; artifacts (files, logs).	# assessed; avg score vs benchmark.	Limited to selected competencies
Automated skill profile	Turn results into a clear skills map.	Personal dashboard; strengths/ gaps by competence/level.	Configurable thresholds/levels (DigComp-aligned).	Profile level per domain; gap list vs role.	Share of staff meeting baseline by unit/role.	Clear explanatory text; printable PDF.
Learning pathway & nudges	Route gaps to training offers.	Recommended courses (internal/external); enroll	Curate catalog; map courses to	Click-throughs; enrollments;	Enrollment→completion conversion; time-to-enroll.	LMS/HRIS API; vendor metadata.

		button; calendar; reminders.	gaps; micro- nudge engine.	completions .			
Individual report	Give each user an actionable plan.	Downloadable report; “what to do next.”	Report template branding; manager view (opt-in).	PDF/HTML report; version timestamp.	% who open/download report; follow-up uptake.	Privacy default; controls sharing.	by user
Manager/Institution dashboards	Support team-level planning.	(If enabled) team snapshot for supervisors.	Aggregated heatmaps by unit/role; filters; export.	Anonymized aggregates; suppression rules.	Coverage by unit; avg gaps; course uptake.		
System-level transparency	Provide public, system-wide metrics.	Public “stats” page with high-level figures.	Configurable open-data feed; periodic publication.	Counts only (exclude any personally identifiable information)	How many tested (12 mo); how many trained; avg completion time; % at/above baseline; courses per user.	Open data; release calendar.	
Certification / micro-badges (optional)	Recognize achievement where relevant.	Digital badges/certificates; wallet download.	Define criteria; verify; revoke.	Issued credentials registry.	# badges issued; validity; renewal rate.	Standards-aligned badges; audit trail.	
Notifications & comms	Drive adoption and completion.	Email/SMS/app reminders; “What’s new” updates.	Campaign scheduler; templates; cohorts.	Open/click rates; reminder cadence.	Completion uplift vs control.	Opt-out controls; language variants.	
Accessibility & language	Ensure equitable access.	RO/EN UI; screen-reader support; low-bandwidth mode.	Content QA; glossary.	Accessibility test logs.	Accessibility conformance score.	WCAG 2.1 AA compliance.	
Audit, logs & security	Guarantee integrity and compliance.	Session timeouts; device warnings.	Full audit logs; role-based data access.	Event logs; consent/audit exports.	Mean time to resolve incidents.	ISO27001 controls; DPIA; retention policy.	

4.4 Integrate learning pathways and recognition

127. **INA, in collaboration with ADR, should develop/curate an approved training catalogue aligned with the digital competency framework.** Each course included should be tagged with essential metadata, such as the specific digital competence it addresses, the required skill level, the modality of delivery (such as in-person, online, or blended learning), the duration, and the assessment method employed. Tagging courses in this structured way allows civil servants to easily identify and select learning opportunities that best match their development needs and career path, promoting personalized and efficient

upskilling. Integrating partner courses from EU-wide resources and local universities further broadens training options and helps standardize digital skills development across all sectors of public administration. Such a systematic, well-tagged catalogue enhances transparency, supports workforce planning, and enables institutions to monitor participation and skills acquisition in real time.

128. **By partnering with leading public universities, INA and ADR can dramatically expand the reach and diversity of their digital skills offerings, integrating academic expertise and cutting-edge research into civil service training programs.** In addition to structured e-learning, the digital platform should actively promote exchange programs, collaborative projects, virtual classrooms, and peer-learning networks, enabling civil servants to benefit from dialogue, teamwork, and the diverse expertise found across academic and administrative communities.
129. **Furthermore, available training programs provided by relevant EU bodies could also be promoted on the platform, such as the offer of the Interoperable Europe Academy.** For example, the Interoperable Europe Academy¹⁰⁹, 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. Its educational catalogue is structured around specific competence areas, learner profiles, and clearly defined learning pathways, allowing for targeted upskilling relevant to public sector roles.
130. **Introduce micro-credentials/badges without tying assessment results to appraisal.** Introduce micro-credentials and badges as tools for recognizing and motivating learning progress, without initially linking assessment results to formal performance appraisal or HR decisions. This approach is supported by the European Council's recommendation on micro-credentials, which highlights their role in promoting flexible, learner-centered education¹¹⁰. As the system matures, certifications obtained through micro-credentials can become an essential source of verified evidence, supporting sustainable workforce development and serving as trusted documentation of staff competencies. Over time, and once robust frameworks and data privacy standards are in place, these certificates and badges can be integrated into wider HR processes - providing a solid basis for career advancement, talent mapping, and targeted training investments. This staged approach helps build trust and engagement, encourages lifelong learning, and aligns with international best practice for public sector digital transformation.
131. **Auto-generate role-aware learning paths.** Immediately after assessment, assign courses tied to a user's gaps vs. expected level. France's PIX ecosystem and Canada's School of Public Service show how to route staff into curated learning tracks that mix compulsory "floor-raising" modules (e.g., cyber hygiene) with elective depth. These learning paths are personalized: they highlight required modules for areas where someone falls below the expected skill level for their job, while also offering elective choices for deeper learning based on individual interests or emerging needs.
132. **A robust approach to public sector cybersecurity training is to require all civil servants to complete a yearly core cyber hygiene module, supplemented with role-based practical exercises.** Drawing inspiration from Estonia's cyber-conscious model¹¹¹, this system should be managed by the lead government digital agency (ADR), and should ensure regular simulated phishing exercises targeting public sector employees. Results should be transparently tracked on manager dashboards, enabling real-time

¹⁰⁹ <https://interoperable-europe.ec.europa.eu/collection/interoperable-europe-academy>.

¹¹⁰ Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02 ST/9790/2022/INIT. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022H0627\(02\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022H0627(02)).

¹¹¹ <https://e-estonia.com/estonias-cyber-security-model-for-europe/>.

monitoring of participation and outcomes, and employees who do not complete or pass essential modules should be required to remediate gaps within 30 days. While Estonia's model does not universally tie completion to e-mail account access, it demonstrates the effectiveness of combining core awareness education with practical, targeted interventions in critical roles or at-risk areas to foster a culture of digital vigilance at scale. Setting a target KPI (such as $\geq 90\%$ annual completion) could also ensure accountability and support continuous improvement of the public sector's cyber resilience.

133. **Update the e-learning catalogue annually based on evolving government priorities, new technologies, and user feedback.** Each cycle should include a brief "What's new" summary and micro-refresh quizzes ("microlearning"), allowing civil servants to quickly adapt to changes and demonstrate ongoing comprehension. For example, priority could be given to adding up-to-date AI modules that address not only technical capabilities but also ethical, data protection, and procurement considerations. The UK Civil Service, for instance, continuously updates its offer of AI e-learning modules for government staff on Civil Service Learning, covering fundamentals, ethics, prompt engineering, and responsible use in procurement as AI adoption accelerates in the public sector¹¹². Making regular, evidence-based catalogue updates and supplementing them with micro-quizzes is increasingly recognized as best practice for maintaining engagement and ensuring knowledge retention.
134. **Expand INA's collaborations with digital academies in other EU member states.** INA is a member of established European networks such as the European Public Administration Network (EUPAN) and can expand connections to digital hubs like the Interoperable Europe Academy, in collaboration with ADR. Such partnerships with digital academies in other EU member states are important to allow exchanging training content, methodologies, and updates in certification standards. Establishing joint programs on core digital competencies, anchored in the DigComp framework, can enable institutions to benefit not only from the collective expertise of partner organizations but also from shared solutions and learning analytics, as seen in transnational initiatives led by the European Commission¹¹³. Such collaboration supports the rapid dissemination of innovation, peer benchmarking, and cost-effective scaling of new learning models, amplifying the impact of digital upskilling campaigns throughout the EU public sector. This strategic approach also helps align Romanian practices with evolving European standards, ensuring continuous improvement and interoperability of digital skills certification across member states.
135. **To inform the future development of training content, Annex 3 includes core elements for digital-competency curriculum for the public administration.** Reflecting the proposed structure of the proposed digital competency framework model, the annex combines two essential building blocks:
 - (i) **learning outcomes**, describing the specific observable knowledge, skills, and attitudes expected at progressive proficiency levels (A-C). The learning outcomes serve as the curriculum spine, defining what public employees must be able to do to operate effectively in digital environments, while the proposed module content translates these outcomes into teachable, assessable units suitable for INA's learning ecosystem; and
 - (ii) **proposed content topics**, outlining the potential scope of learning interventions and examples for practice.
136. **The proposed elements of curriculum are meant to support the link between the digital-competency framework and the content to be developed for the TNA platform.** As part of the TNA Process, individual (self)-assessments against these learning outcomes can generate data on existing skill levels and competency gaps. The structured outcomes enable the TNA tool to produce granular

¹¹² <https://cddo.blog.gov.uk/2024/12/19/artificial-intelligence-must-have-skills-for-the-future/>. Over 70 AI learning modules are available.

¹¹³ <https://interoperable-europe.ec.europa.eu/collection/interoperable-europe-academy>.

diagnostic results (e.g., low proficiency in “Evaluating information” or “Applying data-protection principles”), which can then be aggregated institutionally and system-wide. This ensures that training needs are no longer derived from subjective preferences but from measurable gaps against defined digital competencies. The platform can then automatically match each gap to relevant curriculum components or modules, facilitating data-driven learning recommendations.

137. **For the development of future training programs, the content should be organized around thematic learning areas rather than individual competencies, grouping related skills into coherent, cross-cutting modules.** It is not effective to develop a separate learning module for each individual competency. Instead, modules should be designed and delivered by thematic areas that cluster related competencies into coherent learning experiences. Thematic structuring enables cross-cutting coverage, contextual learning, and better use of resources. For example, a single “Data literacy and evidence-based policymaking” module could integrate competencies from *C1.2 (Evaluating information and data)* and *C1.3 (Managing data and digital content)*, combining analytical and data-management skills in one learning path. Similarly, a “Responsible and ethical digital governance” theme could merge elements from *C2.3 (Digital integrity and accountability)* and *C3.3 (Compliance with digital regulations)*, focusing on integrity, data protection, and responsible AI use.
138. **Digital competencies are inherently interdependent, and effective learning design must reflect their integrated use in real administrative tasks.** In practice, it is almost impossible to design a meaningful task or learning activity that involves only one competence, as most public-administration tasks require the integrated use of two or three competencies simultaneously. For example, a single activity such as formulating a search query based on a research question involves multiple steps—identifying and articulating an information need, locating relevant data, evaluating the credibility of sources, processing the information, and sharing results appropriately. Structuring training by thematic areas therefore ensures that learning reflects how digital work is actually performed, promotes transferability across roles, and supports the acquisition of compound digital capabilities rather than isolated skills. Also, relevant cross-cutting topics (such as digital transformation, AI) were reflected in Output 2 developed under the TSI project.

4.5 Consider a gradual adoption strategy and monitor implementation

139. **Pilot three contrasting settings and publish “how-to” guides.** Pilot the TNA instruments in three contrasting public sector settings, such as one central ministry, one deconcentrated agency, and one municipality, following the example set by Spain’s gradual implementation of the IKANOS project. Use the pilot results to refine survey items, optimize reporting views, and tune user pathways. Document the step-by-step process and outcomes as user-friendly “how-to” guides and FAQs, supporting standardized and scalable deployment. Importantly, piloting across policy-making, service delivery, and operational bodies allows direct testing of both the technical features (such as dashboard views and profile outputs) and the ability of organizational structures to act on the results. This approach ensures that the TNA platform will be adaptable and fit for purpose in a range of public sector contexts, and that it can support organizational learning both for initial launches and future platform updates.
140. **Identify institutional focal points and run time-boxed campaigns on digital skills, with the collaboration of ADR.** Identifying dedicated institutional focal points can be an effective strategy to lift completion rates and rapidly close competency gaps. Mobilizing such digital focal points to support upskilling sessions linked to specific campaigns like the “Cyber Month”¹¹⁴ can lead to more targeted

¹¹⁴ <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/european-cybersecurity-month>.

engagement, better follow-up, and swift improvement in key digital skill areas. Themed campaigns - for example, those focused on cybersecurity awareness, AI literacy, or digital inclusion – can be run in burst periods, combining promotional efforts and peer support to maximize participation and completion within a set timeframe. Ultimately, embedding focal points and periodic campaigns help standardize practice, reinforces the importance of continuous digital learning, and equips organizations to respond rapidly to emerging digital risks or technology adoption needs.

141. **To effectively monitor the TNA process and upskilling of civil servants, a structured monitoring framework should be implemented.** The framework should include both participation and impact indicators, ensuring equity, transparency, and continuous improvement and should enable disaggregation by region, gender, role seniority, and institution. Below is a proposed set of indicators for digital skills TNA and upskilling, presented in a monitoring table:

Table 5 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

4.6 A proposed roadmap for implementation

142. The measures for designing and operationalizing the TNA process and platform for Romania's civil service are proposed for deployment by 2027. A preliminary roadmap is outlined below; however, its timeline and implementation details should be refined in accordance with institutional capacities and available funding resources.

Phase 1 – Governance setup and decision on delivery model (months 0–3)

143. The first phase should focus on establishing clear institutional ownership and project governance arrangements, while also deciding whether the platform will be developed in-house or through an outsourced implementation model. Key actions under this phase could include:

- Establishing an inter-institutional Steering Group comprising representatives from INA, NACS, ADR, and MIPE to oversee the platform's design and financing;
- A formal decision note could be approved to determine the implementation model, either Option A, where the platform is developed and hosted by INA leveraging its existing LMS and e-learning infrastructure, or Option B, where it is procured externally through a competitive tender under a managed-service contract, with INA maintaining data ownership and oversight. In parallel, a three-year financing and staffing plan should be defined, identifying relevant budget lines to support implementation;
- The functional specifications should be approved as the baseline for technical requirements.

Phase 2 – Detailed design and prototyping (months 3–8)

144. **The second phase should focus on translating functional specifications into technical architecture, prototype, and test key workflows.** Key actions under this phase could include:

- Develop technical specifications;
- Develop partnerships and procure services to develop test question bank (A1–A7) and relevant digital courses;
- Define data model and user roles (civil servant, manager, administrator, policymaker);
- Develop wireframes and user journeys: registration, self-assessment, dashboard, and reporting;
- Pilot the self-assessment module internally with 200–300 users across 3 types of institutions;
- Define interoperability requirements with other relevant HRM systems currently under development;
- Prepare technical documentation and security requirements (GDPR, ISO27001 alignment).

Phase 3 – Platform development and pilot deployment (months 8–16)

145. **This phase focuses on building, configuring, and testing the full digital TNA platform under real-world conditions.** It should cover the complete technical development cycle, from system architecture and integration with existing public-administration systems to user-interface design, security protocols, and interoperability with INA's learning infrastructure. Controlled pilot testing should be conducted with selected institutions to validate system functionality, ensure data accuracy, and gather user feedback for refinement prior to full-scale rollout. Key actions under this phase could include:

- Develop and integrate core modules: user registration, self-assessment, reports, dashboards, learning pathways;
- Configure manager and system-level dashboards for aggregated reporting and transparency;
- Conduct technical testing and security audit prior to go-live;
- Train system administrators (INA or vendor) and helpdesk staff;
- Pilot the platform with 3-5 major institutions (at least 3,000 users);
- Collect feedback and refine workflows (data load, user interface, error handling).

Phase 4 – National rollout and capacity building (months 16–28)

146. **This phase focuses on scaling up access to all public institutions and integrating the digital assessment process into a regular, institutionalized TNA cycle.** The aim is to ensure that the platform becomes a standard tool for identifying, updating, and monitoring digital competency development needs across the entire civil service, supporting continuous learning and evidence-based workforce planning. Key actions under this phase could include:

- Onboard all ministries and subordinate agencies to the platform;
- Conduct communication and training campaigns targeting civil servants and HR departments;
- Establish helpdesk and maintenance routines (first- and second-line support);
- Integrate with training catalogues and INA's LMS, enabling one-click enrollment in recommended courses;
- Issue annual individual and institutional reports on digital skills gaps.

Phase 5 – Continuous improvement and transparency (months 28–36 and ongoing)

147. This final phase focuses on institutionalizing the platform's use across Romania's civil service, embedding it into standard HRM and training processes to ensure continuity and long-term impact. It should also strengthen data-driven policymaking by systematically using insights from the platform to inform workforce planning, digital-skills strategies, and training investments. Furthermore, mechanisms for platform maintenance, governance, and periodic updates should be established to guarantee sustainability, scalability, and alignment with evolving EU digital-competence frameworks and national digital-governance priorities. Key actions under this phase could include:

- Publish open data dashboard (number assessed, trained, certifications issued);
- Review question bank annually (update content and add AI-related modules);
- Monitor usage, learning outcomes, and skill improvements;
- Conduct external evaluation;
- Explore integration with EU-level digital academies and certification frameworks.

Table 6 Roadmap for implementation - indicative

Phase	Key Deliverable	Duration	Lead	Option A focus	Option B focus
1	Governance & decision	0–3 mo	INA/ADR/NACS	Define INA team	Prepare TORs
2	Prototype & specs	3–8 mo	INA	Build MVP	Tender & award
3	Pilot platform	8–16 mo	INA/Vendor	Deploy on INA infra	Vendor deploy
4	National rollout	16–28 mo	INA	Internal scaling	Vendor scaling
5	Continuous improvement	28–36+ mo	INA/Steering Group	In-house maintenance	SLA renewals

Annexes

Annex 1 Examples of self-assessment questions using Likert scale, per competence level

Guidance on applying the TNA

- **Create a bank of ~90 Likert statements.** A questions bank of 60–100 items for digital-skills TNAs is common¹¹⁵ Build a larger *bank* and sample from it per session.
- **Per respondent (one sitting):** Keep it **10–15 minutes** (~25–40 Likert items depending on reading speed). Longer surveys degrade data quality due to fatigue
- **Pilot** and target **0.70** pass rate on each subscale; trim or rewrite weak items.
- Align the outcomes to learning paths so results map cleanly to training offers.

Competency (A1–A7)	Level A questions (Basic user)	Level B questions (Independent user)	Level C questions (Advanced/Strategic user)
A1 – Information & Data Literacy	1) I can use institutional websites or online databases to find information for my tasks..	1) I can choose the most relevant online systems or digital repositories for a given task..	1) I can design digital retrieval workflows that integrate multiple systems/datasets.
	2) I can apply basic search functions, filters, or metadata tags in digital tools to locate accurate data.	2) I can use advanced search operators or digital dashboards to verify timeliness and quality	2) I can use data-validation or visualization tools to ensure provenance and compliance.
	3) I can store and organize digital documents (e.g., SharePoint/Teams/cloud) for easy reuse	3) I can combine and summarize data from multiple digital sources to produce a simple analysis or report.	3) I can train colleagues in advanced digital search, data management, and reuse
A2 – Communication & Collaboration	1) I can use email, chat, and videoconference tools to communicate and share files.	1) I can create/manage shared folders or project spaces to coordinate digital work.	1) I can run cross-agency digital channels with appropriate access and security.
	2) I follow digital-etiquette and permissions rules in collaboration tools.	2) I can co-author documents in real time with collaborative editors	2) I can set communication templates/standards that improve clarity and consistency
	3) I can participate in online workspaces (Teams/Drive/SharePoint) created by others.	3) I can organize virtual meetings/webinars and manage digital participation (recording, notes).	3) I can mentor teams on secure file sharing and online facilitation.
A3 – Digital Content Creation	1) I can create basic docs/slides/spreadsheets with office software	1) I can use a CMS/intranet/e-forms tool to publish or update official info..	1) I can design interactive/data-driven content (dashboards, infographics, e-learning)
	2) I can insert images, tables, and charts into digital materials	2) I can adapt content for different audiences/devices (desktop/mobile/PDF)	2) I apply open-data/interoperability standards in institutional content..
	3) I can apply official templates and basic accessibility rules.	3) I ensure version control and consistency across collaborative documents	3) I review/approve content for compliance, accessibility, and impact

¹¹⁵ e.g., DigComp self-assessments run ~80–82 items.

A4 – Security & Data Protection	1) I use strong passwords and MFA on institutional systems.	1) I can manage user permissions and access controls in shared platforms.	1) I can assess cyber-risk exposure and recommend preventive measures.
	2) I can spot phishing/suspicious emails and report them correctly.	2) I recognize/respond to common cyber threats (malware, data leaks).	2) I can coordinate incident response and ensure breach documentation.
	3) I follow basic data-protection rules when handling digital files.	3) I apply secure handling (encryption, anonymization, secure transfer).	3) I contribute to cybersecurity policy/training for the institution.
A5 – Problem Solving & Digital Innovation	1) I use help menus/chatbots/support portals to resolve simple tech issues.	1) I use data-analysis/visualization tools (Excel/BI) to spot inefficiencies.	1) I lead digital-innovation initiatives to streamline processes.
	2) I can identify routine tasks that digital tools could automate	2) I test new software features or pilots in my work.	2) I evaluate cost-benefit and scalability of new tools.
	3) I suggest small improvements to digital forms or processes.	3) I document and share good digital practices that improve workflow	3) I promote a culture of experimentation and learning in transformation projects
A6 – Emerging Tech (incl. AI)	1) I can explain how AI/automation tools affect my daily tasks.	1) I apply AI-enabled/data-driven tools to improve efficiency.	1) I design/oversee AI-assisted workflows or pilots for services.
	2) I can use chatbots/AI assistants for routine retrieval or drafting.	2) I evaluate AI outputs for bias, reliability, and explainability.	2) I advise on ethical, legal, and governance aspects of new tech
	3) I can recognize when an emerging tool is not appropriate (accuracy/privacy).	3) I follow institutional guidance on responsible AI use in decisions	3) I champion responsible adoption and build awareness among colleagues.

1=Not at all confident, 2=Slightly confident, 3=Somewhat confident, 4=Confident, 5=Very confident

Annex 2 Proposed format for assessment reports

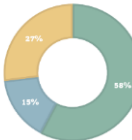
Self – Assessment/ Individual level report - proposed layout

This proposed report aims to provide individuals with a quick overview of their general digital competencies in relation to the institutional framework. It can present the user's current complexity level versus the desired level (A, B, or C), highlight any gaps, and recommend relevant training. The report may also include progress tracker charts based on data collected over time. This example illustrates an assessment report of a high-level civil servant job category, in order to present the most comprehensive format of the report. For the *current* complexity level, the proposed layout includes mockup information, for demonstration purposes. The required levels should be adapted on the platform by each institution as per their specific job categories.

As the report will be in digital format, it can begin with a high-level overview highlighting main gaps in each competency area and recommended actions (Level 1 below). Users should have the option to expand the report for more detailed information (Level 2), including their current complexity level versus the desired level (A, B, or C).

PROFILE SUMMARY

	Name	Ion Maria
	Role Execution Staff, Principal and Superior Department EU Projects and programmes Assessment Date 2025-10-01	

LEARNING & CERTIFICATIONS

Completed: 15
In progress: 4
Not started: 7

LEVEL 1 (Broad view)

Filter by yes/no

Include links where available

	Competency area (Main)	Gap	Recommended actions
FUNDAMENTAL COMPETENCIES	+ 1. Digital literacy	Yes	Course A, Course B
	+ 2. Communication & Collaboration	No	-
	+ 3. Digital content & public services	Yes	Course C, Course E
	+ 4. Resources safe, responsible & sustainable use	No	-
	+ 5. Problem-solving through digital technologies	No	-
DIGITAL TRANSFORMATION	+ 6. Digital transformation in the public administration	Yes	Course G, Course F
DIGITAL LEADERSHIP	+ 7. Digital leadership and governance	Yes	Course H, Course M

LEVEL 2

(Expanded view - includes individual's current complexity level versus the desired level (A, B, or C).

Legend:  Target level  Current level  Current level coincides with target level

	Competency area (Main)	Competency	A	B	C	Recommended actions
FUNDAMENTAL COMPETENCIES	1. Digital literacy	1.1 Searching & accessing data, information, and digital content				Course A, comments
		1.2 Evaluating information, and digital content; data analysis				-
		1.3 Managing data, information, and digital content				-
	2. Communication & Collaboration	2.1 Citizen and businesses participation				Course B, comments
		2.2 Sharing and collaborating				-
		2.3 Ensuring digital integrity and accountability				Course C, Course D
	3. Digital content & public services	3.1 Developing, integrating and re-using digital content				-
		3.2 Delivering and contributing to digital public services				Course G, Course F
		3.3 Ensuring compliance with digital regulatory frameworks and standards				-
	4. Safe, responsible and sustainable use of resources	4.1 Protecting devices and infrastructures				-
		4.2 Managing digital identities, and protecting personal data and privacy				-
		4.3 Promoting healthy and sustainable digital practices				Course G
	5. Problem-solving through digital technologies	5.1 Managing digital devices				Course H
		5.2 Using automation tools				-
DIGITAL TRANSFORMATION	6. Digital transformation in the public administration	6.1 Contributing to digital transformation, driving innovation and improvement				-
		6.2 Developing digital competence in the workplace				- Course I
		6.3 AI Literacy				-
DIGITAL LEADERSHIP	7. Digital leadership and governance	7.1. Managing performance and operations				Course J
		7.2. Leading team development in the digital environment				-
		7.3. Driving and leading innovation and digital transformation				-
		7.4. Ensuring responsible digital governance and cybersecurity				Course M
		Strategic thinking				Course B

Institutional-level dashboard

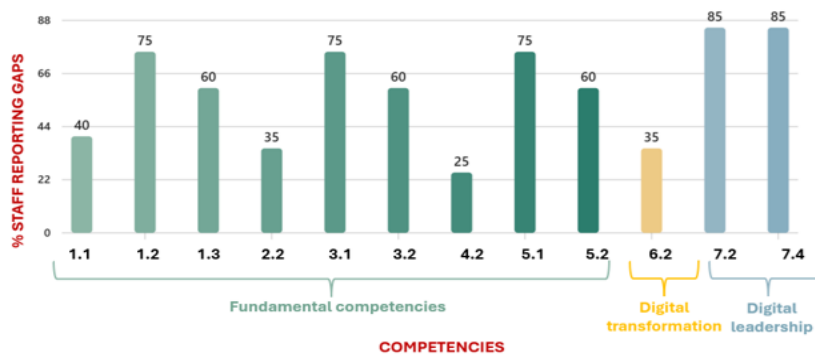
INA level – General overview report

The report presents aggregated percentage gaps for each competency, and outlines recommended actions and training to address identified needs. INA should also have access to assessment reports at institutional, departmental, and individual level.

General overview report					
	Competency area (Main)	Competency	Gap	% staff recording gap	Proposed courses/ actions
FUNDAMENTAL COMPETENCIES	1. Digital literacy	1.1 Searching	Yes	40%	Course A
		1.2 Evaluating	Yes	75%	Course B
		1.3 Managing	Yes	60%	-
	2. Communication & Collaboration	2.1 Citizen and businesses participation	No	-	-
		2.2 Sharing and collaborating	Yes	35%	Course C, comments
		2.3 Ensuring digital integrity and accountability	No	-	-
	3. Digital content & public services	3.1 Developing, integrating and re-using digital content	Yes	75%	Course D
		3.2 Delivering and contributing to digital public services	Yes	60%	Course E, comments
		3.3 Ensuring compliance with digital regulatory frameworks and standards	No	-	-
	4. Safe, responsible and sustainable use of resources	4.1 Protecting devices and infrastructures	No	-	-
		4.2 Managing digital identities, and protecting personal data and privacy	Yes	25%	-
		4.3 Promoting healthy and sustainable digital practices	No	-	Course F
DIGITAL TRANSFORMATION	6. Digital transformation in the public administration	6.1 Contributing to digital transformation, driving innovation and improvement	No	-	-
		6.2 Developing digital competence in the workplace	Yes	35%	-
		6.3 AI Literacy	No	-	Course I
DIGITAL LEADERSHIP	7. Digital leadership and governance	7.1. Managing performance and operations	No	-	Course J, comments
		7.2 Leading team development in the digital environment	Yes	85%	-
		7.3. Driving and leading innovation and digital transformation	No	-	-
		7.4. Ensuring responsible digital governance and cybersecurity	Yes	85%	Course K
		Strategic thinking	No	-	Course M, comments

The general overview report could be accompanied by additional visual representation of the data, such as overall gap view, heatmaps and progress charts. An example is presented below.

Example of public administration overall competencies gap view



Example of data view at institutional level

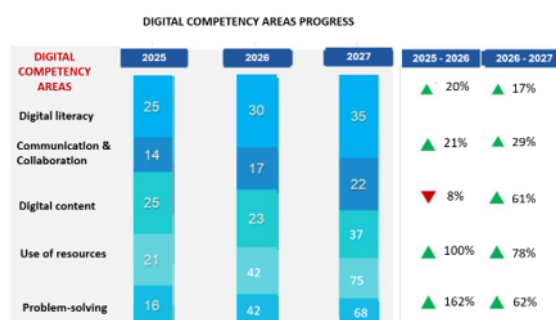
Institutional level			
Department	# Personnel	% GAP	Competency area recording gaps
HR	15	20%	2. Communication & Collaboration
Financial	20	80%	4. Safe, responsible and sustainable use of resources
EU financed Projects	7	35%	3. Digital content & public services
	42	45%	

HR Department, Staff general overview

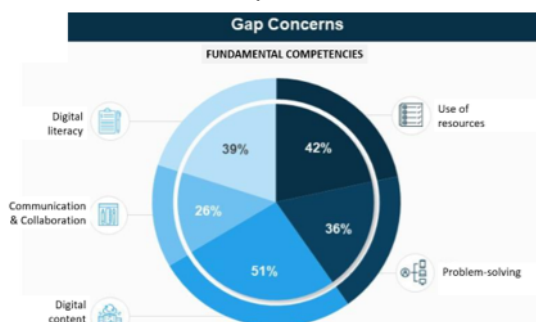
Employee name	Role	Overall skill gap	FUNDAMENTAL COMPETENCIES														DIGITAL TRANSFORMATION			DIGITAL LEADERSHIP			
			1.Digital literacy			2. Communication & Collaboration			3.Digital content			4.Use of resources			5.Problem-solving		6. Digital transformation			7.Digital leadership			
			1.1	1.2	1.3	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3	5.1	5.2	6.1	6.2	6.3	7.1	7.2	7.3	7.4
Maria Ionel	Unit Head	55%	✓	⚠	⚠	✓	✓	⚠	✓	✓	⚠	✓	✓		✓	✓	⚠	✓	⚠	✓	⚠	✓	✓
Ion Maria	Counselor	65%	⚠	✓	✓	⚠	✓	⚠	⚠	✓	✓	✓	⚠	⚠	✓	✓	-	-	-	-	-	-	-

Based on the available data, it should be possible to create additional visualizations, such as overall gap analyses, heatmaps, and progress charts. These representations can help to better illustrate key trends and insights. Two examples are presented below.

Example of visual representation of digital competency areas progress



Example of visual representation of gap concerns with a focus on fundamental competencies



Annex 3 Elements of curriculum proposed based on the proposed general digital competency framework for the public administration

A1. Digital literacy in public administration

C1.1. Searching and accessing data, information and digital content

1) Learning outcomes

D1. Identify and articulate information needs; choose appropriate search services (Level A)

By the end, public employees will be able to:

- Express clear information need linked to a specific task (e.g., report, policy brief, citizen guidance).
- Map the need to suitable services (e.g., general web search, official portals, intranet, open-data catalogues) and justify the choice.
- Draft a simple search plan (keywords, synonyms/abbreviations, basic operators, initial filters).
- Evaluate the initial results for relevance and adjust the plan accordingly (S).
- Record the chosen service, query, and source for transparency and later verification.

D2. Establish simple search strategies on intranet and shared storage (Level A)

By the end, public employees will be able to:

- Navigate sites/libraries using folder structure and views to reach relevant locations.
- Use simple queries and filters (file type, author, modified date, site/folder) to narrow results.
- Check version history/last modified to access the latest valid document and avoid duplicates.
- Share stable links and respect permissions and basic information-security rules.

D3. Search professional content, resources, and databases for PA tasks (Level A)

By the end, public employees will be able to:

- Identify authoritative sectoral databases - RO/EU legislation (i.e., AI Act, Data Act, DGA, DPIA, GDPR, NIS2), statistics (i.e., PNI, INS), standards (i.e., EN 301 549, ISO 2700, ISO 42001), official guidance (e.g., SDG), relevant to their role.
- Formulate 2–5 keyword queries with basic operators and apply filters (date, jurisdiction, document type).
- Open retrieved items and locate the specific figures/facts needed; note the source (title, URL/ID, date).
- Save/bookmark resources for reuse and share them with minimal citation metadata.

D4. Recognize key features and purposes of diverse search services, including AI and specialized databases (Level B)

By the end, public employees will be able to:

- Classify services by scope and typical use-cases (web search, enterprise/intranet, legal/statistical DBs, academic indexes, AI assistants).
- Explain strengths/limitations (provenance, update cycles, coverage, bias) and compliance aspects for each type.
- Select the best-fit service for a defined administrative task and articulate the rationale.
- Describe when to use conversational/AI search versus database queries to optimize effort and evidence quality.

D5. Use advanced features and interact with AI systems by developing/refining prompts (Level B)

By the end, public employees will be able to:

- Compose structured prompts (task, context, preferred sources, constraints, output format) to guide AI retrieval.

- Combine advanced search settings (filetype, site/domain limits, date ranges) with AI prompting (e.g., “explain and cite sources”).
- Iteratively refine prompts with constraints/examples and success criteria to improve precision and recall.
- Save effective prompts/queries as templates and set alerts/saved searches for recurring tasks.
- Assess AI outputs for bias or inaccuracies, documenting any refinements (S/A).

D6. Integrate emerging/complex search technologies (including AI) to surface institutional knowledge and support strategic decisions (Level C)

By the end, public employees will be able to:

- Design integration workflows (connectors/APIs, metadata standards, access controls) across intranet, DMS, data portals, and AI assistants.
- Ensure explainability, provenance, and audit trails in outputs used for decision-making.
- Define and monitor search-quality metrics (coverage, freshness, precision/recall, user feedback) and act on findings.
- Establish governance practices (permissions, retention, responsible AI use) aligned with institutional policies.
- Pilot integrated workflows in a Romanian PA context (e.g., linking NACS HRM data with ADR platforms) and evaluate outcomes (S).

D7. Perform advanced/complex/specialized searches using AI and specialized services to meet complex PA information needs (Level C)

By the end, public employees will be able to:

- Plan and execute multi-source strategies that combine AI-assisted retrieval with sectoral databases, open-data portals, and institutional repositories.
- Triangulate findings, document assumptions and gaps, and report confidence levels for robust evidence.
- Produce concise, source-referenced decision briefs (implications, risks, options) for senior stakeholders.
- Coach teams in the strategic use of AI and specialized search to address non-routine, high-stakes queries.

2) Proposed content topics for potential modules

1. From task to information need (Level A) - turning vague requests into SMART search questions;
Examples: convert “update our citizen guidance” into a precise query plan.
2. Choosing the right service (Level A) - matrix of task vs. source (web search, intranet, legal/statistical DBs, open data, AI assistants);
Examples: selecting the portal for local, national or EU legislation.
3. Intranet & SharePoint essentials (Level A) - library navigation, metadata, version history, stable links, permissions; *example:* finding the latest approved template in a team library.
4. Core operators & filters (Level A) - quotes, AND, site:, filetype:, date ranges;
Examples: narrowing to “.gov.ro” or similar PDFs published in the last 12 months.
5. Sectoral databases for PA (Level A) - legislative, statistical, standards, and guidance repositories;
Examples: retrieving official indicators and citing identifiers/version dates.
6. Understanding service types (incl. AI) (Level B) - features, coverage, update cycles, bias, compliance;
Examples: when conversational AI helps vs. when a legal DB is mandatory.
7. Prompting for retrieval (Level B) - prompt structure (context–task–sources–constraints–format); iterative refinement;

Examples: “Explain and cite” patterns that return verifiable outputs.

8. Search + AI orchestration (Level B) - combining advanced filters with AI summarization and citation extraction;

Examples: building a short brief with linked sources.

9. Integrating search across systems (Level C) - connectors/APIs, shared taxonomies, access controls;

Examples: surfacing DMS records and open-data entries in a single view.

10. Governance, provenance, and audits (Level C) - traceability, retention, responsible AI use;

Examples: maintaining an evidence log for policy notes. Align with NIS2 and Romania's National Cybersecurity Strategy.

11. Measuring search effectiveness (Level C) - coverage, freshness, precision/recall, user feedback;

Examples: improving a saved strategy based on KPI trends.

12. Advanced multi-source searches (Level C) - triangulation and confidence reporting for complex needs;

Examples: cross-checking indicators from multiple official datasets. Incorporate foresight elements (e.g., predictive analytics for digital transformation).

C1.2. Evaluating information and digital content, including data analysis

1) Learning outcomes

D1. Understands that not all online information is reliable and some is designed to influence (Level A)

By the end, public employees will be able to:

- Identify common manipulation patterns (misleading framing, cherry-picking, emotional triggers) and explain why they reduce reliability.
- Distinguish fact, opinion, and advocacy content, and label the type of influence intended (persuasion, mobilization, commercial).
- Apply a quick credibility triage (publisher, purpose, evidence, transparency) before investing time in deeper analysis.

D2. Distinguishes reliable sources of evidence for policy from other information (Level A)

By the end, public employees will be able to:

- Classify sources by evidentiary value (e.g., peer-reviewed research, official statistics, administrative data, expert commentary, media reports).
- Explain the difference between causal, correlational, and descriptive evidence and when each is appropriate in policy work.
- Justify the inclusion/exclusion of a source in a policy brief based on methodological quality, transparency, and relevance.

D3. Evaluates public data and their sources (e.g., INS, Eurostat, OECD) for PA tasks (Level A)

By the end, public employees will be able to:

- Check dataset provenance, update cycle, coverage, and comparability across regions/time.
- Assess fitness-for-purpose (operational definitions, units, denominators, missingness) before analysis or comparison.
- Document reuse conditions and cite datasets correctly (title, publisher, version/date, URL/identifier).

D4. Understands “data-driven public administration” and the value of data (Level B)

By the end, public employees will be able to:

- Articulate how data supports decision-making, process design, service improvement, and delivery.
- Describe the data value chain from collection to impact (ingest → quality assurance → analysis → decisions).

- Identify ethical, legal, and organizational prerequisites (governance, data protection, fairness, accountability).

D5. Use indicators to monitor activities and policies (Level B)

By the end, public employees will be able to:

- Define indicators with clear constructs, formulas, baselines, targets, and data sources.
- Compute and interpret basic indicator types (levels, rates, ratios, trends) and visualize them appropriately.
- Explain limitations (lags, measurement error, denominator effects) and how these affect conclusions.

D6. Values the role of data in decision-making and policy-making (Level B)

By the end, public employees will be able to:

- Formulate decision questions as analyzable problems and specify the minimum evidence needed.
- Weigh trade-offs between timeliness and rigor; recommend proportionate analysis for the decision at hand.
- Advocate for data reuse/sharing where lawful and beneficial to public value.

D7. Critically analyses, compares, and validates digital content and data sources (Level B)

By the end, public employees will be able to:

- Apply a structured appraisal (credibility, reliability, completeness, appropriateness) to documents, datasets, and dashboards.
- Cross-verify claims with independent high-quality sources; record assumptions and confidence levels.
- Detect common analytic pitfalls (survivorship bias, p-hacking cues, misuse of averages) and correct them.

D8. Assesses and compares data, visualizations, and content to make accurate inferences (Level C)

By the end, public employees will be able to:

- Read charts critically (axes, scales, encodings, uncertainty) and spot misleading design choices.
- Choose suitable visual forms for comparisons, change over time, proportions, and distributions.
- Synthesize multi-source evidence into clear, source-referenced findings that support policy development in a defined field.

D9. Evaluates and audits strategies to analyze and interpret data for policy development (Level C)

By the end, public employees will be able to:

- Design proportionate analysis plans (questions, metrics, methods, data sources, quality checks) and justify method choices.
- Conduct light-touch audits of analysis workflows (reproducibility, versioning, documentation, peer review).
- Produce concise audit notes with recommendations to improve data quality, analysis, and interpretability.

2) Proposed content topics for potential modules

1. Credibility triage for online information (Level A) - A rapid screening to decide if content merits deeper analysis, using a few high-yield signals (publisher, purpose, evidence, transparency).
Examples: apply a 4-signal check to a viral claim; flag manipulation patterns (emotional triggers, cherry-picking).
2. Evidence hierarchies for policy (Level A) - How to rank sources by evidentiary value and select proportionate evidence for the decision at hand.
Examples: when to rely on administrative data vs. peer-reviewed studies; weigh expert consensus for urgent guidance.

3. Public datasets fitness-for-purpose (Level A) - Assess provenance, update cycle, coverage, comparability, and licensing before using official datasets.
Examples: evaluate an indicator from INS/Eurostat/OECD; check metadata for definitions, units, and denominators.
4. Data-driven PA in practice (Level B) - Translate decision needs into analyzable questions; map the data value chain and required governance.
Examples: define the evidence needed to redesign a service; identify roles for quality assurance and stewardship.
5. Designing and using indicators (Level B) - Build clear indicators (construct, formula, baseline, target) and interpret levels, rates, and trends.
Examples: compute a rate per 100k; explain why a changing denominator alters conclusions.
6. Data quality and uncertainty (Level B) - Spot and manage missingness, outliers, and measurement error; communicate uncertainty responsibly.
Examples: simple imputation choices; add confidence intervals or caveats to a finding.
7. Chart literacy and visualization ethics (Level C) - Read and design charts that are truthful and clear; avoid misleading encodings.
Examples: identify truncated axes; choose between line, bar, and proportion charts for the message.
8. Comparative analysis across sources (Level B) - Triangulate claims using multiple datasets; reconcile conflicts and document assumptions.
Examples: cross-check a statistic against two official sources; write a short “assumptions & confidence” note.
9. From findings to decision briefs (Level C) - Synthesize evidence into concise, source-referenced briefs with options, risks, and implications.
Examples: one-page brief for a policy choice; annex with cited tables/links.
10. Light-touch analytics audits (Level C) - Check reproducibility, documentation, versioning, and peer review of simple analyses and dashboards.
Examples: run an audit checklist on a monthly KPI report; verify data lineage and last update.
11. Responsible sharing and reuse (Level B) - Apply data-protection, licensing, and minimization principles when sharing or repurposing information.
Examples: choose a lawful basis for reuse; share an anonymized extract via a secure workspace.
12. Common analytical fallacies (Level B) - Recognize cognitive/statistical pitfalls and apply guardrails to avoid them.
Examples: base-rate neglect in trend interpretation; ecological fallacy in regional comparisons.
13. Dashboards and monitoring (Level B) - Read dashboard designs critically; distinguish signal from noise and set actionable thresholds/alerts.
Examples: interpret a sudden spike vs. normal variation; define trigger levels for follow-up.
14. Case labs (role-specific scenarios) (Level C) - Apply end-to-end evaluation on realistic PA tasks, from question to brief.
Examples: validate a statistic for a press note; audit a monitoring report for a funding program.

C1.3. Managing data, information and digital content

1) Learning outcomes

D1. Choose appropriate storage locations (local device, corporate network, cloud) (Level A)

By the end, public employees will be able to:

- Match a task to the most suitable storage location based on sensitivity, collaboration needs, availability, and continuity requirements.
- Explain basic trade-offs (speed, offline access, sharing, security posture) between local, network, and cloud storage.
- Apply institutional rules for file placement, access permissions, and backup/restore procedures.

D2. Organize and format data in spreadsheets for simple management/processing (Level A)

By the end, public employees will be able to:

- Structure a worksheet as tidy data (one row = one record; one column = one variable) and apply consistent data types and formats.
- Use core functions (e.g., text/date cleaning, basic math/aggregation) and validation rules to minimize errors.
- Create simple tables, pivot tables, and filters to support routine reporting and hand-offs.

D3. Identify PA-relevant data management tools and platforms (DMS, collaborative suites, institutional DBs, cloud) (Level A)

By the end, public employees will be able to:

- Describe the purpose and key features of common platforms (document management systems, collaborative workspaces, databases, cloud drives).
- Choose the right tool for a given task (drafting, approval workflow, records retention, data entry/lookup).
- Follow sign-in, roles/permissions, and shared-space conventions for safe collaboration.

D4. Organize, store, and retrieve data/content across institutional tools (Level B)

By the end, public employees will be able to:

- Apply a consistent folder/taxonomy scheme, file naming, and metadata to ensure traceability and retrieval.
- Use search, filters, and saved views to quickly locate authoritative versions; maintain links rather than copies.
- Execute small “content hygiene” actions (archive, de-duplicate, move to correct library) according to institutional guidance.

D5. Apply data-analysis techniques (Excel, Power BI, AI-assisted analytics) to support policy development (Level B)

By the end, public employees will be able to:

- Prepare data for analysis (clean, join, transform) and choose appropriate visual summaries (trend, comparison, composition).
- Build a simple dashboard/report (e.g., in Excel or Power BI) with clear titles, sources, and update cadence.
- Use AI-assisted analysis responsibly (prompt for methods, ask for assumptions, request citations) and verify outputs.

D6. Structure, document, and explain datasets clearly for others (Level B)

By the end, public employees will be able to:

- Knows the institution’s documentation and archiving rules, basic privacy/IP constraints, and what “good” looks like for reusability.
- Models a transparency-and-reuse mindset: proactively documents datasets so colleagues can understand, audit, and extend them.
- Produce a compact data README (purpose, scope, update cycle, fields, definitions, limitations).
- Maintain a data dictionary (variables, units, encodings, allowed values) and version notes.

D7. Use basic data cleaning and validation to ensure accuracy and usability (Level B)

By the end, public employees will be able to:

- Detect and correct common issues (duplicates, inconsistent categories, missing/invalid values, wrong types).
- Implement validation rules, drop-down lists, and controlled vocabularies to prevent data drift.
- Keep an audit log of changes that affect reports or decisions.

D8. Use big-data techniques (e.g., data mining, simulation) for advanced PA analysis (Level C)

By the end, public employees will be able to:

- Explain when advanced techniques are proportionate (scale, complexity, timeliness) and the prerequisites (governance, skills, compute).
- Interpret outputs from data mining/simulation at a conceptual level and communicate uncertainty and assumptions.
- Coordinate with specialized teams to scope an advanced analysis that meets a policy question.

D9. Apply institutional standards, classifications, e-archiving rules, and metadata (Level C)

By the end, public employees will be able to:

- Classify and tag content using approved taxonomies; populate mandatory metadata fields.
- Apply electronic archiving and retention schedules; ensure traceability, provenance, and lawful access.
- Periodically review and update shared libraries to maintain findability and compliance.

D10. Recognize data as a strategic asset for service delivery, management, and innovation (Level C)

By the end, public employees will be able to:

- Articulate how better data management improves citizen services, organizational performance, and policy outcomes.
- Identify opportunities to reuse data safely and ethically, and to automate routine processes.
- Advocate for continuous improvement (feedback loops, metrics, training) in data practices.

2) Proposed content topics for potential modules

1. Storage decisions: local vs. network vs. cloud (Level A) - How to select the right location for security, collaboration, and continuity.
Examples: When to keep a draft on a local device; moving approved documents to the DMS; sharing via a controlled cloud folder.
2. Folder structures, naming, and metadata (Level B) - Practical conventions that make content findable and auditable across teams.
Examples: YYYY-MM-DD naming; project-code prefixes; mandatory metadata fields for programme files.
3. Spreadsheets that don't break (Level A) - Tidy layouts, data types, validation, and lightweight automation for reliable reporting.
Examples: Build a tidy table; apply data validation lists; create a pivot table for a monthly KPI.
4. Everyday cleaning and validation (Level B) - Low-effort techniques to improve accuracy before analysis or sharing.
Examples: Deduplicate beneficiaries; standardize categories; flag out-of-range values with conditional formatting.
5. From table to insight (Excel/Power BI) (Level B) - Turning prepared data into clear visuals and short, source-referenced findings.
Examples: A one-page dashboard with trend, comparison, and target lines; annotate with data source and update date.
6. Working in DMS and collaborative platforms (Level A) - Check-in/out, version history, approvals, and link-sharing best practices.
Examples: Move files from personal drives to a team library; use version comments; create a "read-only" share link.
7. Institutional standards and e-archiving (Level C) - Apply classifications, retention rules, and provenance to keep records trustworthy.
Examples: Tag records with programme codes; archive expired versions; log source and author metadata.
8. Data documentation that others can use (Level B) - Minimal READMEs and data dictionaries that enable reuse and onboarding.
Examples: Write a 10-line README; create a data dictionary with units and allowed values; note limitations.

9. Responsible reuse and sharing (Level B) - Permissions, licensing, and data-minimization principles for safe collaboration.
Examples: Share an anonymized extract; choose the correct license; restrict access to sensitive folders.
10. Search and retrieval across systems (Level B) - Use filters, saved searches, and stable links to find and reference the right version.
Examples: Find the latest approved template via metadata; save a filtered view; replace duplicates with a canonical link.
11. AI-assisted analysis (responsibly) (Level B) - How to prompt for methods, assumptions, and citations; how to verify and document outputs.
Examples: Ask an assistant to suggest a method and list data requirements; validate results against the source table.
12. When to consider advanced techniques (Level C) - Situations where mining/simulation are proportionate and how to engage specialists.
Examples: Scoping a simulation to test service demand; documenting assumptions and uncertainty bands.
13. Quality gates for publication and reporting (Level B) - Lightweight checklists to ensure accuracy, consistency, and traceability.
Examples: Pre-publication checklist; verify figures against source; ensure charts have titles, units, and sources.
14. Data as an organizational asset (Level C) - Building feedback loops and KPIs for continuous improvement in data practices.
Examples: Define a data-management KPI; run a quarterly cleanup; capture lessons learned for the team playbook.

A2. Digital communication and collaboration

C2.1. Communicating, interacting and fostering citizen and businesses participation through digital technologies

1) Learning outcomes

D1. Use appropriate communication styles and linguistic registers; ensure simplicity and clarity (Level A)

By the end, public employees will be able to:

- Match tone, register, and structure to the channel (email, portal notice, social post, chat) and the intended audience.
- Apply plain-language and clarity rules (short sentences, concrete verbs, consistent terminology) to reduce cognitive load.
- Adapt messages for mobile reading (front-loading key information, scannable formatting) and for assistive technologies.

D2. Interact via inclusive digital channels to enable meaningful participation for diverse groups (Level A)

By the end, public employees will be able to:

- Identify barriers to participation (literacy, connectivity, language, disability) and choose inclusive channels accordingly.
- Apply accessibility practices (alt text, captions, readable contrast, simple navigation) and provide low-barrier options (SMS, phone-back, mediated kiosks).

- Design feedback tasks that are understandable and doable for people with limited digital skills.

D3. Understand how digital/social media shape perception and participation and apply this insight in strategies (Level A)

By the end, public employees will be able to:

- Explain how algorithms, virality, and network effects influence public narratives and engagement.
- Incorporate social listening and audience segmentation into outreach plans while mitigating misinformation risks.
- Select formats (threads, reels, infographics, FAQs) that match strategic objectives and community norms.

D4. Use professional digital tools (email, collaborative platforms, internal messaging) effectively (Level A)

By the end, public employees will be able to:

- Compose, send, and organize professional communications using shared mailboxes, labels, templates, and retention rules.
- Coordinate with colleagues via collaborative platforms (channels, @mentions, file links, version history) while respecting records-management policies.
- Choose synchronous vs. asynchronous tools to reduce overload and support traceability.

D5. Select the most appropriate tool to interact with citizens and organizations by legal nature, complexity, and formality (Level B)

By the end, public employees will be able to:

- Use a channel-selection matrix to decide between formal (eDelivery, registered email, portal) and informal (social, chat) options.
- Apply escalation paths from informal contact to formal notice when legal effects are required.
- Document rationale for tool choice and ensure messages meet evidentiary and archiving requirements.

D6. Foster digital engagement by citizens and businesses (platforms, forums, open-data reuse) (Level B)

By the end, public employees will be able to:

- Design and moderate online participation spaces (consultations, forums, Q&A sessions) with clear rules of engagement.
- Encourage third-party reuse of open data (hackathons, challenges, developer guides) and recognize community contributions.
- Close the loop by reporting “you said - we did” outcomes to sustain trust.

D7. Develop and deliver digital presentations tailored to audiences and administrative purposes (Level B)

By the end, public employees will be able to:

- Plan audience-specific narratives (purpose, key message, evidence) and choose suitable formats (slides, dashboards, one-pagers).
- Apply design fundamentals (readable typography, chart choice, alt text) and ensure remote-friendly delivery (recording, captions).
- Publish presentation artefacts with source references and accessible downloads.

D8. Recognize citizens’ digital interactions as expressions of digital citizenship (Level B)

By the end, public employees will be able to:

- Frame digital contact not just as service demand but as participation in public life.
- Identify opportunities to empower users (self-service, co-design sessions, idea boards) and remove unnecessary friction.
- Reflect citizen rights and responsibilities in terms of use, privacy notices, and community guidelines.

D9. Assess and audit digital interaction tools against communication/interaction goals (Level C)

By the end, public employees will be able to:

- Evaluate tools on accessibility, data protection, security, auditability, multilingual support, analytics, and integration features.
- Run proportional risk and context checks (sensitivity of use case, required reliability, user capabilities).
- Produce short assessment notes with recommendations and migration paths where needed.

D10. Contribute to open and participatory digital ecosystems that enhance engagement, trust, and satisfaction (Level C)

By the end, public employees will be able to:

- Build partnerships with communities, NGOs, and businesses to co-create content, services, and standards.
- Implement transparency practices (open roadmaps, changelogs, public dashboards) and publish structured feedback responses.
- Monitor engagement and trust indicators, and adapt approaches to strengthen legitimacy and satisfaction.

2) Proposed content topics for potential modules

1. Plain language and register across channels (Level A) - Techniques to simplify messages and match tone to email, portals, social, or chat.
Examples: Rewrite a legalistic notice into a clear citizen update; convert a chat response into a formal portal announcement.
2. Inclusive-by-design communication (Level A) - Remove barriers for low digital skills, low bandwidth, and accessibility needs.
Examples: Create alt text and captions; provide an SMS fallback for a consultation; design a “simple language” FAQ.
3. Channel selection and escalation (Level B) - Decide which tool fits the message’s legal effect, complexity, and urgency.
Examples: Choose between chat vs. formal portal message; define when to escalate to registered delivery.
4. Professional email and collaboration hygiene (Level A) - Structure team inboxes, use templates, and keep a usable audit trail.
Examples: Build a reply template library; set retention labels; replace attachments with document links.
5. Social media for public value (Level A) - Strategy, social listening, content formats, and risk controls for institutional accounts.
Examples: Plan a myth-busting thread; set a moderation protocol; choose formats (carousel, short video) for engagement.
6. Designing participation spaces (Level B) - Create and moderate online consultations, forums, and Q&A with clear participation rules.
Examples: Draft a code of conduct; set moderation workflows; conduct a live Q&A with a follow-up summary.
7. Open data engagement and civic tech (Level B) - Enable third-party reuse and showcase value created by businesses and communities.
Examples: Launch a dataset improvement challenge; publish API guides; feature reuse stories on the portal.
8. Digital presentations and storytelling (Level B) - Build audience-centric presentations and remote-friendly delivery.

Examples: Turn a complex policy memo into a 5-slide story; add captions and accessible charts for a webinar.

9. Community management and moderation (Level B) - Maintain healthy dialogue and safe spaces across institutional channels.

Examples: Draft response ladders for difficult comments; implement escalation for harassment or misinformation.

10. Privacy, security, and records in digital communications (Level B) - Communicate lawfully and keep trustworthy records.

Examples: Write a privacy notice for a survey; classify a thread for retention; choose secure channels for sensitive topics.

11. Measuring engagement, trust, and satisfaction (Level B) - Define KPIs, collect feedback, and act on insights.

Examples: Build a simple engagement dashboard; run a post-interaction survey; conduct A/B tests on a service update.

12. Tool assessment and procurement basics (Level C) - Audit features, accessibility, compliance, and total cost for interaction tools.

Examples: Compare two live-chat platforms; document risks and a migration plan; assess multilingual support.

13. Crisis and incident communication online (Level B) - Coordinate rapid, accurate, and compassionate messaging under pressure.

Examples: Draft holding statements; set approval chains; maintain a real-time updates page with timestamps.

14. Co-creation labs with citizens and businesses (Level C) - Facilitate collaborative problem-solving and feedback loops.

Examples: Run an ideation sprint; publish a “you said - we did” report; integrate suggestions into a public roadmap.

15. Ethics of digital participation (Level B) - Promote fairness, inclusion, and respectful dialogue; recognize digital citizenship.

Examples: Review a participation plan for bias; ensure language and imagery are inclusive; set rules for respectful debate.

C2.2. Sharing and collaborating in digital teams in intra and interinstitutional contexts

1) Learning outcomes

D1. Use collaborative tools to coordinate activities and monitor progress (Level A)

By the end, public employees will be able to:

- Set up and manage team workspaces (project boards, shared calendars, time-reporting) to track tasks, owners, status, and due dates.
- Configure views (Kanban, calendar, Gantt) and basic automations (reminders, status rules) to keep work flowing.
- Produce concise progress updates and dashboards for managers and partners.

D2. Work effectively in digital teams through documentation, shared calendars, and task-tracking (Level A)

By the end, public employees will be able to:

- Establish and follow a light documentation standard (meeting notes, decision logs, how-to pages) that supports hand-over and continuity.

- Coordinate schedules using shared calendars and availability etiquette; align task boards with meeting cadences.
- Maintain a single source of truth (linking documents to tasks/events) to reduce duplication.

D3. Co-develop materials and coordinate using shared documents and boards (Level A)

By the end, public employees will be able to:

- Co-author documents/spreadsheets/presentations in real time (track changes, comments, versions) with clear ownership and review steps.
- Break down deliverables into tasks, define acceptance criteria, and monitor progress through milestones.
- Run short “working sessions” in which materials are produced collaboratively rather than discussed abstractly.

D4. Manage roles and permissions in collaborative environments and workflow tools (Level B)

By the end, public employees will be able to:

- Apply least-privilege access (viewer, commenter, editor, owner) and time-bound sharing links for both synchronous and asynchronous work.
- Grant/revoke access to files and workflows; audit who has access and why.
- Resolve common permission issues and document the rationale for access decisions.

D5. Use institutional tools/platforms that enable inter-institutional coordination and joint service delivery (Level B)

By the end, public employees will be able to:

- Navigate case-management systems, inter-agency portals, and shared databases to progress joint workflows.
- Exchange structured updates (case notes, status codes, service SLAs) that other institutions can act on.
- Escalate blockers across organizations using agreed protocols and evidence.

D6. Value and apply open data standards to promote trust and reliability (Level B)

By the end, public employees will be able to:

- Explain why open formats, metadata, and standard vocabularies improve access, reuse, and public trust.
- Choose interoperable formats when publishing or exchanging non-sensitive data.
- Reference datasets with clear provenance (publisher, version/date) to enable verification.

D7. Promote documenting basic workflows in digital formats to preserve institutional knowledge (Level B)

By the end, public employees will be able to:

- Capture step-by-step procedures (who/what/when/tools/inputs/outputs) with screenshots or short clips.
- Keep workflow pages current via versioning and change logs; archive superseded steps.
- Embed workflow links in task templates so teams can execute consistently.

D8. Use secure digital systems and protocols to exchange information with other institutions/external stakeholders (Level B)

By the end, public employees will be able to:

- Select appropriate secure channels (eDelivery, encrypted email/portals, SFTP/API) based on sensitivity and legal effect.
- Apply governance rules (classification, retention, audit trails) when sending/receiving documents.
- Verify counterpart identity and maintain evidence of transmission and receipt.

D9. Explain the benefits of interoperable information systems for administrative data reuse (Level C)

By the end, public employees will be able to:

- Articulate how interoperability (standards, semantics, APIs) reduces duplication and speeds up services.
- Identify reuse opportunities that avoid re-collecting data from citizens and businesses.
- Communicate cost, quality, and timeliness benefits to decision-makers.

D10. Recognize mechanisms that facilitate data reuse within/across administrations (Level C)

By the end, public employees will be able to:

- Describe mechanisms such as interoperability frameworks, open-data portals, catalogues, and data-sharing agreements.
- Choose proportionate reuse routes (public open data vs. controlled inter-agency sharing) for a given case.
- Document reuse conditions and responsibilities in short data-sharing notes.

2) Proposed content topics for potential modules

1. Team workspaces and project boards (Level A) - Set up task boards, owners, and statuses; create views and lightweight automations for progress tracking.
Examples: Build a Kanban for a policy project; auto-notify assignees on status changes.
2. Shared calendars and coordination etiquette (Level A) - Align events with deliverables; use availability, holds, and meeting hygiene to reduce conflicts.
Examples: Link key milestones to calendar events; apply “documents ready 24h before” rules.
3. Collaborative document authoring (Level A) - Co-edit with comments, suggestions, and version history; run focused writing sessions.
Examples: Turn a meeting into a live drafting sprint; resolve tracked changes and publish a clean version.
4. Roles, permissions, and secure sharing (Level B) - Apply least-privilege and time-bound links; troubleshoot access problems.
Examples: Create a partner-view link that expires; audit who can edit a sensitive spreadsheet.
5. Working across institutions (case systems & portals) (Level B) - Move cases through joint workflows with standard updates and evidence.
Examples: Update a shared case record; record an inter-agency SLA breach and escalation.
6. Open formats and metadata in practice (Level B) - Choose formats and fields that make data findable and reusable.
Examples: Publish a CSV with a minimal data dictionary; add source and update cadence to a dataset.
7. Documenting workflows and playbooks (Level B) - Capture how work is done so others can reproduce outcomes.
Examples: Write a one-page SOP with inputs/outputs; add a short Loom/clip to clarify a tricky step.
8. Secure exchange channels and protocols (Level B) - Match channel to sensitivity and legal effect; maintain audit evidence.
Examples: Send a document via eDelivery; exchange a CSV via SFTP with checksum verification.
9. Interoperability essentials for non-technical staff (Level C) - Understand the “what/why” of standards, semantics, and APIs.
Examples: Explain how a shared ID reduces duplication; map a form field to a common vocabulary.
10. Data reuse mechanisms and agreements (Level C) - Navigate open data, catalogues, and controlled sharing with other authorities.
Examples: Register a dataset in the catalogue; draft a simple inter-agency data-sharing note.

11. Meeting-light collaboration (Level B) - Replace status meetings with async updates and decision logs.
Examples: Weekly written updates on the board; use a decision log template for approvals.
12. Cross-boundary incident handling (Level B) - Coordinate responses to outages or security events across institutions.
Examples: Use a shared channel for incident updates; record actions and post-incident lessons.
13. Records and retention in collaborative tools (Level B) - Keep communications and files compliant and discoverable.
Examples: Apply retention labels; move final artefacts from chat to the records library.
14. Measuring collaboration health (Level B) - Define and track simple KPIs (cycle time, WIP, on-time delivery, participation).
Examples: Add a throughput chart to the board; review blockers and rebalance workloads.
15. Onboarding and knowledge transfer (Level B) - Use checklists and “start here” pages to ramp up new team members.
Examples: Create a team handbook; link SOPs and templates in a single index.

C2.3. Ensuring digital integrity and accountability in public administration

1) Learning outcomes

D1. Apply digital etiquette and behavioral norms to ensure respectful, inclusive, purpose-oriented interaction (Level A)

By the end, public employees will be able to:

- Use plain, respectful language and inclusive formats; de-escalate and redirect inappropriate behavior online.
- Apply channel-specific netiquette (email, chats, social platforms, portals) that supports constructive dialogue.
- Recognize and mitigate exclusionary patterns (jargon, culture-specific idioms, inaccessible content).

D2. Uphold ethical principles when using digital tools and technologies in professional contexts (Level A)

By the end, public employees will be able to:

- Explain and apply fairness, non-discrimination, transparency, and accountability in everyday digital work.
- Identify ethical risks in common scenarios (profiling, targeting, automated filtering) and propose proportionate safeguards.
- Document ethical considerations and trade-offs in short decision notes.

D3. Promote ethical digital practices aligned with good governance and codes of conduct (Level B)

By the end, public employees will be able to:

- Translate codes of conduct into concrete do's/don'ts for digital communications and services.
- Set and moderate participation rules that protect dignity, safety, and equal voice.
- Close the feedback loop with transparent “you said - we did” summaries to build trust.

D4. Take accountability when AI is used in PA tasks (verification, harm checks, policy compliance) (Level B)

By the end, public employees will be able to:

- Run proportionate pre-use checks (task suitability, data sensitivity) and post-use validations (factual accuracy, policy conformance).

- Request and record sources/citations from AI systems and verify them against authoritative references.
- Escalate edge cases, log issues, and document residual risks.

D5. Apply human-centric AI principles: fairness, accountability, transparency, safety, privacy, diversity, information integrity, environmental sustainability (Level B)

By the end, public employees will be able to:

- Map these principles to practical controls (purpose limitation, minimization, bias checks, explainability notes, energy-aware settings).
- Conduct light-touch AI impact considerations appropriate to the context and sensitivity.
- Communicate limitations and safeguards to non-technical stakeholders.

D6. Maintain a professional digital reputation and manage the institutional digital footprint (Level B)

By the end, public employees will be able to:

- Separate personal/professional boundaries on platforms; use official profiles appropriately.
- Apply naming, archiving, and retention practices that protect both integrity and discoverability.
- Detect and remediate footprint risks (oversharing, metadata leaks, unvetted links).

D7. Ensure transparency and accountability of AI systems; scrutinize how AI shapes interpretation of data/information (Level C)

By the end, public employees will be able to:

- Request basic model/system information (purpose, training scope, update cycle) and log it in a usage note.
- Identify points where AI framing may bias interpretation; seek raw evidence and counter-examples.
- Require provenance (links, identifiers, timestamps) for AI-assisted outputs used in decisions.

D8. Identify and mitigate risks from digital misinformation and AI-specific risks (algorithmic bias, opacity) (Level C)

By the end, public employees will be able to:

- Triage claims with a quick credibility check; cross-verify with independent, authoritative sources.
- Recognize bias patterns (sampling, proxy variables) and opacity risks (“black box” effects) and apply mitigations or escalate.
- Craft proportionate public clarifications or corrections aligned with institutional policy.

2) Proposed content topics for potential modules

1. Digital etiquette and respectful online conduct (Level A) - Practical norms for tone, inclusivity, and purpose-driven conversations across channels.
Examples: Rewrite a terse email into an inclusive update; design a comment policy for a portal thread.
2. Ethical principles in day-to-day digital work (Level A) - Turn fairness, non-discrimination, transparency, accountability into routine checks.
Examples: Add a fairness check to a targeted outreach; document transparency notes on a public dashboard.
3. Codes of conduct → service rules (Level B) - Operationalize governance principles for interactions with citizens and businesses.
Examples: Draft “house rules” for online consultations; create a moderation and escalation ladder.
4. Accountability when using AI (Level B) - Human-in-the-loop review, source verification, harm screening, and policy compliance.

Examples: Verify AI-generated FAQs against legal guidance; log exceptions and corrections in a usage register.

5. Human-centric AI in practice (Level B) - Apply privacy, safety, diversity, integrity, and sustainability principles with proportionate controls.
Examples: Minimize personal data in prompts; request citations; prefer energy-efficient settings for batch tasks.
6. Professional digital reputation & footprint (Level B) - Manage profiles, content traces, and records to protect integrity and trust.
Examples: Tune privacy settings on work platforms; remove geotags from shared images; apply retention labels.
7. Transparency and explainability of AI systems (Level C) - What to ask vendors/systems, how to record provenance, how to communicate limits.
Examples: Capture model/version info in a template; annotate a brief with data lineage and timestamps.
8. Bias, opacity, and fairness basics (Level C) - Recognize algorithmic bias pathways and “black box” risks; choose mitigations.
Examples: Spot proxy variables in a risk score; require a simple fairness test or alternative rule-based fallback.
9. Misinformation resilience for PA (Level C) - Rapid credibility triage, triangulation, and proportionate public responses.
Examples: Debunk a viral claim using authoritative sources; publish a short correction with links.
10. Records, audit trails, and accountability logs (Level C) - Keep defensible evidence of decisions and AI-assisted steps.
Examples: Create a minimal decision log; attach prompts/outputs and verification notes to the record.
11. Privacy-by-design in communications and AI use (Level B) - Limit data, respect consent/expectations, and avoid unnecessary exposure.
Examples: Redact personal data before sharing; craft a privacy notice for an online form.
12. Accessibility and inclusion as integrity enablers (Level A) - Ensure everyone can participate and understand decisions.
Examples: Add captions/alt text; provide “easy-to-read” versions; plan low-bandwidth options.
13. Incident response for digital integrity breaches (Level C) - Detect, contain, notify, and learn from misconduct or AI failure.
Examples: Draft a holding statement; run a quick post-incident review capturing root causes and fixes.
14. Procurement and vendor accountability for AI/tools (Level C) - Build transparency, audit, and fairness clauses into contracts.
Examples: Require model cards or documentation; set service levels for explainability and bug-fix response.
15. Integrity KPIs and continuous improvement (Level C) - Measure and improve integrity practices across teams and services.
Examples: Track “issues found vs. corrected”; monitor time-to-correction; run quarterly integrity reviews.

A3. Digital content and digital public services

C3.1. Developing, integrating and re-using digital content

1) Learning outcomes

D1. Prepare and modify digital presentations tailored to specific audiences and administrative purposes (Level A)

By the end, public employees will be able to:

- Analyze audience needs (purpose, prior knowledge, constraints) and choose suitable presentation formats.
- Structure clear narratives with scannable slides, coherent visuals, and appropriate technical settings (aspect ratio, export).
- Apply institutional visual standards and ensure presentations are accessible and platform-ready.

D2. Tailor digital materials to different target audiences (citizens, partners, organizations) (Level A)

By the end, public employees will be able to:

- Segment audiences and adapt tone, reading level, and structure accordingly.
- Translate core content into channel-appropriate artefacts (report → summary → FAQ → social card).
- Validate that adaptations preserve accuracy and intent while improving usability.

D3. Comply with professional and institutional standards when creating/formatting content (Level A)

By the end, public employees will be able to:

- Apply official templates, branding, and style rules consistently.
- Include required elements (disclaimers, references, version/date, contact) for formal documents.
- Meet records-management expectations (naming, versioning, retention).

D4. Create and format professional content using institutional templates and text tools (Level A)

By the end, public employees will be able to:

- Use headings, styles, tables, and references to ensure clarity and structural integrity.
- Collaborate with comments/track-changes and produce clean final versions.
- Check grammar, terminology, and metadata for correctness and findability.

D5. Use AI tools ethically and safely to generate content, employing prompt-engineering techniques (Level A)

By the end, public employees will be able to:

- Craft prompts that define task, audience, sources, constraints, and output format.
- Request citations/provenance and verify outputs against authoritative sources.
- Respect privacy, security, and appropriateness when supplying inputs to AI tools.

D6. Apply institutional guidelines for using AI systems in content production (Level A)

By the end, public employees will be able to:

- Run suitability checks (what is/ isn't appropriate for AI assistance) and maintain human-in-the-loop review.
- Log prompts/outputs, decisions, and verifications for transparency and audit.
- Escalate edge cases and follow exception-handling procedures.

D7. Provide constructive feedback to help colleagues improve digital content (Level B)

By the end, public employees will be able to:

- Use structured review checklists (clarity, accuracy, accessibility, compliance).
- Offer specific, actionable feedback and examples rather than vague critiques.
- Facilitate short peer-review sessions to uplift team-wide quality.

D8. Reduce risk of biased/harmful/inaccurate AI outputs through better inputs and controls (Level B)

By the end, public employees will be able to:

- Apply prompt patterns that specify inclusivity, neutrality, and safety constraints.

- Detect bias or unsafe phrasing in outputs and iterate prompts to mitigate it.
- Document limitations and provide corrective notes where needed.

D9. Document good practices, workflows, and lessons learned in reusable formats (Level B)

By the end, public employees will be able to:

- Produce templates, checklists, and internal guides that codify repeatable processes.
- Maintain concise READMEs and “how-to” notes linked to examples and sources.
- Version and curate these artefacts to support onboarding and institutional memory.

D10. Understand official accessibility standards (e.g., WCAG 2.1, EN 301 549) (Level B)

By the end, public employees will be able to:

- Explain core principles (perceivable, operable, understandable, robust) and the relevance to PA content.
- Identify common accessibility barriers in documents and web-based artefacts.
- Use basic testing tools and checklists to detect issues.

D11. Create/adapt content to meet accessibility and interoperability standards; ensure cross-platform reuse (Level B)

By the end, public employees will be able to:

- Produce accessible files (alt text, proper headings, tagged PDFs, captions) and interoperable formats (HTML, CSV, PDF/A).
- Apply metadata and consistent vocabularies to support discoverability and reuse.
- Validate content behavior across devices and assistive technologies.

D12. Create design guidelines for complex digital materials (interactive presentations, data-driven reports) (Level C)

By the end, public employees will be able to:

- Define modular components, layouts, and style tokens that scale across audiences and channels.
- Build reusable templates and content blocks to speed up production.
- Set update cadences and ownership for living materials.

D13. Analyze and audit advanced content production that incorporates AI, ensuring ethical, responsible, transparent processes (Level C)

By the end, public employees will be able to:

- Assess workflows for risks (bias, privacy, provenance), controls, and audit trails.
- Check that AI use follows institutional policy and yields verifiable outputs.
- Produce short audit notes with recommendations and improvement actions.

2) Proposed content topics for potential modules

1. Audience analysis and content mapping (Level A) - Turn objectives and user needs into a content plan and format choices.
Examples: Convert a 20-page report into a 2-page brief + FAQ; map content to citizen vs. professional audiences.
2. Presentation design for public administration (Level A) - Build clear, accessible slide decks aligned with institutional templates.
Examples: Redesign a dense slide using hierarchy and captions; export accessible PDFs with correct tagging.
3. Professional document creation with templates (Level A) - Use styles, references, and layouts to produce compliant documents.
Examples: Apply a house style; automate a table of contents; insert standard disclaimers and citation blocks.

4. Accessibility by design (WCAG 2.1 / EN 301 549) (Level B) - Bake accessibility into documents, visuals, and web artefacts.
Examples: Add alt text and headings; fix color contrast; caption a short explainer video.
5. Interoperable formats and metadata (Level B) - Choose formats and fields that make content reusable across platforms.
Examples: Publish a CSV with a data dictionary; export PDF/A with metadata; tag content for findability.
6. Content adaptation for diverse audiences (Level A) - Reframe the same facts for citizens, businesses, or other authorities.
Examples: Transform a policy note into a citizen-friendly FAQ; create a partner briefing with actionable steps.
7. Responsible AI-assisted content creation (Level A) - Use AI to draft, summarize, or translate while preserving integrity and privacy.
Examples: Prompt for “explain and cite” outputs; verify claims against official sources; redact personal data before prompting.
8. Prompt engineering for safe and accurate outputs (Level B) - Structure inputs to reduce bias and errors; request provenance.
Examples: Add constraints and counter-examples; require links/identifiers and a confidence note in the output.
9. Reusable templates, components, and style tokens (Level C) - Build modular content that speeds production and ensures consistency.
Examples: Create a slide/brief template set; define reusable callout and data-table components.
10. Publishing workflows and version control (Level B) - Move from draft to approved artefact with traceability and retention.
Examples: Set up review steps and sign-offs; name and archive versions; publish with “last updated” labels.
11. Data-driven reports and visual storytelling (Level B) - Turn datasets into accurate, understandable narratives and visuals.
Examples: Build a one-page indicator brief; annotate charts with units, sources, and caveats.
12. Peer review and constructive feedback (Level B) - Raise quality through checklists, exemplars, and short review sprints.
Examples: Run a 15-minute content clinic; apply a “clarity–accuracy–accessibility” checklist.
13. Documenting workflows and lessons learned (Level B) - Capture processes in reusable guides and playbooks.
Examples: Write a 1-page SOP with inputs/outputs; maintain a living template library with version notes.
14. AI governance in content production (Level C) - Operationalize institutional AI rules for safe, auditable content creation.
Examples: Maintain an AI usage log; define when human review is mandatory; record sources and limitations.
15. Content quality audits and improvement cycles (Level C) - Check accessibility, compliance, provenance, and reuse readiness.
Examples: Run a quarterly content audit; fix non-compliant PDFs; measure template adoption rates.

C3.2. Delivering and contributing to digital public services

1) Learning outcomes

D1. Awareness of national digital public services (e.g., ghiseul.ro, e-guvernare.ro, Single Digital Gateway contact point) (Level A)

By the end, public employees will be able to:

- Identify the main platforms relevant to their policy/service area and explain each platform's purpose, scope, and ownership.
- Navigate core user journeys (e.g., payment, application, status tracking) and signpost escalation routes.
- Maintain a simple "service map" for their role to guide colleagues and beneficiaries.

D2. Understand digital accessibility and apply basic practices (Level A)

By the end, public employees will be able to:

- Define digital accessibility in practical terms and recognize common barriers affecting citizens and businesses.
- Apply quick checks/fixes for documents, web pages, and forms (e.g., headings, alt text, captions, contrast).
- Know when and how to escalate complex accessibility issues.

D3. Provide inclusive first-line support to access digital content (Level A)

By the end, public employees will be able to:

- Offer clear, step-by-step guidance tailored to user capabilities (plain language, phone/chat support, printed checklists).
- Recognize when tools must be adapted (low-bandwidth, mobile-first, assisted channels) and request adjustments.
- Capture frequent issues to inform service improvements.

D4. Enable confident use of digital service tools and platforms (Level A)

By the end, public employees will be able to:

- Design short onboarding materials (micro-demos, FAQs, one-page guides) for the most common user tasks.
- Run brief "show-and-do" sessions to help beneficiaries complete transactions independently.
- Measure comprehension and adapt materials based on user feedback.

D5. Collaborate in multidisciplinary service teams (Level A)

By the end, public employees will be able to:

- Participate effectively with policy, IT, legal, and front-office colleagues in scoping and iterative design.
- Translate user/operational insights into backlog items with acceptance criteria.
- Keep work aligned with institutional standards and service goals.

D6. Support secure e-identity journeys (e.g., ROeID) (Level B)

By the end, public employees will be able to:

- Explain e-ID registration, authentication, and recovery flows to users; verify identity requirements.
- Triage common access problems and escalate safely when needed.
- Promote privacy-preserving practices during support interactions.

D7. Turn beneficiary feedback into actionable improvements (Level B)

By the end, public employees will be able to:

- Collect formal and informal feedback ethically; categorize by severity, frequency, and impact.
- Prioritize and route feedback to owners; communicate "you said - we did" updates.
- Track resolution and learning for continuous improvement.

D8. Contribute to development, testing, and simplification of services (Level B)

By the end, public employees will be able to:

- Propose small, safe changes (form simplification, clearer messages, automated steps) and test them.
- Run light usability checks and record evidence supporting a change request.
- Document effects on usability, transparency, and processing time.

D9. Explore and pilot emerging service tools responsibly (e.g., chatbots, schedulers) (Level C)

By the end, public employees will be able to:

- Define a small pilot with success criteria, risk controls, and accessibility considerations.
- Collect pilot data, synthesize lessons, and recommend scale-up or pivot decisions.
- Ensure transparency about pilot status with internal and external stakeholders.

D10. Evaluate and audit new or changed digital services (Level C)

By the end, public employees will be able to:

- Apply proportionate checklists covering user needs, accessibility, security/privacy, interoperability, and alignment to strategies/standards.
- Produce concise audit notes with findings, recommended fixes, owners, and timelines.
- Re-test after fixes and log outcomes for accountability.

2) Proposed content topics for potential modules

1. National digital service landscape (Level A) - Orient staff in the ecosystem: what platforms exist, ownership, and how journeys connect.
Examples: Map a common journey on ghiseul.ro; identify hand-offs to back-office or partner systems.
2. Digital accessibility essentials (Level A) - Practical steps to make pages, files, and forms usable by everyone.
Examples: Add headings/alt text; fix contrast; caption a short video; convert a PDF form into an accessible web flow.
3. Inclusive front-line support (Level A) - Methods to guide diverse users with empathy and clarity.
Examples: Create a one-page “how to apply” guide; design a callback script for low-connectivity users.
4. Onboarding materials that work (Level A) - Build micro-demos, FAQs, and checklists that boost confidence and completion rates.
Examples: Record a 2-minute screen-walk; draft a step-by-step card for a frequent task; test comprehension with 3 users.
5. Working in multidisciplinary teams (Level A) - Collaboration patterns that translate insights into delivery.
Examples: Convert complaints into backlog items; run a joint refinement session with acceptance criteria.
6. Secure e-ID support (ROeID) (Level B) - What to explain, what to check, and when to escalate.
Examples: Walk through ROeID signup; troubleshoot MFA; provide privacy tips during in-person assistance.
7. Service simplification and plain language (Level B) - Reduce friction with clearer content and fewer fields.
Examples: Shorten a 40-field form; rewrite error messages; measure time-to-complete before/after.
8. Light-touch automation and templates (Level B) - Identify repetitive steps and introduce safe, auditable automation.
Examples: Auto-route requests; set SLAs and alerts; create reusable reply and evidence templates.

9. Feedback loops and “you said - we did” (Level B) - Close the loop to build trust and legitimacy.
Examples: Launch a post-transaction micro-survey; synthesize themes; publish monthly changes with plain-language notes.
10. Piloting emerging tools (Level C) - Structure small experiments with clear criteria and guardrails.
Examples: Pilot a chatbot for one service; define accuracy and escalation KPIs; run an accessibility check on the pilot.
11. Readiness checks and mini-audits (Level C) - Ensure quality, accessibility, and compliance before and after release.
Examples: Use a 1-page checklist; log issues/owners/due dates; re-test and record outcomes.
12. Inter-institutional coordination for once-only services (Level B) - Handoffs, SLAs, and information sharing that make journeys seamless.
Examples: Draft a simple inter-agency handoff protocol; define a status code list that two teams share.
13. Communications through the service lifecycle (Level B) - Inform users with timely, understandable messages.
Examples: Write notification emails/SMS in plain language; design a maintenance banner; create a short “how-to” video.
14. Incident handling and continuity (Level B) - Prepare for outages and security events with roles, scripts, and evidence logs.
Examples: Table-top an outage scenario; publish a status update; document a blameless post-mortem and fixes.

C3.3. Ensuring compliance with digital regulatory frameworks and standards

1) Learning outcomes

D1. Copyright and licensing for digital products (software, audiovisual, other) (Level A)

By the end, public employees will be able to:

- Recognize that software, audiovisual works, datasets, and documents may be copyrighted and require appropriate licenses for public-sector use.
- Identify permitted uses (use, share, adapt) under common licenses (proprietary, open-source, Creative Commons) and apply institutional rules before deployment or publication.
- Record license terms in a simple compliance note (rights holder, license type, scope, attribution needs).

D2. Legally valid electronic submissions to PA (Level A)

By the end, public employees will be able to:

- Describe the legally recognized methods for valid electronic submission of applications/declarations to PA bodies (e.g., designated portals, qualified e-signatures, registered electronic delivery).
- Advise citizens/businesses on admissible channels and required evidences (timestamps, receipts, identity proofs).
- Maintain auditable logs of received submissions consistent with institutional procedures.

D3. Core legal requirements for data protection, security, IP, licensing, and responsible digital/AI use (Level A)

By the end, public employees will be able to:

- Explain in plain language the basics of data protection, information security controls, intellectual property and licensing obligations, and responsible use of digital technologies - including generative AI.
- Apply proportionate safeguards (purpose limitation, minimization, access control, encryption, logging) in routine work.
- Escalate edge cases and document decisions and justifications.

D4. EU data-subject rights (access, rectification, erasure/Right to be Forgotten) (Level B)

By the end, public employees will be able to:

- Explain these rights to citizens and describe institutional procedures to handle requests.
- Verify identity, route requests to the right owner, respect deadlines, and document outcomes.
- Communicate lawful limits/exemptions where applicable.

D5. Support institutional compliance in one's area (procurement, documentation, audit trails) (Level B)

By the end, public employees will be able to:

- Follow internal procedures that demonstrate compliance (checklists for digital procurement, template decision notes, audit logs).
- Keep traceable records (versions, approvals, change history) aligned with retention policies.
- Contribute evidence for internal/external audits.

D6. e-Government developments and implications (EU digital identity and wallet) (Level B)

By the end, public employees will be able to:

- Summarize key EU e-Government developments (Digital Identity Regulation, European Digital Identity Wallet) and national implications for service delivery and user journeys.
- Identify organizational changes and capability needs resulting from these initiatives.
- Communicate practical impacts to colleagues and beneficiaries.

D7. Guidance on the main elements of the digital regulatory framework and initiatives (Level C)

By the end, public employees will be able to:

- Describe core principles and obligations of: Cybersecurity standards (aligned with the National Cybersecurity Strategy), Data governance & interoperability (Law 242/2022, PNI platform), Government Cloud & data protection, Digital Identity Systems (ROeID), and AI-enabled decision-making (National AI Strategy 2024–2027).
- Translate these into proportionate actions/checks for their projects (security baselines, interoperability requirements, cloud data-classification, identity assurance, human-in-the-loop for AI).

D8. Laws governing data and data management (incl. Interoperability Act) (Level C)

By the end, public employees will be able to:

- Identify relevant legal principles for data creation, sharing, reuse, quality, and interoperability - especially those stemming from the Interoperability Act.
- Apply mandatory metadata/classification and once-only/reuse principles where applicable.
- Document data-sharing conditions and responsibilities.

D9. Review and assess major EU digital acts for relevance to PA tasks (Level C)

By the end, public employees will be able to:

- Summarize the scope and key provisions of GDPR, Data Act, Data Governance Act, Digital Services Act, and relevant parts of the AI Act.
- Assess implications and potential relevance to a specific task/service (e.g., lawful basis, role as controller/processor, access/portability, content governance, AI risk category).
- Produce short, actionable compliance notes with recommended controls and owners.

2) Proposed content topics for potential modules

1. Copyright and licensing in practice (Level A) - How to recognize protected content and choose/apply the correct license in PA.
Examples: Check a software/library license before deployment; attribute a CC-BY source in a public report.
2. Legally valid e-submissions (Level A) - Channels, signatures, receipts, and evidence to make applications/declarations admissible.
Examples: Configure a portal intake with qualified e-signature; verify a registered e-delivery receipt.
3. Data protection and security basics (Level A) - Proportionate safeguards for everyday processing and sharing.
Examples: Apply minimization to a form; set role-based access; log a disclosure with lawful basis and retention.
4. Handling data-subject rights (Level B) - Operational steps from intake to closure for access/rectification/erasure.
Examples: Triage a Right to be Forgotten request; draft a plain-language response within statutory timelines.
5. Compliance evidence and audit trails (Level B) - Build lightweight, durable documentation for decisions and procurements.
Examples: Write a one-page procurement compliance note; attach approvals and version history to a change request.
6. EU e-Government changes on the horizon (Level B) - What the Digital Identity Regulation and EU Wallet mean for services.
Examples: Map a future e-ID login flow; list capability gaps for front-office support.
7. Cybersecurity standards for non-specialists (Level B) - Security baselines linked to the National Cybersecurity Strategy.
Examples: Apply MFA, backups, vulnerability patch cadence; document incident escalation routes.
8. Data governance & interoperability (Law 242/2022 / PNI) (Level C) - Policies and practical steps for cross-agency data flows.
Examples: Add mandatory metadata to a dataset; draft a minimal data-sharing note referencing the PNI platform.
9. Government Cloud and data protection (Level C) - Classification, residency, and controls when using the Government Cloud.
Examples: Classify a dataset before cloud upload; set encryption/retention; record a DPIA trigger check.
10. Digital identity systems (ROeID) in service journeys (Level B) - Assurance levels, onboarding, recovery, and support.
Examples: Explain identity proofing steps; handle a recovery case; log evidence for an audit.
11. Responsible AI in PA (National AI Strategy 2024–2027) (Level C) - Guardrails, human oversight, and documentation.
Examples: Record prompts/outputs and verifications; define human-in-the-loop points; add a provenance note to a brief.
12. EU digital acts overview for practitioners (Level C) - GDPR, Data Act, DGA, DSA, AI Act: scopes, roles, and red flags.
Examples: Determine controller vs. processor; identify a DSA content-moderation duty; place an AI use case into a risk category.

13. Templates and checklists for compliance (Level B) - Reusable, proportionate tools to operationalize the framework.
Examples: Data-sharing template with roles/metadata; compliance checklist for launching a new digital form.
14. Case clinics (role-specific scenarios) (Level C) - Apply the above to realistic tasks in services, data flows, and communications.
Examples: Review a new online application flow for legal admissibility; assess a data-integration project for interoperability and privacy.

A4. Safe, responsible and sustainable use of resources

C4.1. Protecting devices and infrastructure

1) Learning outcomes

D1. Generate and periodically change secure credentials; use multi-factor authentication (MFA) (Level A)

By the end, public employees will be able to:

- Create strong passwords/passphrases and rotate them on an institutional cadence; enable MFA on all supported systems.
- Recognize that as attack techniques evolve, defensive behaviors must adapt; apply updated guidance without delay.
- Store and share secrets safely (e.g., approved password managers, no plaintext sharing).

D2. Understand one's role in institutional safety protocols (Level A)

By the end, public employees will be able to:

- Describe how everyday actions (screen lock, clean desk, secure printing, careful sharing) reduce organizational risk.
- Follow escalation paths (who to notify, how, and what evidence to record) when a policy or control fails.
- Contribute to culture: flag unsafe practices and propose improvements respectfully.

D3. Apply institutional safety protocols and preventive measures on devices and infrastructure (Level A)

By the end, public employees will be able to:

- Keep systems updated; verify antivirus/EDR status; apply encryption and device-lock settings as required.
- Use only authorized software, networks, and storage; recognize and report policy exceptions.
- Perform basic self-checks (patch level, last scan, backup status) and request IT support when gaps are found.

D4. Stay informed about evolving cyber risks (phishing, spoofing, malware, ransomware) (Level B)

By the end, public employees will be able to:

- Detect common attack signals in email, chat, web, and mobile; handle suspected messages safely (do-not-click, report).
- Distinguish between urgent-but-legitimate and socially engineered requests; verify via trusted channels.
- Summarize recent threat trends in simple briefings for colleagues.

D5. Implement secure data handling in PA tasks, in collaboration with IT (Level B)

By the end, public employees will be able to:

- Classify working data; apply minimum necessary access, secure transfer, and safe storage/archiving.
- Use approved channels for sharing; redact or anonymize when appropriate; maintain audit trails.
- Seek timely IT guidance for higher-risk processing, documenting decisions and controls.

D6. Describe cybercrime categories and relevant legislation/standards (Level C)

By the end, public employees will be able to:

- Define common cybercrimes (unauthorized access, data theft, fraud, extortion) and their indicators.
- Outline key legal/strategic instruments (EU Cybersecurity Act, Cyber Solidarity Act, NIS framework) and institutional implications.
- Route potential incidents appropriately (report, preserve evidence, avoid contamination).

D7. Apply Romania's Cyber Security Strategy (2022–2027) policies in daily work; collaborate with DNSC (Level C)

By the end, public employees will be able to:

- Align device/media handling with strategy-aligned policies (access verification, least privilege, removable-media control).
- Follow incident reporting and response practices; cooperate with DNSC guidance where applicable.
- Evidence compliance (checklists, logs, confirmations) for internal/external oversight.

2) Proposed content topics for potential modules

1. Stronger passwords & MFA in practice (Level A) - Everyday methods to create, rotate, and manage credentials; when and how to use approved password managers and MFA.
Examples: Turn weak passwords into passphrases; enable MFA on email/VPN; store secrets in an approved vault.
2. Your role in institutional security (Level A) - Translate policies into routines that reduce risk (screen lock, secure printing, clean desk, verified sharing).
Examples: Set auto-lock to 5 minutes; configure secure print; replace ad-hoc shares with permissioned links.
3. Device hardening and safe configuration (Level A) - Updates, antivirus/EDR, encryption, backups; what to check and how to fix gaps.
Examples: Verify patch level; confirm disk encryption; check last backup and run a test restore.
4. Phishing and social engineering defense (Level B) - Recognize lures and spoofing; report safely; verify out-of-band.
Examples: Analyze a suspicious email without clicking; use a validation script; submit an abuse report.
5. Secure data handling for PA workflows (Level B) - Classify, minimize, protect, and track data through its lifecycle; collaborate effectively with IT.
Examples: Share a file via the approved platform with expiring access; redact personal data before transfer; log the share.
6. Cybercrime & the legal landscape (Level C) - What categories exist and why they matter for non-technical staff.
Examples: Identify a suspected ransomware pattern; record evidence; reference the applicable EU acts when reporting.
7. Romania's Cyber Security Strategy in daily work (Level C) - Convert strategic principles into practical controls and evidence.

Examples: Implement removable-media restrictions; complete an incident report using the institutional template; note DNSC contact points.

8. Secure collaboration and remote work (Level B) - Safe Wi-Fi, VPN, approved devices, and handling of removable media while mobile.

Examples: Switch from public Wi-Fi to hotspot + VPN; encrypt a USB key; avoid personal cloud for official files.

9. Incident response essentials (Level B) - Recognize, contain, report, and learn from security events; keep evidence and timelines.

Examples: Isolate an infected laptop; notify the helpdesk/DNSC; write a short post-incident note with lessons learned.

10. Security awareness refreshers (Level B) - Staying current with threats and evolving best practices; building a feedback culture.

Examples: Run a monthly micro-quiz; post “you said - we did” updates after awareness campaigns; update a quick reference guide.

C4.2. Managing digital identities, and protecting personal data and privacy

1) Learning outcomes

D1. Understand “digital identity” (authentication + personal data trail) (Level A)

By the end, public employees will be able to:

- Define digital identity both as a way to authenticate users and as an aggregate of data about an individual created across systems.
- Distinguish identifiers, credentials, and attributes, and explain how they are combined during identity proofing and access.
- Describe risks of linkability and over-collection, and state simple mitigations (purpose limitation, data minimization).

D2. Know that PA uses e-signatures; understand pros/cons (Level A)

By the end, public employees will be able to:

- Explain levels/types of electronic signatures used in PA and when each is appropriate.
- Describe advantages (speed, integrity, non-repudiation) and limits/risks (wrong certificate, expired keys, poor process).
- Follow institutional policies for validating signatures and archiving signed records.

D3. Safeguard one’s own personal data and workplace information in digital environments (Level A)

By the end, public employees will be able to:

- Apply baseline protections (strong authentication, least privilege, secure sharing, secure devices) in daily work.
- Recognize common disclosure risks (screenshots, misaddressed email, public links) and prevent them.
- Log what was shared, with whom, and on what legal basis.

D4. Use digital authentication services for PA staff; execute e-sign workflows (Level A)

By the end, public employees will be able to:

- Authenticate with the official employee identity solution and access connected services according to role.
- Execute end-to-end e-sign workflows (prepare, sign, verify, file) and resolve frequent errors.
- Document the identity assurance level and evidence trail for audits.

D5. Configure privacy controls on devices and cloud services (Level B)

By the end, public employees will be able to:

- Set privacy/security options on work devices and cloud apps (permissions, location/camera/mic controls, sharing scopes).
- Choose appropriate default settings (private by default; time-bound access) and review them periodically.
- Explain residual risks and when to request IT hardening.

D6. Apply privacy principles and data minimization (Level B)

By the end, public employees will be able to:

- Identify the minimum personal data needed for a task and avoid collecting or keeping more than necessary.
- Separate identification data from content data where feasible; prefer pseudonymized views for routine analysis.
- Record the purpose, lawful basis, and retention rule for each data use.

D7. Explain how citizens use eID to access digital public services (e.g., ROeID) (Level B)

By the end, public employees will be able to:

- Describe the eID journey (enrolment → authentication → authorization) and levels of assurance.
- Support users in resolving common eID issues and signpost to official help.
- Communicate privacy and security implications in plain language.

D8. Use and share personally identifiable information (PII) lawfully inside PA (Level B)

By the end, public employees will be able to:

- Apply rights-based, need-to-know access; use approved channels for transfers; maintain provenance and access logs.
- Choose proportionate safeguards (encryption, redaction, role-based access, secure portals) for internal and inter-institutional sharing.
- Draft a short sharing note indicating purpose, roles, legal basis, and retention/erasure conditions.

D9. Conduct proportionate privacy risk assessments to protect sensitive data (GDPR-aligned) (Level C)

By the end, public employees will be able to:

- Perform a light privacy risk check (data categories, purposes, recipients, risks, controls); trigger a DPIA when criteria are met.
- Identify typical risks (re-identification, function creep, excessive retention) and propose mitigations.
- Record outcomes, owners, and review dates in a simple register.

D10. Recognize how user data can be combined for profiling; understand safeguards (Level C)

By the end, public employees will be able to:

- Describe how personal, behavioral, and contextual data may be combined to create profiles or predictions.
- Identify high-risk uses (eligibility, benefits allocation, sensitive inferences) and apply stronger checks (purpose limits, human oversight, transparency).
- Communicate clearly with citizens about profiling where applicable and document opt-outs or legal bases.

2) Proposed content topics for potential modules

1. Digital identity fundamentals (Level A) - Clarify identifiers, credentials, attributes, and assurance levels; separate authentication from authorization.

Examples: Map a staff login flow; list attributes released to an internal app and why.

2. e-Signatures in public administration (Level A) - When to use each signature level; validation steps; record-keeping and expiry handling.
Examples: Verify a signature certificate; file a signed decision with proper metadata.
3. Personal data hygiene for staff (Level A) - Practical routines to prevent accidental disclosure in daily tools.
Examples: Replace public links with permissioned shares; scrub personal data from screenshots before sending.
4. Employee authentication & access management (Level A) - Using the institutional identity service and adhering to least-privilege.
Examples: Request role-based access; document an access change with approval trail.
5. Privacy settings on devices and cloud apps (Level B) - Configure defaults that reduce exposure; periodic reviews.
Examples: Disable unnecessary app permissions; set link sharing to “organization-only, expires in 14 days.”
6. Data minimization in practice (Level B) - Collect only what’s needed; reduce granularity; define retention and deletion.
Examples: Redesign a form to remove non-essential fields; set an auto-purge rule for temporary files.
7. Citizen eID journeys (ROeID) (Level B) - Support, escalation, and plain-language guidance for enrolment and login.
Examples: Create a one-page ROeID guide; troubleshoot a two-factor issue and log steps taken.
8. Lawful use and sharing of PII inside PA (Level B) - Rights-based access, secure transfer, logging, and accountability.
Examples: Draft a short data-sharing note (purpose, basis, recipients, retention); send a file via a secure portal with audit trail.
9. Privacy risk assessment (DPIA-lite) (Level C) - Rapid screening, risk identification, mitigations, and triggers for full DPIA.
Examples: Run a DPIA-lite for a new survey; document risks (re-identification) and mitigations (aggregation, shorter retention).
10. Profiling and high-risk processing (Level C) - What counts as profiling; safeguards; transparency to citizens.
Examples: Assess a proposed eligibility scoring; add human-in-the-loop and explanation notes.
11. De-identification and pseudonymization (Level B) - Techniques, limits, and when anonymization is (not) feasible.
Examples: Replace IDs with tokens for analysis; keep the key separately with restricted access.
12. Consent, transparency, and notices (Level B) - Write clear privacy notices; manage expectations; handle withdrawals.
Examples: Draft a plain-language notice for a public form; process a consent withdrawal and reflect it in systems.
13. Third-party processors and data-sharing agreements (Level B) - Roles, responsibilities, and minimum clauses.
Examples: Review a processor agreement for security and deletion obligations; set up a controlled data exchange.
14. Breach response and lessons learned (Level B) - Detect, contain, notify, and improve.
Examples: Run a tabletop for an email mis-send; issue a proportionate notification; record corrective actions.
15. Records management for identity and privacy artefacts (Level B) - Keep defensible evidence of decisions and access.

Examples: Maintain an access log; file e-sign verification proofs; record DPIA-lite outcomes with owners and dates.

C4.3. Promoting healthy and sustainable digital practices

1) Learning outcomes

D1. Energy-efficient use of digital devices at work (Level A)

By the end, public employees will be able to:

- Explain where energy is consumed across devices, networks, and cloud services, and identify high-impact reduction actions.
- Configure power settings, automatic sleep, and adaptive performance; schedule heavy tasks during off-peak times when appropriate.
- Track simple metrics (e.g., idle time, unnecessary file sync) and report improvements for their team.

D2. Recognize wellbeing risks from digital technology use (posture, sleep, techno-stress, digital dependency, online harms) (Level A)

By the end, public employees will be able to:

- Identify signs of strain (poor ergonomics, fatigue, sleep disruption), techno-stress, and early indicators of harmful dependency.
- Apply micro-habits (20-20-20 eye rule, movement breaks, notification hygiene, night-mode/blue-light controls) and escalate when support is needed.
- Promote respectful online behavior to reduce exposure to cyberbullying and grooming risks.

D3. Identify and act upon cyberbullying or internet fraud in the institution (Level B)

By the end, public employees will be able to:

- Recognize behavioral and technical red flags of workplace cyberbullying, harassment, scams, and fraud.
- Follow safe response steps: preserve evidence, avoid retaliation, report via defined channels, and request support.
- Contribute to prevention through clear community guidelines and bystander-intervention techniques.

D4. Promote responsible, future-oriented attitudes to digital resources (devices, AI systems, platforms) (Level B)

By the end, public employees will be able to:

- Articulate how ethics, public value, and sustainability shape choices about tools and practices (e.g., AI usage, cloud storage, devices).
- Model proportionate, purpose-limited use and encourage colleagues to adopt low-impact, high-value behaviors.
- Document trade-offs and rationale in short “why this tool” notes.

D5. Contribute to a respectful, inclusive digital work culture that supports diverse needs (Level B)

By the end, public employees will be able to:

- Apply inclusive communication norms (plain language, accessible formats, considerate timing) and champion reasonable accommodations.
- Detect exclusionary patterns (meeting-only culture, synchronous overload) and propose inclusive alternatives.
- Facilitate equitable access to tools and support for all staff and service users.

D6. Apply sustainable digital practices considering environmental impacts (energy, device lifecycle, data storage) (Level B)

By the end, public employees will be able to:

- Reduce footprint by extending device life, repairing over replacing, and right-sizing data storage/retention.
- Prefer low-bandwidth formats where fit-for-purpose and prune redundant data to cut storage and transmission loads.
- Include environmental considerations in procurement and project proposals.

D7. Assess and audit digital-tool usage to support socially and environmentally responsible behavior in PA (Level C)

By the end, public employees will be able to:

- Use short checklists to review tools/workflows for wellbeing, inclusion, safety, and sustainability impacts.
- Log issues, owners, and improvements; share “you said - we did” updates to close the feedback loop.
- Recommend proportionate mitigations (e.g., moderation settings, privacy-by-default, energy-aware configurations).

D8. Assess and audit institutional practices related to health, wellbeing, and inclusion in digital environments (Level C)

By the end, public employees will be able to:

- Conduct light-touch audits (policies, onboarding, workspace setup, meeting norms) and identify gaps.
- Prioritize actions, propose indicators (e.g., meeting load, async uptake, accessibility conformance), and track progress.
- Advocate for continuous improvement and governance alignment.

2) Proposed content topics for potential modules

1. Energy-smart computing at work (Level A) - Practical ways to cut energy use in devices, networks, and cloud without hurting productivity.
Examples: Set power profiles and auto-sleep; stop unneeded background sync; schedule large downloads off-peak.
2. Ergonomics and micro-habits for digital wellbeing (Level A) - Evidence-based posture, movement, and screen-time routines that reduce strain.
Examples: Apply the 20-20-20 rule; configure an ergonomic desk; use focus modes to prevent overload.
3. Techno-stress and digital dependency (Level B) - Recognize triggers and set organizational guardrails to keep work healthy.
Examples: Redesign notification settings; introduce “quiet hours”; offer a support pathway for early dependency signs.
4. Preventing and responding to cyberbullying & fraud (Level B) - Policies, signals, safe responses, and supportive reporting.
Examples: Draft a short code of conduct; create a bystander-intervention flow; preserve evidence and escalate safely.
5. Responsible use of AI and digital platforms (Level B) - Align everyday choices with ethics, public value, and sustainability.
Examples: Choose low-impact formats; request citations and run verifications for AI outputs; log rationale for tool choices.
6. Inclusive-by-design digital culture (Level B) - Communication and collaboration patterns that include diverse needs.

Examples: Convert meetings to async updates when possible; provide accessible materials; use inclusive language templates.

7. Sustainable data practices (Level B) - Reduce storage/transmission waste and extend device lifecycles.

Examples: Archive or delete redundant files; compress media; plan procurement with repairability criteria.

8. Healthy collaboration rhythms (Level B) - Balance synchronous/asynchronous work to lower stress and increase equity.

Examples: Weekly written updates instead of daily status calls; shared decision logs; rotating meeting times.

9. Digital safety for staff and citizens (Level B) - Build safer spaces through moderation, privacy-by-default, and clear norms.

Examples: Enable comment moderation on portals; default links to “organization-only” with expiry; publish a “how we keep you safe” page.

10. Green ICT quick wins (Level B) - Simple configuration and procurement choices with measurable impact.

Examples: Prefer energy-efficient settings; extend device replacement cycles; choose refurb options where feasible.

11. Audit checklists for wellbeing & sustainability (Level C) - Lightweight tools to review teams, tools, and workflows.

Examples: Run a monthly wellbeing/sustainability scan; log actions, owners, and due dates; report “you said - we did.”

12. Ethical digital citizenship in PA (Level B) - Model respectful, future-oriented behavior in public interactions.

Examples: Write an inclusive comment policy; publish transparent updates on improvements prompted by feedback.

13. Measuring impact: people, planet, performance (Level C) - Choose indicators and feedback loops for continuous improvement.

Examples: Track meeting hours, async adoption, storage trimmed, and device lifetime; share quarterly dashboards.

A5. Problem-solving through digital tools

C5.1. Managing digital devices, including identifying and managing technical problems

1) Learning outcomes

D1. Use institutional devices, environments, and core applications safely and confidently (Level A)

By the end, public employees will be able to:

- Start, configure, and operate workstations, printers, and core apps (DMS, e-archive, workflow/case tools, service portals) following institutional policies.
- Apply basic security and hygiene (screen lock, secure printing, approved storage/sharing) during routine tasks.

D2. Telework autonomously using institutional tools (Level A)

By the end, public employees will be able to:

- Connect remotely using approved solutions (VPN/VDI, MFA), access shared resources, and keep records compliant.
- Set up a productive remote workspace (bandwidth checks, audio/video, peripherals) and follow continuity procedures.

D3. Understand basic operating logic of devices, tools, and infrastructure to resolve routine issues (Level A)

By the end, public employees will be able to:

- Explain fundamental concepts (OS, drivers, network, permissions, storage) and how they interact in PA systems.
- Use this mental model to perform first-line checks before escalating (restart sequence, cable/Wi-Fi check, account status).

D4. Diagnose simple technical problems (login, connectivity, file compatibility) (Level A)

By the end, public employees will be able to:

- Triage common issues with structured questions and reproduce errors safely.
- Run standard fixes (password/MFA reset path, network adapter reset, file conversion/open-with alternatives) and verify resolution.

D5. Identify and apply appropriate alternatives when technology limits block work (Level B)

By the end, public employees will be able to:

- Choose proportionate workarounds (alternate apps, web versions, mobile scan/upload, different file formats) that respect policy.
- Document temporary fixes and revert to canonical tools when the limitation is removed.

D6. Proactively apply standard procedures to resolve frequent HW/SW issues (Level B)

By the end, public employees will be able to:

- Use institutional playbooks/knowledge base to run scripted steps (updates, cache clear, profile repair, printer reset).
- Keep a minimal log of actions taken and outcomes for accountability.

D7. Document and report complex incidents effectively to IT/helpdesk (Level B)

By the end, public employees will be able to:

- Prepare high-quality tickets (context, exact steps, screenshots, error codes, urgency/impact) and attach relevant logs.
- Follow up professionally, test proposed fixes, and confirm closure in the tracking system.

D8. Analyze complex situations and create step-by-step user guidance (incl. video tutorials) (Level C)

By the end, public employees will be able to:

- Facilitate remote or on-site troubleshooting with colleagues, capture the solution path, and convert it into clear guidance.
- Produce short, accessible how-to artefacts (one-pagers, clips) and keep them versioned.

D9. Coordinate with specialists to restore operations and ensure continuity (Level C)

By the end, public employees will be able to:

- Communicate impact, dependencies, and priorities; align on workarounds and maintenance windows.
- Verify that essential services are restored and lessons learned are recorded in the team's playbook.

2) Proposed content topics for potential modules

1. Getting started with institutional devices and core apps (Level A) - Essential setup and safe daily use of workstations, printers, DMS, and service platforms.

Examples: Configure a new laptop; add a secure printer; check out/in a file in the DMS.

2. Remote work that just works (Level A) - Reliable telework setup with VPN/VDI, MFA, and smooth audio/video.
Examples: Run a bandwidth test and fix jitter; enroll a second factor; mount a network drive remotely.
3. How your device actually works (for non-engineers) (Level A) - A simple mental model of OS, drivers, network, and storage to guide first-aid fixes.
Examples: Diagnose a driver issue after an update; free space and repair a user profile.
4. Login, network, and file-compatibility triage (Level A) - Step-by-step checks for the top three user blockers.
Examples: Resolve an MFA lockout; reset a network adapter/DNS; convert a .odt/.pages to .docx or PDF.
5. Workarounds without cutting corners (Level B) - Choosing compliant alternatives when tools fail.
Examples: Scan with a mobile app and upload to DMS; switch from desktop to web version; export to an interoperable format.
6. Self-service fixes with institutional playbooks (Level B) - Using KB articles and scripts safely and documenting outcomes.
Examples: Clear cache to fix portal errors; reinstall a printer; run OS update and reboot sequence.
7. Writing the perfect helpdesk ticket (Level B) - What IT needs to solve your issue fast.
Examples: Attach reproducible steps and screenshots; include error IDs; state business impact and deadlines.
8. From fix to guide: creating reusable help (Level C) - Turn solved problems into short SOPs and 2-minute videos.
Examples: Record a screenwalk on mapping a drive; publish a one-pager on secure printing setup.
9. Coordinating incidents and continuity (Level C) - Communicating with specialists, agreeing on workarounds, and closing the loop.
Examples: Run a mini-post-incident review; document temporary measures; verify service restoration.
10. Peripheral (and printer) essentials (Level B) - Common setup and troubleshooting patterns for scanners, docks, and printers.
Examples: Fix a stuck print queue; reinstall a driver; configure a scanner-to-email workflow.
11. Safe data handling while troubleshooting (Level B) - Keep privacy and security intact during fixes and file transfers.
Examples: Redact screenshots before tickets; use approved channels for log sharing; remove temporary data after resolution.
12. Monitoring the basics (Level B) - Simple self-checks that prevent downtime.
Examples: Verify patch/AV status; check disk health and backups; set alerts for low storage.

C5.2. Using automation tools

1) Learning outcomes

D1. Identify repetitive digital tasks that can be streamlined with simple automation (Level A)

By the end, public employees will be able to:

- Scan daily workflows to spot repetitive, rule-based steps (routing emails, renaming files, populating templates) suitable for automation.

- Prioritize opportunities using a quick matrix (frequency × effort × risk) and document the current vs. automated flow.

D2. Follow basic instructions to automate simple tasks (Level A)

By the end, public employees will be able to:

- Configure entry-level automations (email rules, calendar/meeting automations, form/document templates, folder rules, basic “if-this-then-that” flows) using approved tools.
- Test, enable, disable, and safely roll back automations; record changes and ownership.

D3. Decompose problems and choose suitable entry points for solutions (Level A)

By the end, public employees will be able to:

- Break a problem into sub-tasks, identify data inputs/outputs, and map decision points that lend themselves to automation.
- Choose a lowest-risk starting point (e.g., notifications, data validation, file movement) before attempting end-to-end flows.

D4. Take initiative to simplify procedures and improve service quality using available tech or small pilots (Level B)

By the end, public employees will be able to:

- Propose small, safe changes (template packs, shared checklists, auto-routing) that reduce manual effort and error.
- Plan a lightweight pilot with success criteria, stakeholder sign-off, and a rollback plan; communicate “you said - we did.”

D5. Explain the steps of computational thinking and apply them to PA tasks (Level B)

By the end, public employees will be able to:

- Describe problem decomposition, pattern recognition, abstraction, and algorithmic thinking in plain language.
- Apply these steps to design a simple rule set or flow for a routine public-administration task.

D6. Evaluate office automations in complex tasks for responsible use (Level C)

By the end, public employees will be able to:

- Assess data accuracy, transparency (log of steps, who/what/when), and compliance (access, retention, auditability) before enabling automations that touch sensitive data or multi-actor workflows.
- Document controls and risks in a short automation note; schedule periodic reviews.

D7. Represent and interpret simple symbolic sequences (Level C)

By the end, public employees will be able to:

- Sketch a simple flow (symbols or pseudo-code) that others can implement; interpret colleagues’ flows to execute or improve them.
- Translate a symbolic sequence into a working rule/automation using institutional tools.

2) Proposed content topics for potential modules

1. Spotting automation opportunities (Level A) - Techniques to identify repetitive, rule-based steps and rank them by impact and risk.
Examples: Map an email triage routine and convert it into rules; list five “copy-paste” tasks to template.
2. Quick wins with everyday tools (Level A) - Configure email filters, calendar automations, and document/form templates to remove busywork.
Examples: Auto-file messages by case ID; generate a pre-filled response letter from a template.
3. Problem decomposition for non-coders (Level A) - Break a process into inputs, decisions, and outputs; pick safe starting points.

Examples: Decompose a permit intake into sub-flows; automate just the acknowledgment email first.

4. Computational thinking in practice (Level B) - Apply pattern recognition, abstraction, and algorithmic steps to real PA tasks.

Examples: Generalize three similar approval flows into one rule set; write pseudo-code for a file-naming routine.

5. Designing simple flows (no-/low-code) (Level B) - Build “if-this-then-that” automations with triggers, conditions, and actions; test and roll back safely.

Examples: When a form is submitted, validate fields, save to the DMS, and notify the case owner.

6. Templates, checklists, and data validation (Level B) - Standardize inputs to reduce errors and speed reviews.

Examples: Add dropdown validation to a spreadsheet; create a checklist that gates submission quality.

7. Responsible automation: accuracy, transparency, compliance (Level C) - Build logs, approvals, and safeguards into your flow.

Examples: Record every automated rename/move; restrict access on automated shares; schedule a quarterly review.

8. From idea to pilot (Level B) - Plan a small experiment with success metrics, stakeholders, and rollback; communicate outcomes.

Examples: Pilot auto-routing of citizen requests; compare turnaround time and error rate before/after.

9. Reading and drawing simple flowcharts (Level C) - Use common symbols to express and understand processes across teams.

Examples: Convert a written SOP into a flowchart; implement a colleague’s diagram as an email rule set.

10. Scaling what works (Level B) - Turn pilots into reusable assets (templates, shared flows, SOPs) and maintain them.

Examples: Publish a “starter pack” of rules/templates; create a change log and ownership table.

A6. Digital transformation in public administration

C6.1. Contributing to digital transformation in public administration, driving innovation and improvement

1) Learning outcomes

D1. Understand key drivers of digital transformation in one’s PA field (Level A)

By the end, public employees will be able to:

- List and explain major drivers (user expectations, legislation/standards, data availability, interoperability, cost/efficiency, security, inclusion).
- Map drivers to concrete opportunities/constraints in their unit and articulate expected public value.

D2. Distinguish tasks suited to digital tools versus human judgement (Level A)

By the end, public employees will be able to:

- Classify work items as “automate/augment/keep human-led” using risk, complexity, and empathy criteria.

- Justify choices with examples (e.g., auto-routing vs. discretionary case assessments) and define oversight points.

D3. Identify innovation initiatives using digital/emerging tech in their domain (Level A)

By the end, public employees will be able to:

- Scan their ecosystem to surface relevant initiatives (chatbots, once-only data exchange, open data reuse, e-ID journeys).
- Summarize objectives, enablers, risks, and lessons learned in short briefs.

D4. Support leadership and new managerial practices that enable transformation (Level A)

By the end, public employees will be able to:

- Describe how procurement, budgeting, and governance can encourage iterative, user-centred delivery.
- Provide concise evidence notes that help leaders sequence investments and manage risk.

D5. Engage with and support implementation of digital initiatives in one's area (Level B)

By the end, public employees will be able to:

- Translate user pain points into backlog items; contribute to service redesign, workflow automation, and data improvements.
- Track benefits (time-to-complete, errors reduced, satisfaction) and communicate "you said - we did."

D6. Shape the enabling environment for transformation (Level B)

By the end, public employees will be able to:

- Propose conditions that foster change (clear ownership, standards/templates, sandboxing, skills, openness).
- Draft lightweight operating principles for cross-unit collaboration and evidence-sharing.

D7. Use horizon scanning and outward-looking approaches around the policy cycle (Level C)

By the end, public employees will be able to:

- Run simple horizon-scanning routines (signals, trends, drivers) and relate them to policy planning, design, implementation, and evaluation.
- Produce periodic scanning notes that feed roadmaps and risk registers.

D8. Track disruptive developments to inform capacity and workforce planning (Level C)

By the end, public employees will be able to:

- Maintain a skim-level view of key technology shifts and their implications for roles, skills, and org design.
- Recommend proportionate upskilling/reskilling actions for their team.

D9. Apply iteration, rapid feedback, pilots, and incremental development (Level C)

By the end, public employees will be able to:

- Design small experiments with clear success criteria, feedback loops, and safe-to-fail guardrails.
- Sequence work in increments, assess impact, and scale what works while documenting evidence and trade-offs.

2) Proposed content topics for potential modules

1. Drivers of digital transformation (Level A) - Understand why change is needed and where value comes from (users, law, data, cost, inclusion).
Examples: Map drivers for a permit service; link each driver to a measurable outcome.
2. What to digitize vs. where humans matter (Level A) - A simple framework to decide automate/augment/human-only, with safeguards.
Examples: Automate intake triage; keep complex eligibility decisions human with AI-assisted summaries.

3. Spotting and cataloguing innovation in your domain (Level A) - Scan, shortlist, and write 1-page briefs on relevant initiatives.
Examples: Compile three comparable chatbot pilots; extract success factors and pitfalls.
4. Leadership enablers: procurement, budgeting, governance (Level A) - How process tweaks unlock iterative delivery and reduce risk.
Examples: Design a milestone-based procurement; create a discovery → alpha → beta budget outline.
5. From pain points to backlog (Level B) - Turn evidence from citizens/staff into user stories with acceptance criteria.
Examples: Convert five frequent complaints into backlog items; define metrics for “done.”
6. Building the enabling environment (Level B) - Operating principles, roles, and standards that help teams move faster together.
Examples: Draft a 1-page “ways of working”; publish templates for service pages and forms.
7. Horizon scanning 101 (Level C) - Lightweight methods to track signals/trends and feed the policy cycle.
Examples: Monthly trend scan; add tech drivers to a policy impact log.
8. Skills for tomorrow’s PA (Level C) - Translate tech shifts into role/skill implications and a micro-upskilling plan.
Examples: Identify three roles impacted by AI-assisted triage; design a 4-week learning path.
9. Designing small pilots with big learning (Level C) - Safe-to-fail experiments, success criteria, and ethics/compliance checks.
Examples: Pilot an appointment scheduler; define KPIs (no-show rate, satisfaction), guardrails, and exit criteria.
10. Incremental development and feedback loops (Level C) - Plan work in slices; validate early with real users.
Examples: Release a simplified form; measure completion time; iterate on error messages.
11. Measuring public value (Level B) - Choose KPIs that reflect user outcomes, not just activity.
Examples: Track time-to-complete, successful first-time completion, and user trust signals.
12. Change communication and stakeholder alignment (Level B) - Keep leadership, partners, and users informed and engaged.
Examples: Publish a plain-language roadmap; run “you said - we did” updates after each iteration.
13. Risk, compliance, and ethics in innovation (Level C) - Balance speed with safety (privacy, security, accessibility, fairness).
Examples: Add a light compliance checklist to each pilot; record provenance for AI-assisted outputs.
14. Scaling what works & retiring what doesn’t (Level C) - Criteria to expand pilots, document playbooks, and sunset experiments.
Examples: Write a “go/no-go” note; create a reusable template and SOPs for scale-up.
15. Learning health: retrospectives and knowledge sharing (Level C) - Institutionalize lessons and avoid reinvention.
Examples: Run a 30-minute retro with 3 keep/3 change items; publish a two-page case note.

C6.2. Developing digital competence in the workplace

1) Learning outcomes

D1. Openness to adopt new digital tools with adequate training (Level A)

By the end, public employees will be able to:

- Articulate their learning needs when a new tool is introduced and select appropriate training formats (quick starts, sandbox practice, clinics).
- Complete a basic onboarding plan (setup → first tasks → feedback) and reach a defined “minimum viable proficiency.”
- Document issues/insights during adoption to inform team-wide roll-out.

D2. Awareness of institutional training strategies and offers (e.g., PA e-learning campuses) (Level A)

By the end, public employees will be able to:

- Locate and summarize the strategic lines of their organization’s digital-skills plan and related catalogues.
- Build a personal learning itinerary aligned with role goals and organizational priorities.
- Track progress in a simple learning record and share it with their manager.

D3. Engage with learning opportunities that fit professional development needs; practice lifelong learning (Level A)

By the end, public employees will be able to:

- Compare learning options (self-paced, cohort, peer learning, mentoring) against time, depth, and relevance constraints.
- Set quarterly learning goals and evidence outcomes in day-to-day work (before/after examples).
- Contribute to a peer-learning session by sharing a short “how we solved it” case.

D4. Demonstrate motivation and responsibility; model good digital practices and encourage others (Level B)

By the end, public employees will be able to:

- Apply and model core practices (secure sharing, versioning, accessibility, documentation) in routine tasks.
- Offer constructive feedback and micro-coaching to colleagues adopting new tools.
- Recognize and celebrate improvements to reinforce a learning culture.

D5. Apply new digital skills in daily tasks; evaluate effectiveness and refine practices (Level B)

By the end, public employees will be able to:

- Implement a new skill in a work scenario, measure its impact (time saved, errors reduced, quality), and iterate.
- Capture “before/after” metrics and lessons learned in a brief improvement note.
- Propose minor process updates or templates to codify the improvement.

D6. Follow international trends and reference frameworks for digital competence (Level C)

By the end, public employees will be able to:

- Summarize key ideas from recognized frameworks and explain how proficiency levels evolve.
- Map their own strengths/gaps to these references and identify next-step capabilities.
- Share a short outlook note on trends relevant to their role.

D7. Assess and audit methods to identify workplace digital-competence gaps; suggest training and mentoring (Level C)

By the end, public employees will be able to:

- Use light-touch diagnostics (task audits, remote-work readiness checks) to surface skill gaps.
- Recommend fit-for-purpose interventions (micro-lessons, peer clinics, mentoring pairs) with simple success criteria.
- Track completion and impact, and refine the training mix accordingly.

2) Proposed content topics for potential modules

1. Adopting new tools with confidence (Level A) - A practical playbook for going from “new app” to “minimum viable proficiency.”
Examples: Create a 2-week onboarding checklist for a new collaboration tool; run a sandbox exercise and record lessons.
2. Reading the training strategy & building your learning plan (Level A) - Align personal goals with institutional priorities and catalogues.
Examples: Extract three priorities from the PA e-learning campus; assemble a 90-day learning itinerary.
3. Choosing the right learning format (Level A) - Match need, depth, and time to self-paced, cohort, peer learning, or mentoring.
Examples: Turn a workflow problem into a peer clinic; select a micro-course for a just-in-time skill.
4. Modelling good digital practices (Level B) - Everyday behaviors that elevate team quality and safety.
Examples: Introduce a one-page “sharing & versioning” guide; coach a colleague on accessibility basics.
5. From learning to impact (Level B) - Apply a new skill, measure the effect, and iterate.
Examples: Replace manual steps with a template; show time saved and error reduction in a brief note.
6. Using reference frameworks to plan growth (Level C) - Make sense of proficiency continua and plan next steps.
Examples: Map your current skills to levels; identify two priority capabilities for the next quarter.
7. Diagnostics for digital-competence gaps (Level C) - Simple audits that reveal training needs in everyday tasks and remote work.
Examples: Run a task audit to find low-skill bottlenecks; propose a micro-lesson and mentoring pair to close a gap.
8. Designing peer learning and mentoring (Level B) - Create lightweight, high-impact knowledge-sharing formats.
Examples: Launch a monthly “show-and-tell”; set up mentor/mentee goals and a feedback loop.
9. Tracking progress and showcasing results (Level B) - Build a simple learning record and share improvements.
Examples: Maintain a skills log; present a 3-slide “you said - we did” update after a learning sprint.
10. Lifelong learning habits (Level C) - Routines that keep skills current without overload.
Examples: Curate a 15-minute weekly reading list; schedule quarterly goal reviews and horizon scans.

C6.3. AI Literacy in public administration

1) Learning outcomes

D1. Openness to consider opportunities of AI systems for PA functions (Level A)

By the end, public employees will be able to:

- Describe plausible AI-enabled improvements to their workflows (efficiency, quality, accessibility) and articulate expected public value.

- Distinguish “nice-to-have” from “high-value” use-cases using simple criteria (impact, risk, feasibility).

D2. Ensure users of AI in PA are provided a sufficient level of AI literacy (Level A)

By the end, public employees will be able to:

- Identify the minimum AI literacy elements staff and beneficiaries need (purpose, limitations, data handling, oversight).
- Draft short guidance/briefings to accompany any AI-enabled interaction.

D3. Recognize what AI is (and is not) in general terms (Level A)

By the end, public employees will be able to:

- Explain, in plain language, the difference between rules-based automation and AI/ML systems, with relatable examples.
- Spot “AI-washing” and request clarification when a tool’s intelligence is overstated.

D4. Critically evaluate where AI can support or substitute human skills (Level B)

By the end, public employees will be able to:

- Compare tasks where AI augments judgement vs. tasks where substitution risks are high; recommend human-in-the-loop controls.
- Document trade-offs (speed vs. explainability; coverage vs. bias) for decision-makers.

D5. Identify which regular tasks are (not) suitable for generative AI (Level B)

By the end, public employees will be able to:

- Triage daily tasks into “OK for GenAI”, “OK with safeguards”, and “Not suitable”, with examples and rationale.
- Create a personal “GenAI do/don’t” list aligned with institutional policy.

D6. Know core AI concepts (LLMs, machine learning, deep learning) (Level B)

By the end, public employees will be able to:

- Define LLMs, ML, and DL at a non-technical level; explain inputs/outputs, training data, and inference.
- Relate these concepts to concrete PA use-cases (summarization, classification, routing).

D7. Value discussion of ethical and social implications (inclusion/exclusion) (Level B)

By the end, public employees will be able to:

- Facilitate brief, structured discussions on equity, accessibility, and societal impact for any AI use in their area.
- Capture concerns and mitigations in a short “ethics note.”

D8. Avoid risky inputs: sensitive, proprietary, or personal data (Level B)

By the end, public employees will be able to:

- Apply “privacy-by-default” prompting: minimize data, strip identifiers, use approved secure channels.
- Explain leakage risks and appropriate redaction/pseudonymization before using any AI tool.

D9. Be aware of risks of specific AI tools and basic mitigation steps in context (Level B)

By the end, public employees will be able to:

- Complete a simple pre-use checklist (purpose, data, audience, risks, safeguards) for a given AI tool and context.
- Log provenance (sources/links) and set verification steps proportionate to the use.

D10. Respect organizational rules about freely available GenAI tools (Level B)

By the end, public employees will be able to:

- Locate and apply institutional policy for public GenAI use (allowed, restricted, banned scenarios).
- Choose an approved alternative when open tools lack required oversight.

D11. Outline examples of high-risk/prohibited AI systems under the AI Act and their impacts (Level C)

By the end, public employees will be able to:

- Identify high-risk and prohibited categories relevant to their field; describe potential negative impacts and affected rights.
- Signpost complaint/appeal channels and user rights where applicable.

D12. Contribute to institutional AI literacy practices and guidance (Level C)

By the end, public employees will be able to:

- Draft or adapt short internal guidance aligned with regulatory expectations (e.g., AI Act Article 4) and industry standards.
- Run a 15-minute “AI basics” huddle for colleagues and capture Q&A for a living FAQ.

2) Proposed content topics for potential modules

1. What AI is (and isn't) (Level A) - Demystify AI vs. rules-based automation; recognize AI-washing and request clarity.
Examples: Classify five tools (macro, rules engine, ML model, LLM assistant, chatbot script).
2. Core concepts for non-technical (Level B) - LLMs, training data, prompts, inference, and typical PA use-cases.
Examples: Map “input → model → output → verification” for an AI summarizer used on public reports.
3. Where AI helps vs. where humans must decide (Level B) - Framework to choose augment/substitute/human-only with oversight points.
Examples: Allow AI drafting of plain-language notices; require human approval for eligibility decisions.
4. Generative AI at work: do's and don'ts (Level B) - Practical triage of daily tasks into OK / OK-with-guardrails / Not suitable.
Examples: “OK”: rewrite for clarity with sources; “Guardrails”: dataset summary with citations; “Not suitable”: PII-rich case triage.
5. Safe prompting and data minimization (Level B) - Techniques to avoid leaking sensitive, proprietary, or personal data.
Examples: Redact identifiers; use synthetic examples; route PII tasks to approved secure assistants.
6. Provenance and verification (Level B) - Ask for citations/links, check authority/recency, and keep an evidence log.
Examples: Require “explain and cite” outputs; verify against official portals before publication.
7. Ethics and social impact conversations (Level B) - Lightweight methods to surface inclusion, bias, and accessibility concerns.
Examples: Run a 10-minute ethics check; record mitigations in an “ethics note” attached to the task.
8. Institutional rules for GenAI (Level B) - Understand and apply your organization's policy on public vs. approved tools.
Examples: Replace a public chatbot with an approved enterprise assistant; log exceptions with rationale.
9. Tool-specific risk awareness and mitigations (Level B) - Read a basic “model card” or tool note; apply proportionate controls.
Examples: Limit scope; set confidence thresholds; require human-in-the-loop for sensitive outputs.
10. AI Act basics for practitioners (Level C) - High-risk vs. prohibited uses, sector-relevant examples, and user rights.

Examples: Flag a proposed biometric categorization as prohibited; identify documentation needs for a high-risk risk-scoring tool.

11. Designing AI literacy artefacts (Level C) - Create concise internal guides, FAQs, and quick-starts for colleagues and beneficiaries.

Examples: Draft a one-page “Using AI safely at work”; record a 2-minute explainer for a new assistant.

12. Practice lab: from idea to safe use (Level C) - Apply the full chain: opportunity → ethics/risk check → safe prompt → verification → record.

Examples: Use an assistant to draft a citizen FAQ, verify sources, add citations, and log oversight steps.

A7. Digital leadership and governance in public administration

C7.1. Managing performance and operations in the digital environment

1) Learning outcomes

D1. Operate with core concepts of digital performance & operations (Level A)

By the end, public employees will be able to:

- Define and relate digital project management, collaborative platforms, workflow management, performance monitoring, dashboards, KPIs/OKRs, open-data standards, data-quality management, and automatic reports.
- Map these concepts to their own unit’s operational cycle (plan → deliver → monitor → learn → improve).

D2. Use collaborative platforms for systematic activity management (Level A)

By the end, public employees will be able to:

- Configure projects/boards (e.g., Asana/Trello/Monday), assign owners & due dates, and connect simple AI dashboards for KPI tracking, alerts, and real-time status views.
- Maintain a single source of truth linking tasks, files, and performance indicators.

D3. Implement digital feedback systems (including AI-powered self-assessment) (Level A)

By the end, public employees will be able to:

- Deploy lightweight, continuous feedback loops (surveys, in-product prompts) and AI tools that enable self-assessment and transparent indicator sharing with stakeholders.
- Prioritize improvements from feedback and close the loop (“you said - we did”).

D4. Create and maintain personalized performance dashboards (Level A)

By the end, public employees will be able to:

- Build role-specific dashboards in Excel or Data Studio (now Looker Studio), document definitions and sources, and keep a traceable evaluation record in a central system.
- Validate data quality and update cadence.

D5. Share performance indicators transparently (Level A)

By the end, public employees will be able to:

- Publish periodic KPI packs in accessible formats and proactively solicit feedback for continuous improvement.
- Apply plain-language explanations of indicators, trends, and caveats.

D6. Operate with advanced analytics & BI concepts (Level B)

By the end, public employees will be able to:

- Explain business intelligence, advanced performance analytics, process optimization, workforce analytics, predictive modelling, and integrated management systems at a practitioner level.
- Select fit-for-purpose analytical approaches for typical operational questions.

D7. Interpret financial performance indicators (Level B)

By the end, public employees will be able to:

- Compute and interpret cost/unit and cost/beneficiary, relate them to throughput and quality, and use them in efficiency decisions.

D8. Develop demand & capacity predictive models (Level B)

By the end, public employees will be able to:

- Integrate data from ERP/CRM/monitoring platforms, build simple demand forecasts, and translate outputs into capacity planning and staffing recommendations.

D9. Configure early-warning systems & automated reporting (Level B)

By the end, public employees will be able to:

- Set KPI thresholds and anomaly alerts; generate automated narrative reports using NLG techniques for timely decision-making.

D10. Apply A/B testing & what-if scenario analysis (Level B)

By the end, public employees will be able to:

- Design proportionate experiments and scenario models to evaluate operational changes, reading results alongside financial KPIs for optimization.

D11. Demonstrate digital agility with new BI/AI tools (Level B)

By the end, public employees will be able to:

- Trial emerging BI/AI solutions, compare against current tools, and adopt those that measurably improve performance.

D12. Operate with strategic performance management concepts (Level C)

By the end, public employees will be able to:

- Explain enterprise governance, organizational transformation, policy development cycles, quality standards for public services, and international benchmarking - and connect them to KPIs/OKRs.

D13. Use process mining & advanced analytics for institutional optimization (Level C)

By the end, public employees will be able to:

- Apply process mining to identify redundancies/bottlenecks and present evidence-based options to leadership.

D14. Optimize strategic budget distribution with analytics (Level C)

By the end, public employees will be able to:

- Use predictive analytics and scenario modelling in integrated BI systems to propose budget allocations that maximize impact and efficiency.

D15. Develop AI governance for performance management (Level C)

By the end, public employees will be able to:

- Draft proportionate AI governance measures (impact assessment, traceability of automated decisions, roles & oversight) and coordinate with institutional digital-governance systems.

D16. Promote a culture of continuous optimization (Level C)

By the end, public employees will be able to:

- Use analytics to detect bottlenecks, run improvement cycles, and demonstrate measurable gains in public-service outcomes, including digital services.

2) Proposed content topics for potential modules

1. Digital performance concepts 101 (Level A) - Build a common language: KPIs vs. OKRs, workflows, dashboards, data quality, open-data principles, and auto-reports.
Examples: Translate a policy objective into an OKR; define KPIs with sources and update cadence.

2. Work orchestration on collaborative platforms (Level A) - Configure projects/boards, set owners/SLAs, connect AI widgets for live KPI views and alerts.
Examples: Create a “Permits” board on Asana with SLA alerts; surface on-time completion as a dashboard card.
3. Continuous feedback & transparent reporting (Level A) - Design digital feedback systems (incl. self-assessment) and publish accessible KPI packs.
Examples: Launch a monthly micro-survey; issue a “you said - we did” performance note.
4. Dashboarding with Excel/Looker Studio (Level A) - Build role-based dashboards; ensure definitions, traceability, and documentation.
Examples: Create a manager dashboard with backlog, throughput, and cost/unit; link each tile to its data dictionary.
5. Business intelligence & advanced analytics for operations (Level B) - Choose methods and models that answer day-to-day performance questions.
Examples: Use a control chart for processing times; segment workload by channel/complexity.
6. Financial KPIs that matter (Level B) - Read and act on cost per unit/beneficiary and related efficiency indicators.
Examples: Attribute cost drivers; propose a process change that lowers cost/beneficiary without harming quality.
7. Demand forecasting & capacity planning (Level B) - Integrate ERP/CRM/monitoring data to anticipate volumes and match resources.
Examples: Forecast monthly applications; plan staffing and opening hours accordingly.
8. Early-warning & automated narratives (NLG) (Level B) - Configure KPI thresholds and generate auto-reports in plain language.
Examples: Trigger alerts on SLA breaches; auto-compose a weekly summary with trend explanations.
9. A/B tests & what-if analysis for improvement (Level B) - Test operational changes safely; pair results with financial indicators.
Examples: A/B test a simplified form; run a what-if on staffing mix vs. wait times.
10. Process mining for public services (Level C) - Discover actual workflows, find bottlenecks, and quantify impact.
Examples: Use event logs to show rework loops; propose a rule change that removes a redundant step.
11. Strategic performance management & benchmarking (Level C) - Align service KPIs with organizational objectives and external standards.
Examples: Map unit KPIs to strategic OKRs; benchmark processing time internationally.
12. Budget optimization with analytics (Level C) - Allocate resources using predictive models and scenarios; track impact.
Examples: Re-balance budget lines to improve throughput; justify changes with modelled outcomes.
13. AI governance for performance management (Level C) - Ensure traceability, oversight, and impact assessment for AI-driven monitoring.
Examples: Record an AI impact note; log automated decisions with human-review checkpoints.
14. Digital agility & tool adoption (Level B) - Evaluate and responsibly adopt emerging BI/AI solutions that improve operations.
Examples: Pilot a new anomaly-detection widget; compare precision/effort vs. current method and decide on rollout.
15. Culture of continuous optimization (Level C) - Establish improvement rhythms (retros, metric reviews) and celebrate measurable wins.

Examples: Run a monthly “bottleneck clinic”; publish a before/after metric card for each improvement.

C7.2. Leading team development in the digital environment

1) Learning outcomes

D1. Operate with core learning concepts (digital learning, e-learning platforms, skills assessment, competency mapping, microlearning, digital mentoring, constructive feedback) (Level A)

By the end, leaders will be able to:

- Explain each concept and when to use it in team development plans.
- Select suitable modalities (microlearning vs. cohort courses) and align them to role competencies.
- Deliver constructive, timely feedback using agreed rubrics and examples.

D2. Know principles of digital leadership, async collaboration, digital inclusion, EQ in virtual work, hybrid team dynamics (Level A)

By the end, leaders will be able to:

- Model inclusive, psychologically safe behaviors in hybrid/remote settings.
- Balance synchronous vs. asynchronous rhythms; use EQ cues to prevent conflict and burnout.

D3. Use collaborative platforms (Teams/Slack/Miro) for systematic coordination and competency observation (Level A)

By the end, leaders will be able to:

- Configure channels/boards, run rituals (stand-ups, retros), and link tasks to learning goals.
- Evaluate digital skills via structured observation and short self-assessments; record evidence.

D4. Promote AI copilots and prompt-engineering in daily workflows (Level A)

By the end, leaders will be able to:

- Identify safe, high-value use cases for copilots (drafting, summarizing, translation) and coach staff on prompt patterns.
- Establish verification and provenance routines for AI-assisted outputs.

D5. Create individual digital-competence development plans linked to performance; implement recurring feedback (Level A)

By the end, leaders will be able to:

- Map role expectations to capability gaps and define quarterly learning OKRs.
- Run cadence reviews and adapt plans based on progress data and feedback.

D6. Encourage continuous development via supportive leadership and digital guidance/recognition (Level A)

By the end, leaders will be able to:

- Offer micro-coaching, curate resources, and use digital badges/recognition to reinforce progress.
- Remove blockers and ensure equitable access to learning time/tools.

D7. Operate with advanced learning concepts (learning analytics, blended/organizational learning, change management, digital coaching, future skills, adaptive learning, motivation psychology in remote work) (Level B)

By the end, leaders will be able to:

- Interpret learning data to target interventions; pair change-management tactics with coaching.
- Design blended pathways that build future skills and sustain motivation (autonomy, belonging, fairness).

D8. Use development indicators and learning strategies for digital optimization (Level B)

By the end, leaders will be able to:

- Define and track completion, skill-improvement, and engagement metrics; iterate based on signal, not noise.
- Report outcomes in plain language with visuals and next steps.

D9. Configure personalized development plans using external platforms (Coursera, TalentLMS) with learning analytics (Level B)

By the end, leaders will be able to:

- Curate course playlists, set milestones, and monitor progress dashboards.
- Adjust pathways based on difficulty, pace, and performance data.

D10. Develop predictive models for future competency needs and strategic workforce development (Level B)

By the end, leaders will be able to:

- Translate strategy and service roadmaps into skills forecasts; use simple predictive signals to plan upskilling.
- Prioritize training investments and succession pipelines accordingly.

D11. Implement integrated learning ecosystems (e-learning + microlearning + self-development + digital recognition) (Level B)

By the end, leaders will be able to:

- Stitch tools into a cohesive learner journey with single entry points and badge criteria.
- Measure ecosystem effectiveness and reduce duplication.

D12. Demonstrate proactive stewardship of team digital development (Level B)

By the end, leaders will be able to:

- Identify emerging competence needs early and mobilize the right resources.
- Keep an up-to-date capability map and learning backlog.

D13. Operate with strategic talent concepts (capability, future of work, culture, leadership pipeline, digital succession) (Level C)

By the end, leaders will be able to:

- Connect capability building to transformation goals; maintain ready-now/ready-soon leader pools.
- Embed equity and inclusion in pipeline decisions.

D14. Use AI/ML for data-driven task allocation and workforce optimization (Level C)

By the end, leaders will be able to:

- Match tasks to competencies using approved tools; monitor fairness and workload balance.
- Review algorithmic outputs and retain human oversight.

D15. Build organizational capability strategies and implement enterprise talent systems (Level C)

By the end, leaders will be able to:

- Define governance, processes, and data needed to run talent systems (skills inventory, learning records, mobility).
- Monitor adoption and outcomes; iterate standards/templates.

D16. Use AI for strategic human-capital planning; manage resistance and cultural change (Level C)

By the end, leaders will be able to:

- Run change playbooks (stakeholder mapping, comms, quick wins) for AI transitions.
- Anticipate resistance, co-design guardrails, and track sentiment.

D17. Promote a culture of continuous learning, collaboration, and digital innovation (Level C)

By the end, leaders will be able to:

- Lead by example, sponsor communities of practice, and mainstream experimentation with emerging technologies.
- Publish “you said - we did” updates that link learning to improved services.

2) Proposed content topics for potential modules

1. Foundations: digital leadership & hybrid team dynamics (Level A) - Core behaviors for inclusive, high-trust, hybrid teams; async vs. sync balance.
Examples: Redesign a weekly meeting into an async update + focused clinic; draft team “ways of working.”
2. Learning architecture & competency mapping (Level A) - Translate role expectations into skills maps and blended pathways.
Examples: Build a competency map for a service team; convert it into a microlearning + cohort plan.
3. Collaborative platforms as learning hubs (Level A) - Use Teams/Slack/Miro to coordinate work, surface learning needs, and document feedback.
Examples: Create a learning channel with monthly challenges; track observations on a shared board.
4. Constructive feedback & digital mentoring (Level A) - Practical models and rituals that make feedback safe, specific, and useful.
Examples: Run 15-minute feedback sprints; pair mentors/mentees with a simple goal sheet.
5. AI copilots & prompt-engineering for teams (Level A) - Integrate copilots safely to boost quality and throughput; teach prompt patterns.
Examples: Create a “prompt gallery” for standard tasks; add a verification checklist with citations.
6. Learning analytics & indicators (Level B) - Define completion, skill-gain, and engagement metrics; interpret and act on them.
Examples: Build a one-page learning KPI dashboard; decide which course to retire/replace.
7. Personalized learning with Coursera/TalentLMS (Level B) - Curate playlists, set milestones, and adapt pacing via analytics.
Examples: Assemble a track for “digital service associate”; adjust based on quiz performance.
8. Motivation psychology in remote work (Level B) - Design learning that supports autonomy, belonging, and fairness.
Examples: Offer choice of learning formats; rotate facilitation to increase belonging.
9. Change management for learning & AI adoption (Level B) - Plan communications, quick wins, and feedback loops to reduce resistance.
Examples: Launch a 30-day AI pilot with office hours; publish FAQs and “you said - we did” notes.
10. Predicting future skills & workforce planning (Level B) - Use signals and simple models to anticipate competency demand.
Examples: Build a skills heatmap from upcoming projects; prioritize two critical upskilling themes.
11. AI-assisted task allocation & fairness (Level C) - Match tasks to skills while monitoring equity and outcomes.
Examples: Pilot an allocation tool; audit for load balance and bias; keep human override.
12. Integrated learning ecosystems & digital recognition (Level B) - Orchestrate e-learning, microlearning, self-study, and badges.
Examples: Implement a “Learn → Apply → Share” badge; automate badge issuance on course completion.
13. Enterprise talent systems & leadership pipeline (Level C) - Processes and data to identify, develop, and retain future leaders.
Examples: Configure a skills inventory; design “ready-soon” rotational assignments.

14. Organizational learning & optimization loops (Level B) - Turn lessons into playbooks; retire low-value activities.
Examples: Publish a “how we fixed X” note; archive outdated materials and replace with concise guides.
15. Culture of continuous learning & digital innovation (Level C) - Rituals and incentives that make learning visible and valued.
Examples: Monthly “demo day” of micro-improvements; micro-grants for experimenting with emerging tools.

C7.3. Driving and leading innovation and digital transformation

1) Learning outcomes

D1. Operate with core innovation and transformation concepts (Level A)

By the end, leaders will be able to:

- Define and relate innovation management, change management, design thinking, digital transformation, emerging technologies, open innovation, and digital resilience in the PA context.
- Select which concept/tool fits a given challenge and justify the choice with expected public value.

D2. Apply public-sector delivery principles (user-centered, iterative, agile, sandboxing) (Level A)

By the end, leaders will be able to:

- Frame problems through user needs, plan iterative delivery with timeboxed experiments, and use controlled testing environments for safe learning.
- Evidence learning with short “discovery → alpha → beta” notes.

D3. Recognize automation opportunities; facilitate digital analysis; propose AI proofs-of-concept (Level A)

By the end, leaders will be able to:

- Use process and data analysis tools to surface bottlenecks; shortlist steps for automation; scope an AI PoC with clear success criteria and ethics/compliance guardrails.

D4. Initiate simple process improvements and contribute to digitization pilots (Level A)

By the end, leaders will be able to:

- Launch small pilots (templates, online forms, routine automations), track effects on time, errors, and satisfaction, and decide scale/stop.

D5. Document and communicate lessons learned through knowledge-sharing platforms (Level A)

By the end, leaders will be able to:

- Publish concise case notes, reusable templates, and “you said - we did” updates to grow institutional memory.

D6. Operate with portfolio-level concepts (frameworks, pipelines, lifecycles, roadmaps, scaling methods, AI-enabled ecosystems, accessibility-by-default, usability testing) (Level B)

By the end, leaders will be able to:

- Build an innovation pipeline, maintain a transformation roadmap, embed accessibility/usability checks, and plan scale-up paths for successful pilots.

D7. Measure innovation impact with proportionate metrics (Level B)

By the end, leaders will be able to:

- Define innovation metrics and transformation KPIs; perform cost-benefit analyses for digital initiatives; present findings in plain language.

D8. Set prioritization criteria, enable controlled experimentation, and draft departmental strategies (Level B)

By the end, leaders will be able to:

- Establish idea-evaluation rubrics, run digital sandboxes with guardrails, and write a departmental transformation strategy linked to a structured pipeline.

D9. Scale AI solutions across services with interoperability and resources, keeping UCD principles (Level B)

By the end, leaders will be able to:

- Plan cross-service deployment (APIs, data standards, training) and protect user-centered design throughout scale-up.

D10. Measure ROI and build partnerships with technology providers (Level B)

By the end, leaders will be able to:

- Calculate ROI with direct/indirect benefits, negotiate partnership models, and align vendor work to institutional outcomes.

D11. Provide strategic vision on emerging technologies and prepare teams to adapt (Level B)

By the end, leaders will be able to:

- Articulate plausible impacts of emerging tech on services and workforce; outline readiness actions and change narratives.

D12. Operate with strategic ecosystem concepts (digital maturity, disruption strategy, strategic partnerships, cultural and regulatory innovation, public-private ecosystems, governance) (Level C)

By the end, leaders will be able to:

- Assess digital maturity, choose disruption strategies responsibly, and set up governance for public-private innovation ecosystems.

D13. Develop an institutional digital-transformation vision aligned with national strategy; run enterprise innovation management (Level C)

By the end, leaders will be able to:

- Draft a clear vision statement, align it with national agendas, and implement an enterprise framework that coordinates initiatives, budgets, and benefits.

D14. Build an institutional AI roadmap aligned with the AI Act and Digital Decade; lead cultural change (Level C)

By the end, leaders will be able to:

- Prioritize AI opportunities, embed compliance/ethics, and drive change management for adoption at scale.

D15. Implement innovation scouting and strategic partnerships for high-value tech integration (Level C)

By the end, leaders will be able to:

- Run structured scouting, evaluate fit, and negotiate collaborations to integrate solutions that raise public-service value.

D16. Develop strategic partnerships across the tech ecosystem to deliver value (Level C)

By the end, leaders will be able to:

- Create multi-party agreements with clear objectives, governance, data/interoperability clauses, accessibility, and measurable outcomes.

2) Proposed content topics for potential modules

1. Innovation & transformation foundations (Level A) - Build a shared language (innovation management, change, DT, design thinking, open innovation, resilience) and when to use each.
Examples: Map a service problem to design thinking vs. change management; define success in citizen terms.

2. User-centered, iterative delivery in PA (Level A) - From problem framing to sandbox tests and timeboxed iterations.
Examples: Run a 2-week alpha on a simplified form; capture insights before beta.
3. Finding automation & AI PoC candidates (Level A) - Use process data to spot bottlenecks and scope safe AI proofs-of-concept.
Examples: Identify a triage step for automation; draft a PoC charter with guardrails and KPIs.
4. Quick wins: templates, forms, micro-automations (Level A) - Launch low-risk pilots that cut effort and errors.
Examples: Convert a paper request to an online form; auto-route submissions; compare before/after throughput.
5. Communicating what works (Level A) - Knowledge-sharing that scales learning (case notes, playbooks, “you said - we did”).
Examples: Publish a 2-page case with metrics and reusable artefacts.
6. Pipelines, roadmaps, and scaling methods (Level B) - Manage an innovation pipeline, maintain a transformation roadmap, and plan scale-up paths.
Examples: Move three pilots through “incubate → prove → scale”; embed accessibility and usability checks.
7. Measuring impact & value (Level B) - Innovation metrics, transformation KPIs, and proportionate cost-benefit/ROI.
Examples: Calculate time-saved and cost/beneficiary; present a one-page ROI note.
8. Prioritization & digital sandboxes (Level B) - Criteria to rank ideas; set up safe environments for controlled experiments.
Examples: Score a backlog by impact/effort/risk; run a sandbox with data minimization and audit logs.
9. Scaling AI across services (Level B) - Interoperability, training, and governance for cross-unit deployments with UCD kept intact.
Examples: Roll out a classification model to multiple services; maintain a common API and feedback loop.
10. Partnerships that deliver (Level B) - Vendor and ecosystem collaborations aligned to outcomes, not features.
Examples: Co-create a pilot with a tech partner; write output-based acceptance criteria.
11. Emerging-tech horizon & workforce readiness (Level B) - Sense what’s coming and prep skills, roles, and governance.
Examples: Draft a one-page “so what” on an emerging tech; identify training for affected roles.
12. Digital maturity & disruption strategies (Level C) - Assess where you are and choose fit-for-purpose levers (culture, regulation, partnerships).
Examples: Complete a maturity scan; design an intervention targeting the weakest domain.
13. Institutional vision & enterprise innovation management - Align to national strategy; coordinate portfolios and benefits.
Examples: Write a vision statement linked to measurable outcomes; stand up a lightweight portfolio board.
14. AI roadmap aligned with AI Act & Digital Decade (Level C) - Prioritize use-cases, compliance checkpoints, and change mgmt.
Examples: Place use-cases on a roadmap with risk categories; plan training and comms for each wave.
15. Innovation scouting & ecosystem partnerships (Level C) - Systematically find, assess, and integrate external solutions.
Examples: Run a quarterly scouting sprint; pilot with a civic-tech SME; evaluate scale-up fit.

16. Governance for digital innovation (Level C) - Roles, standards, documentation, and decision logs that keep speed with safety.
Examples: Create an innovation charter; implement a decisions register with provenance.
17. Accessibility-by-default & usability testing (Level B) - Bake inclusion and evidence into every iteration.
Examples: Add quick WCAG checks and 5-user tests to each pilot; publish fixes and learning.
18. From pilot to scale → to sunset (Level C) - Criteria to scale, standardize, or retire initiatives; manage benefits over time.
Examples: Apply go/no-go gates; convert a pilot into SOPs/templates; sunset a low-value tool and reinvest.

C7.4. Ensuring responsible digital governance and cybersecurity

1) Learning outcomes

D1. Operate with core concepts and principles (data governance, transparency by design, lifecycle, classification, interoperability, standards, GDPR, digital ethics & integrity) (Level A)

By the end, public employees will be able to:

- Define each concept in plain language and explain how they interact in day-to-day PA work.
- Map a dataset through its lifecycle, apply a basic classification, and state transparency-by-design measures.
- Identify common ethical risks and write a short integrity note for a digital initiative.

D2. Operate with digital security and sustainability basics (cyber hygiene, passwords, phishing, backup, incident reporting, green IT) (Level A)

By the end, public employees will be able to:

- Apply routine protections (MFA, updates, least privilege), recognize phishing signals, and execute backup/restore checks.
- Report incidents using institutional procedures and propose low-effort “green IT” actions in their team.

D3. Apply basic team cybersecurity policies; implement data classification; use AI ethics checklists with privacy settings (Level A)

By the end, public employees will be able to:

- Enforce strong credentials, update cadence, approved VPN use, and secure sharing.
- Classify information using institutional categories and document access rules.
- Run a proportionate AI ethics/privacy checklist before enabling AI features.

D4. Monitor compliance, report incidents, and document decisions for traceability (Level A)

By the end, public employees will be able to:

- Track team adherence to security standards, escalate with evidence, and keep decision/action logs that enable audits.

D5. Ensure accessibility/transparency while enforcing access control (need-to-know, WCAG 2.1) (Level A)

By the end, public employees will be able to:

- Produce accessible documents/pages and balance openness with appropriate access controls and logging.

D6. Operate with advanced frameworks and practices (data governance frameworks, ISO 27001, NIS2, OWASP, DPIA, business continuity & disaster recovery) (Level B)

By the end, public employees will be able to:

- Summarize what each framework requires at practitioner level and apply checklists for DPIA and BCP/DR preparations.

D7. Know PA-specific regulations/standards (Interoperability Law 242/2022, national security standards, AI Act) (Level B)

By the end, public employees will be able to:

- Identify which provisions affect their projects and list mandatory actions/roles for compliance.

D8. Develop departmental digital-governance policies and implement audit systems (Level B)

By the end, public employees will be able to:

- Draft concise policies aligned to organizational strategy and set up proportionate compliance checks with evidence trails.

D9. Evaluate ethical aspects of technology (bias, discrimination, transparency, AI dilemmas) (Level B)

By the end, public employees will be able to:

- Run structured ethics reviews, document trade-offs, and recommend mitigations (testing, oversight, user communication).

D10. Assume departmental security responsibility: implement controls and report risk to executives (Level B)

By the end, public employees will be able to:

- Maintain a simple risk register, implement control owners/due dates, and brief leadership on status and residual risks.

D11. Operate with strategic concepts (institutional digital governance, risk management, zero trust, EU/national compliance, ISO 42001, cyber resilience, digital sovereignty, AI governance, national strategies) (Level C)

By the end, public employees will be able to:

- Explain these concepts and position current initiatives against them; propose steps to strengthen resilience and governance maturity.

D12. Develop organizational digital-governance strategies aligned with law and standards, incl. comprehensive AI governance (Level C)

By the end, public employees will be able to:

- Produce a strategy outline (principles, roles, processes, metrics) and an AI governance annex (risk tiers, oversight, documentation).

D13. Define governance for emerging tech (AI, blockchain, IoT), contribute to national policy, and coordinate cyber-threat response (Level C)

By the end, public employees will be able to:

- Set decision rights and assurance steps for new tech, coordinate multi-agency responses, and feed lessons into policy updates.

D14. Advocate integration of digital ethics and responsible AI (transparency, explainability, fairness) into transformation strategies (Level C)

By the end, public employees will be able to:

- Embed ethics criteria and KPIs into programmes, ensuring ongoing monitoring and public communication.

2) Proposed content topics for potential modules

1. Foundations of digital governance (Level A) - Build a common language for governance, transparency-by-design, lifecycle, classification, interoperability, standards, GDPR, and ethics.
Examples: Map a dataset's lifecycle with classification and transparency notes; write a one-page integrity checklist.

2. Cyber hygiene & sustainability essentials (Level A) - Daily practices that lower risk and footprint (MFA, updates, phishing defense, backups, green IT).
Examples: Run a phishing drill; test a restore from backup; create a team “green IT” quick-wins list.
3. Team-level controls that actually stick (Level A) - Operationalize complex passwords, VPN use, and secure sharing; apply institutional data-classification and AI-ethics checklists.
Examples: Classify a shared folder; set time-bound access; complete an AI checklist before enabling a feature.
4. Accessibility + access control (Level A) - Make information usable for all (WCAG 2.1) while enforcing need-to-know with auditable permissions.
Examples: Fix headings/alt text on a report; configure role-based access and review logs monthly.
5. Compliance frameworks in practice (ISO 27001, NIS2, OWASP, DPIA, BCP/DR) (Level B) - What they require and proportionate ways to comply.
Examples: Run a DPIA-lite; draft a BCP scenario; map a web form against top OWASP risks.
6. PA-specific laws & standards (Level B) - Interoperability Law 242/2022, national security standards, AI Act - so what for your project?
Examples: Add mandatory metadata for interoperability; classify an AI use-case under the AI Act risk schema.
7. Writing departmental governance policies (Level B) - Turn principles into concise rules, roles, and routines; set evidence requirements.
Examples: Publish a 2-page data-classification policy with examples; define a quarterly control review.
8. Audits, logs, and traceability (Level B) - Build lightweight audit systems and decision registers that survive scrutiny.
Examples: Create an issue/owner/due-date log; attach evidence (screens, tickets) to each control check.
9. Ethics clinics for digital projects (Level B) - Structured conversations on bias, discrimination, explainability, and transparency.
Examples: Review a scoring tool for bias; draft a public “how this works” explainer.
10. Security leadership & risk reporting (Level B) - Own controls, maintain a risk register, and brief executives with clear heatmaps and actions.
Examples: Present top 5 risks with mitigations; assign control owners and review dates.
11. Strategic governance concepts (zero trust, resilience, sovereignty, ISO 42001, AI governance) (Level C) - Position current initiatives and plan maturity steps.
Examples: Draft a zero-trust rollout sketch; propose resilience drills; outline an AI governance matrix.
12. Organization-wide governance strategy + AI annex (Level C) - Align to national/European standards; define roles, processes, metrics, and AI oversight.
Examples: Write a strategy one-pager; add an AI risk tiering table and oversight checkpoints.
13. Governance for emerging tech (AI, blockchain, IoT) (Level C) - Decision rights, assurance steps, and procurement clauses.
Examples: Add explainability and provenance clauses to an RFP; define minimum logging for an IoT pilot.
14. Institutional & national coordination for cyber threats (Level C) - Roles, channels, and playbooks for cross-agency response.
Examples: Run a tabletop cyber incident; produce a post-incident “lessons learned” note and update the playbook.

15. Ethics-by-design in transformation programs (Level C) - Bake transparency, explainability, and fairness into roadmaps and KPIs.

Examples: Add “explainability tests passed” as a milestone; publish a transparency page for a new service.

C7.5. Using digital technologies for anticipatory and strategic thinking

1) Learning outcomes

D1. Operate with core analytical and decision concepts (data analysis, operationalization, cause–effect models, central tendency, basic systems thinking, structured/data-driven decisions) (Level A)

By the end, public employees will be able to:

- Translate policy or operational questions into measurable variables (clear operational definitions and simple causal assumptions).
- Calculate and interpret basic indicators (mean, median) and read simple cause–effect diagrams to inform a structured decision process.
- Explain how systems thinking reframes single problems as parts of wider feedback loops.

D2. Apply visualization and analysis techniques (dashboards, scenarios, simulations, predictive and comparative/benchmark analysis) (Level A)

By the end, public employees will be able to:

- Build or interpret basic analytical dashboards and choose appropriate chart types.
- Run simple planning scenarios and “table-top” simulations to explore options and trade-offs.
- Use comparative/benchmarking analysis to position their service against peers.

D3. Use preconfigured ML tools for short-term anticipation (root-cause & pattern discovery) (Level A)

By the end, public employees will be able to:

- Prepare clean, minimal datasets for no/low-code ML tools; run root-cause and association analyses safely.
- Interpret model outputs (feature importance, clusters) to anticipate near-term demand or issues and propose proportionate responses.

D4. Create what-if scenarios and analyze recurrent causes to understand interdependencies in team/service work (Level A)

By the end, public employees will be able to:

- Draft what-if models that test policy/process changes and capture likely side effects.
- Facilitate team reviews that connect recurring incidents to upstream causes and cross-team dependencies.

D5. Take responsibility for analysis quality and transparency (Level A)

By the end, public employees will be able to:

- Verify sources, document assumptions/limitations (data gaps, bias, timeliness), and communicate uncertainty clearly to colleagues and beneficiaries.
- Maintain concise evidence logs linking datasets, methods, and decisions.

D6–D7. Operate with intermediate concepts (predictive analytics, statistical modelling, data mining, BI, participatory foresight, scenario planning, systems thinking) and leverage advanced methods (regression, clustering, decision trees) in decisions (Level B)

By the end, public employees will be able to:

- Explain, in plain language, how common models work and what questions they answer.
- Interpret outputs from BI/statistical tools (coefficients, clusters, tree splits) and translate them into options, risks, and safeguards for decision-makers.

D8. Use scenario models and early-warning systems; apply AI-assisted portfolio analytics (Level B)

By the end, public employees will be able to:

- Configure indicators and thresholds for early warnings (opportunities/risks) and simulate policy impacts under multiple futures.
- Read AI-assisted portfolio views to understand how team performance affects public-service quality and prioritize interventions.

D9. Promote anticipatory and systemic thinking in teams (Level B)

By the end, public employees will be able to:

- Facilitate short sessions that visualize interdependencies (stocks/flows, causal loops) and help colleagues anticipate downstream effects before acting.
- Embed anticipatory routines (signals review, scenario refresh) in team cadences.

D10–D11. Operate with strategic anticipation & organizational intelligence; model policy impacts and co-create via open data & citizen participation (Level C)

By the end, public employees will be able to:

- Summarize external change signals in brief outlook notes that inform policy cycles.
- Model potential policy impacts and design simple co-creation loops (open-data reuse, participatory inputs) to stress-test decisions.

D12–D14. Develop institutional foresight capacity; lead responsible AI-supported foresight; promote an anticipatory vision organization-wide (Level C)

By the end, public employees will be able to:

- Stand up lightweight foresight practices (horizon scanning, trend synthesis, scenario sets) integrated with BI/AI pipelines.
- Lead responsible foresight initiatives (ethics, transparency, inclusiveness) and brief leadership on readiness actions for emerging social/technological shifts.
- Communicate an anticipatory vision and track adoption through simple maturity indicators.

2) Proposed content topics for potential modules

1. From question to metric (operationalization & causality basics) (Level A) - Turn policy questions into measurable indicators, sketch simple causal paths.
Examples: Define “processing time” and “first-time success” precisely; draw a quick cause–effect diagram for delays.
2. Dashboards that inform decisions (Level A) - Build/read compact dashboards; pick chart types that reduce cognitive load.
Examples: Convert a weekly report into a one-page dashboard; add notes on data freshness and caveats.
3. Scenarios, simulations, and what-if thinking (Level A) - Explore multiple futures and design proportionate responses.
Examples: Model what happens to wait times if demand rises 20%; test a new appointment rule in a sandbox.
4. Preconfigured ML for practitioners (Level A) - Use no/low-code tools safely to spot patterns and root causes.
Examples: Run a one-click classification to learn top drivers of case rework; validate with a holdout sample.
5. Benchmarking & comparative analysis (Level A) - Position your service vs. peers and learn from outliers.
Examples: Compare completion rates across counties; study positive deviants to copy practices.
6. Early-warning indicators & risk/opportunity sensing (Level B) - Set thresholds, alerts, and reviews for leading indicators.

- Examples:* Trigger an alert when backlog > X; open an “opportunity ticket” when a trend improves for 3 months.
7. Portfolio analytics for public-service impact (Level B) - See how project performance aggregates into service outcomes.
Examples: Link team throughput to complaint rates; prioritize items with the highest predicted impact on citizen experience.
 8. Participatory foresight and open-data co-creation (Level C) - Bring citizens/businesses into anticipatory work using open data.
Examples: Host a mini-scenario workshop with community inputs; publish an open dataset that supports reuse ideas.
 9. Reading model outputs like a policymaker (Level B) - Interpret regression, clustering, and trees without math overload; focus on decisions and risks.
Examples: Turn coefficients/clusters into “so-what” recommendations with confidence/limitations notes.
 10. Systems thinking in one page (Level B) - Tools to visualize interdependencies (stocks/flows, causal loops) that teams can use fast.
Examples: Map how staffing, demand, and rework form a feedback loop; identify leverage points.
 11. Quality & transparency of analysis (Level B) - Document sources, assumptions, and limitations; communicate uncertainty.
Examples: Add a methodology box to each brief; keep a lightweight evidence/provenance log.
 12. Horizon scanning & strategic anticipation (Level C) - Set up a cadence to track signals, trends, and drivers linked to policy/operations.
Examples: Produce a quarterly “signals to watch” note; link each signal to potential service implications.
 13. AI for foresight - responsibly (Level C) - Where AI adds value (classification, summarization, portfolio insights) and where human oversight is essential.
Examples: Use an assistant to cluster consultation feedback; publish the method/limitations alongside results.
 14. Institutional foresight capability & governance (Level C) - Build repeatable practices, roles, and minimal standards for anticipatory work.
Examples: Create a foresight playbook; set a monthly scenario refresh and an annual capability review.
 15. Anticipatory leadership & communication (Level C) - Craft narratives that prepare the organization for upcoming shifts and justify timely action.
Examples: Write a one-page “why act now” brief; run a leadership huddle with scenarios and readiness actions.

Annex 4 Example of knowledge-based TNA survey for the proposed general digital competency framework (levels A and B for digital competency areas 1-6)

A1. Digital literacy in public administration

Level A

Q1. single

Your institution introduces a new internal document management system (DMS) to replace email attachments. What is the first responsible step for all staff?

- A. Upload and tag documents only in the institutional DMS using official templates
- B. Continue sharing drafts by personal email accounts
- C. Save files on USB drives for easy access
- D. Print and archive all electronic copies in binders

Q2. multi-select

A colleague from another department requests a file containing citizen data. Which options show responsible sharing?

- A. Use the institution's encrypted email or file transfer system
- B. Confirm that the colleague is authorized to access the file
- C. Compress the file and send it from your personal email
- D. Upload the file on a public drive for convenience

Q3. single

You are preparing a report in Excel for the institution. Which feature helps you avoid manual calculation errors?

- A. Use built-in formulas (SUM, AVERAGE, IF) and verify with sample data
- B. Type each total manually to control results
- C. Add all numbers on a calculator and insert them by hand
- D. Ask a colleague to review without checking formulas

Q4. single

When using *data.gov.ro* for public data, which action ensures accuracy?

- A. Check the dataset's publication date before use
- B. Assume that all datasets are automatically updated
- C. Use only the first dataset found in search results
- D. Download large files without checking their content

Q5. multi-select

You receive an email that looks official but contains an unexpected link. What are correct actions?

- A. Report it immediately to your institution's IT or cybersecurity officer.
- B. Avoid clicking any links or downloading attachments.
- C. Alert colleagues to pay attention "just in case they got it too."
- D. Delete it silently without reporting.

Q6. single

You are editing a shared document using an approved collaborative platform (e.g. Microsoft Teams or Google Docs) with colleagues from another department.

Which practice ensures efficiency and version control?

- A. Edit in the shared file simultaneously and use “Track changes” for visibility
- B. Download and reupload the file after every modification
- C. Rename your file “final_final_version.docx” and email it
- D. Copy all text into a new document each time

Q7. multi-select

For policy evidence, which sources are typically acceptable?

Peer-reviewed research (when relevant)

Official statistics (INS or Eurostat)

Public comment threads

Administrative data published by an authority

Q8. single

Before comparing county rates, you should check:

- A. Definitions, units, and denominators in the dataset metadata
- B. Page footer icons
- C. Font family
- D. Comment count

Level B

Q1. single

Your institution is transitioning to the Government Cloud infrastructure. What is the key responsibility of department coordinators during this process?

- A. Ensure that all data is migrated securely and that staff are trained on access procedures
- B. Upload all files manually to a personal account for faster transfer
- C. Share login credentials among colleagues for convenience
- D. Wait for IT staff to complete everything without supervision

Q2. single

Your manager asks you to prepare a data report showing processing times for citizen requests. What principle ensures both accuracy and institutional trust?

- A. Use verified data sources, apply consistent definitions, and document calculation methods
- B. Include only data that shows improvement
- C. Average all numbers quickly, even if some are missing
- D. Collect feedback informally instead of data

Q3. multi-select

A ministry sends an urgent request for statistical data. Which actions ensure reliability and compliance?

- A. Verify the accuracy and completeness of data before submission.
- B. Use the designated official channel for sending information.
- C. Keep a record of the version and source of the data sent.
- D. Forward unverified drafts to meet the deadline.

Q4. multi-select

When training colleagues to use *data.gov.ro*, what practices reflect digital responsibility?

- A. Teach how to verify dataset sources and publication dates
- B. Explain how to filter and export data safely
- C. Encourage download of all datasets for later use
- D. Recommend editing official datasets locally

Q5. single

A group of employees uses personal cloud accounts to share internal files. What is the appropriate response?

- A. Provide institutional storage and clear policy on secure data sharing
- B. Allow personal accounts if they are convenient
- C. Ignore the issue unless a problem occurs
- D. Ask staff to send printed copies instead

Q6. multi-select

During an audit, multiple versions of the same project document are found. What steps build sustainable version control?

- A. Establish shared folder structures with clear naming conventions.
- B. Use track-changes or version history features.
- C. Delete all older files to avoid confusion.
- D. Require approval before any document is saved.

A2. Digital communication and collaboration

Level A

Q1. single

Your institution updates its website with a new news section. What is the first rule for publishing information there?

- A. Ensure that all posts are verified, dated, and written in an official tone
- B. Allow any staff member to post news without review
- C. Publish news before verifying facts to be the first to post
- D. Add long technical details that only highly trained experts can understand

Q2. multi-select

A citizen sends an inquiry through your department's official email. What are the correct steps to ensure a professional reply?

- A. Confirm receipt within the legal deadline
- B. Use the institutional format and sign with your official contact details
- C. Archive the message in the institutional record system
- D. Copy your personal email to keep track of the thread

Q3. single

Your team collaborates with another institution via email. Which subject line follows good administrative practice?

- A. "Collaboration request – Joint project on e-Services (Ref. no. 12/2025)"
- B. "Hello, small question :)"
- C. "URGENT – PLEASE REPLY NOW!!!"
- D. "Follow-up"

Q4. multi-select

When uploading reports to your institution's website, what practices ensure accessibility and compliance?

- A. Use searchable PDF format and include publication date
- B. Provide a short summary in plain language
- C. Avoid scanned images of text
- D. Upload only internal versions for staff

Q5. multi-select

Your institution plans to open a Facebook profile page for citizen communication. What must be ensured before launch?

- A. Define moderation rules and authorized administrators
- B. Align content tone with institutional communication policy
- C. Create a policy for managing comments and data protection
- D. Publish without moderation for full transparency

Q6. single

You receive an official letter from the Ministry. How should you share it internally?

- A. Forward through the institutional intranet or official mailing list, preserving the original format
- B. Copy-paste the content into a chat group
- C. Print and place it on a noticeboard only
- D. Send it through personal email accounts

Q7. single

A department wants to publish an infographic about public spending. What ensures credibility?

- A. Data comes from official sources (e.g., data.gov.ro or reports from the Ministry of Finance) and includes the publication date
- B. Use approximate figures for simplicity
- C. Add decorative icons and slogans instead of data
- D. Publish without referencing any source

Q8. multi-select

Your institution's social media post receives critical comments. Which reactions show professionalism and institutional maturity?

- A. Respond politely and provide factual clarifications
- B. Address repeated or offensive comments according to moderation policy
- C. Avoid emotional or defensive tone
- D. Delete all critical posts to avoid escalation

Q9. single

When writing an announcement about new digital services, what should be prioritized?

- A. Clarity, plain language, and key steps citizens must follow
- B. Use of institutional jargon and acronyms
- C. A very long text with detailed legal background
- D. Posting the announcement only in PDF format

Q10. single

You are creating an email signature for official communication. Which option follows the correct institutional format?

- A. Full name, position, institution, official contact details, and institutional logo
- B. First name and favorite quote
- C. Name and personal mobile number
- D. Name only, without title or contact information

Q11. single

What is the most effective way for a team to track simple tasks and owners when no advanced project-management tools are available?

- A. Use a shared task or project board in the organization's digital workspace (e.g., SharePoint, Teams, Google Workspace)
- B. Personal notes on paper
- C. A private chat thread
- D. Sticky notes on a wall

Q12. single

You want colleagues to see who owns a task and when it is due

- A. Add owner and due date fields on the shared board (task tracking instrument)
- B. Keep owners in a private file
- C. Put names inside a long comment
- D. Do not record dates

Q13. single

When co-authoring a memo with a colleague the fastest way to avoid version confusion is to

- A. Edit the same online document with comments and tracked changes
- B. Send many email attachments
- C. Save copies with new names everytime
- D. Paste the text into chat

Level B

Q1. single

Your institution prepares a press release on a new eGovernment service. What is the best first step to ensure clarity and trust?

- A. Verify all facts with the responsible department and use plain, citizen-oriented language
- B. Copy the technical project proposal into the release
- C. Use complex terms to sound authoritative

D. Publish without review to be the first

Q2. multi-select

You manage your institution's Facebook profile page during a temporary service outage. What communication actions ensure transparency and trust?

- A. Publish a factual update explaining the issue and expected resolution time
- B. Reply courteously to citizens' concerns with available information
- C. Avoid blaming partners publicly
- D. Provide contact details for further questions

Q3. single

You are coordinating an interinstitutional campaign on online safety. What ensures consistency across ministries and agencies?

- A. Use a shared communication brief and pre-approved key messages with institutional logos
- B. Allow each institution to post its own message freely
- C. Share drafts via WhatsApp groups only
- D. Adapt the message without consulting the lead ministry

Q4. single

Your team is designing an infographic on the use of EU funds. What must be included for credibility?

- A. Clear source references (e.g., Ministry of Finance, data.gov.ro, europa.eu) and update date
- B. Only positive results to promote the institution
- C. Slogans instead of numbers
- D. Graphs without explanations

Q5. single

A draft communication about a public tender is ready for publication. What review step should you prioritize?

- A. Legal and factual validation by the procurement and PR departments
- B. Approval by whoever is available
- C. Automatic translation without review
- D. Upload immediately to save time

Q6. multi-select

Your institution is launching a public consultation on digital services. Which elements make it effective and credible?

- A. Publish clear questions in plain language.
- B. Summarize results transparently and indicate next steps.
- C. Ensure that all interested stakeholders have an opportunity to participate and provide feedback.
- D. Notify contributors of the consultation outcome.

Q7. multi-select

Staff use different online channels for citizen messages (Facebook, website, WhatsApp). What ensures coherent and ethical communication?

- A. Adopt a unified protocol for response tone and privacy
- B. Store and log conversations in the official record
- C. Train staff on GDPR and citizen engagement
- D. Allow staff to reply from personal devices if urgent

A3. Digital content and digital public services

Level A

Q1. single

Your institution must post a slide announcing the new online payment service. What is the best headline?

- A. "Pay online – quick, secure and available 24/7"
- B. "Conformably with the applicable provisions"
- C. "Citizens are kindly requested to consider the stipulations hereunder"
- D. "A technical update of the information system"

Q2. single

Before preparing a short public presentation on e-services, what should you do first?

- A. Identify the audience, key message, and examples relevant to citizens, then design 3-5 clear slides
- B. Fill every slide with detailed legal articles
- C. Add animations and emojis to make it attractive
- D. Write all text in small font to save space

Q3. single

You must quote an EU regulation in a slide. Where should the hyperlink lead?

- A. To the official EUR-Lex page for that regulation
- B. To your manager's blog post summarizing it
- C. To a photo of the document posted it on Wikipedia
- D. To an informal discussion thread where the Commissioner offered a comment

Q4. single

To make a presentation readable on mobile devices, you should:

- A. Use short sentences, large text, and one idea per slide
- B. Include long paragraphs and dense tables
- C. Add small footnotes on each slide
- D. Use complex color gradients and animations

Q5. single

Before uploading a presentation to your institution's portal, what technical step is essential?

- A. Use the institutional template, check accessibility tags, and export to PDF with metadata
- B. Upload as images only
- C. Compress without checking fonts or tags
- D. Skip review to save time

Q6. single

When creating the cover page for a formal report in digital format, what elements must appear?

- A. Title, version/date, author or contact, and official logo or reference source
- B. Only a decorative photo
- C. A motivational quote
- D. A background with the official logo, for simplicity

Q7. multi-select

Your department needs to summarize a 20-page technical note for citizens. What combination of steps ensures accessibility and credibility?

- A. Extract key actions and explain them in plain language.
- B. Link to the full document on the institutional website.
- C. Add visual cues (icons or diagrams) where appropriate.
- D. Shorten the text by removing references entirely.

Q8. single

Before citing a Romanian law, where do you verify the text?

- A. legislatie.just.ro or monitoruloficial.ro
- B. the official website of a reputable news journal
- C. the institutional chatroom, where conversations were made on the topic
- D. the personal blog of your distinguished former professor of public law

Q9. single

Which practice shows respect for readers in digital documents?

- A. Use plain language, clear structure, and citations to sources
- B. Use legal jargon and acronyms without explaining them
- C. Hide the source of data
- D. Replace current facts with older ones from similar cases

Level B

Q1. multi-select

Before publishing an open dataset on *data.gov.ro*, what ensures it creates public value?

- A. Data is complete, anonymized, and updated
- B. Metadata clearly indicates the source and licensing terms
- C. The dataset responds to an institutional need
- D. The dataset contains all internal data for maximum openness

Q2. single

You are reviewing content from multiple agencies for inclusion on your ministry's website. What ensures consistency and reliability?

- A. Use a shared editorial template and verify each dataset or document with its original source institution
- B. Edit all texts to match your institution's writing style
- C. Merge documents without citing their source, as everyone knows where the data comes from
- D. Publish all content immediately to show professionalism

Q3. multi-select

A local administration wants to reuse datasets from the Ministry of Finance for a dashboard on public spending. Which steps guarantee accuracy and compliance?

- A. Verify update frequency and compare data with official reports
- B. Cite the original dataset and include last update date
- C. Use only aggregated values if data contain personal identifiers
- D. Remove source references to simplify the display

Q4. single

Your team is designing an internal knowledge database using materials from previous EU projects. What should be verified first?

- A. That materials are still relevant, rights of use are clear, and outdated content is marked as archived
- B. That all materials look modern and use the official log
- C. That every file has the same format, regardless of content
- D. That only internal staff can view them

Q5. single

You are asked to align your institution's reports with the EU's *Digital Compass* indicators. What demonstrates analytical understanding?

- A. Map national progress using verified metrics and explain any deviations from EU averages
- B. Copy figures from the EU report without explanation
- C. Use data from previous EU reports
- D. Ignore EU indicators because they differ in method

Q6. single

A public institution publishes an interactive dashboard on public spending. What ensures sustainable content management?

- A. Regular data updates, transparent methodology, and user feedback collection
- B. Static charts created once per year
- C. Removing old data to simplify presentation
- D. Allowing only the IT department to edit content

Q7. multi-select

When preparing a multi-source report for the Court of Accounts, what ensures coherence and credibility?

- A. Use consistent definitions across datasets
- B. Briefly summarize the main data processing steps in the report body.
- C. Keep evidence of data provenance and verification
- D. Harmonize numbers manually to ensure alignment

Q8. single

Your institution shares training materials online. What practice best supports responsible reuse?

- A. Publish under a Creative Commons license, include author credit, and ensure accessibility standards
- B. Keep materials private to avoid misuse
- C. Allow free download without stating any license
- D. Post scanned PDFs without text recognition

A4. Safe, responsible and sustainable use of resources

Level A

Q1. multi-select

You are completing a mandatory online course on the INA platform. What shows responsible digital behaviour?

- A. Use your institutional account instead of a personal one
- B. Log in only from secure, trusted devices
- C. Save course materials in a secure institutional folder
- D. Share screenshots of test questions with colleagues

Q2. multi-select

You receive an email claiming to offer “exclusive public administration e-learning content.” What’s the correct reaction?

- A. Check the sender’s domain and avoid clicking unknown links
- B. Report the message to the IT or security team
- C. Verify if the offer is listed on an official training website
- D. Download the attachments immediately to review them

Q3. multi-select

You’re asked to join an online training course via Zoom. What shows awareness of digital safety?

- A. Join through the official institutional link
- B. Avoid sharing the meeting ID publicly
- C. Enable camera and mic only when needed
- D. Record and share the session on social media

Q4. multi-select

Your department encourages staff to learn using open digital platforms (Coursera, etc.). Which practices ensure safe and ethical participation?

- A. Avoid downloading files or clicking on links from unverified sources in course forums
- B. Regularly update passwords used for online learning accounts
- C. Log out of shared or public computers after accessing course materials
- D. Post internal examples from your job in public course forums

Q5. multi-select

You attend an online training session organized by the National Institute of Administration. Which actions demonstrate digital etiquette and safety?

- A. Mute your microphone when not speaking
- B. Avoid sharing your screen without permission
- C. Use your full name and institutional email for registration
- D. Download every link shared in the chat automatically

Q6. multi-select

A colleague asks you to send sensitive information by personal email because the institutional server is “slow.” How do you handle this responsibly?

- A. Decline politely and use only institutional channels
- B. Explain the data protection policy briefly
- C. Suggest using the secure institutional platform and offer to help troubleshoot access issues
- D. Send files via WhatsApp to speed things up

Q7. multi-select

You’re part of a WhatsApp group for a professional course. Which practices show responsible digital participation?

- A. Keep discussions related to course topics only

- B. Avoid sharing internal institutional files
- C. Respect privacy and avoid saving participants' phone numbers without consent
- D. Share personal information to show respect and maintain engagement

Q8. multi-select

You're using an online collaboration platform (Google Drive or MS Teams) for a group project. How can you ensure safe and efficient teamwork?

- A. Assign file access levels (viewer, editor) based on roles
- B. Avoid editing shared documents offline to prevent version loss
- C. Keep sensitive data in secure folders with limited access
- D. Rename files frequently to keep them safe

Q9. single

Which of the following is a common wellbeing risk associated with prolonged digital device use at work?

- A. Improved sleep patterns from screen time
- B. Techno-stress leading to anxiety and burnout
- C. Enhanced self-perception from constant online feedback
- D. Reduced risk of cyberbullying in professional emails

Q10. multi-select

Which are signs of digital dependency or wellbeing threats from work-related technology use?

- A. Frequent headaches or eye strain from poor posture at a desk
- B. Difficulty disconnecting from work emails after hours affecting sleep
- C. Receiving harassing messages from colleagues online (cyberbullying)
- D. Using a standing desk to improve productivity

Level B

Q1. multi-select

Your organization is adopting new software tools to manage digital documents and communication. Which actions promote safe, responsible, and sustainable use of these resources?

Assign access rights based on job roles and responsibilities.

Store confidential documents in secure, access-controlled folders.

Regularly review and update permissions to remove unnecessary access.

Download and print documents unnecessarily to ensure availability offline.

Q2. multi-select

While participating in an e-learning course, you receive a pop-up asking you to install a "security plug-in." What demonstrates informed digital behaviour?

- A. Verify the plug-in's legitimacy with the IT department
- B. Check the platform's official update log
- C. Install only after institutional IT approval
- D. Ignore the alert and continue the lesson

Q3. multi-select

Your department wants to reuse videos from previous training courses. How can you ensure ethical and sustainable reuse?

- A. Confirm copyright and licensing conditions
- B. Update content to reflect current legislation or tools
- C. Compress file sizes responsibly to reduce storage costs
- D. Post them publicly without checking authors' consent

Q4. multi-select

During an online workshop, a participant accidentally shares sensitive internal data on screen. What steps maintain digital ethics and trust?

- A. Pause the meeting and remind everyone about confidentiality
- B. Delete any recorded segment containing that data
- C. Review and update meeting protocols to prevent future incidents
- D. Ignore the incident if few people noticed

Q5. multi-select

A ministry wants to promote "green digital behaviour" among staff. Which practices contribute most to digital sustainability?

- A. Choose energy-efficient devices and settings for workstations
- B. Encourage use of shared institutional drives instead of duplicate storage
- C. Recycle or repurpose old devices securely
- D. Store all files locally to ensure faster access

Q6. multi-select

Your institution is testing a new AI-based assistant for internal use. What ensures its ethical and responsible use?

- A. Verify that the assistant uses only non-sensitive institutional data
- B. Include a disclaimer about AI-generated content and human verification
- C. Review outputs for bias or factual inaccuracy
- D. Allow the assistant to access staff files to "personalize" results.

Q7. multi-select

A colleague suggests saving training materials on a free cloud service. Which actions reflect good digital governance?

- A. Confirm that the service complies with institutional security standards
- B. Request approval from IT or data-protection staff before uploading
- C. Review the cloud service's privacy policy and terms of use
- D. Use the service immediately if it's faster to access

Q8. multi-select

You are preparing documentation for a collaborative project that will be shared externally. Which practices help ensure compliance with data governance and support ongoing accessibility??

- A. Remove personal data before uploading public files
- B. Organize materials with clear naming and versioning rules
- C. Store metadata about content source and license
- D. Save all materials in local folders for each team member

Q9. multi-select

A cybersecurity awareness campaign is launched in your organisation. What measures best support a lasting culture of digital safety?

- A. Include real-life examples of incidents (e.g., phishing, ransomware)
- B. Reinforce safe behaviour through regular micro-learning sessions
- C. Encourage peer reporting of suspicious digital activities
- D. Rely solely on posters and emails to convey digital safety messages

Q10. multi-select

Your department must dispose of 50 outdated laptops. Which actions demonstrate responsible and sustainable management?

- A. Wipe all data using approved deletion protocols
- B. Donate or recycle equipment through certified channels
- C. Record serial numbers and disposal certificates
- D. Discard devices as standard office waste

A5. Problem-solving through digital tools

Level A

Q1. single

You must learn to use a new scheduling tool but have limited time this week. What's a smart learning approach?

- A. Watch a 10-minute tutorial and try some practical tasks immediately after
- B. Enroll in a full-week advanced course
- C. Read promotional materials about the tool
- D. Wait until your supervisor forces training

Q2. multi-select

Your department introduces a new module for reporting. Which actions help you adapt efficiently and safely?

- A. Follow the user manual and complete at least two test reports
- B. Ask the IT support team for feedback on accuracy
- C. Save your credentials securely
- D. Share screenshots with colleagues to compare answers.

Q3. single

Your team is onboarding a new app for internal reporting. Which step belongs in the first two weeks?

- A. Install the app, complete test reports, and schedule a short feedback session
- B. Create a user-friendly interface
- C. Delay testing until you receive information about it from another public institution
- D. Wait for the IT audit as you do not have competencies on that

Q4. multi-select

You need to prepare a short training session on the new *ROeID* login process. Which steps ensure effective peer learning?

- A. Demonstrate login safely without revealing credentials
- B. Explain the security benefits of single sign-on
- C. Include examples of password misuse to avoid repeating mistakes

D. Distribute screenshots containing personal data

Q5. single

You are writing a one-page plan to learn the new eForms module used for procurement. What improves learning?

- A. Practice each step of the eForms module with sample data
- B. Watch a long webinar without practice
- C. Read the regulation only
- D. Change interface colors

Q6. multi-select

Good digital etiquette during new tool adoption includes:

- A. Use clear, respectful questions when seeking help
- B. Share tips that helped you
- C. Record recurring issues to support updates
- D. Hide mistakes instead of reporting them

Q7. single

You must demonstrate that a micro course improved your efficiency. What's the simplest proof?

- A. A task completed faster or with fewer errors, described briefly in a note
- B. The training poster
- C. A photo with the other participants
- D. A long self-assessment with no evidence

Level B

Q1. multi-select

You are asked to lead a small "digital improvement task force" in your ministry. Which steps show both leadership and strategic thinking?

- A. Identify one measurable process to digitize fully within a limited time frame
- B. Involve users from two departments to test the prototype
- C. Focus only on purchasing new software
- D. Avoid documenting results until the project is finished

Q2. multi-select

During an internal skills audit, you find that staff use outdated reporting templates. Which combination of actions creates sustainable improvement?

- A. Update templates to align with the latest eForms version
- B. Provide a short tutorial and feedback session
- C. Replace the templates without consulting end users
- D. Post the new format on intranet with no guidance

Q3. multi-select

A central institution uses several digital tools that do not "talk" to each other. What is the best immediate solution before requesting a new platform?

- A. Map workflows and data overlaps to identify bottlenecks
- B. Check whether existing APIs or integration features can be activated
- C. Request a full software replacement immediately

D. Allow each department to keep separate databases indefinitely

Q4. multi-select

Your institution uses an AI tool to classify citizen requests. What steps ensure accountability and transparency?

- A. Document algorithm logic and decision criteria
- B. Allow human review of flagged cases
- C. Publish basic information about how the system works
- D. Hide details to protect the institution from criticism

Q5. multi-select

A manager wants to purchase multiple digital tools for similar tasks. What approach ensures sustainable investment?

- A. Evaluate overlapping functionalities before purchase
- B. Choose interoperable tools that share data securely
- C. Pilot solutions before institutional rollout
- D. Approve all purchases to encourage innovation

Q6. single

When your standard software for editing PDFs is unavailable due to a network issue, which alternative would you apply to complete the task?

- A. Wait until the software is fixed
- B. Use a free online PDF editor via your browser
- C. Scan the document with your phone's camera app and convert it using a built-in tool
- D. Print and manually edit the document

Q7. single

When reporting a complex hardware issue like a malfunctioning printer to IT support, which elements should you include in your documentation for efficient resolution?

- A. Only the error code
- B. Context of when it occurred, screenshots of the error, and steps tried so far
- C. A general description without visuals
- D. Wait for IT to ask for details

A6. Digital transformation in public administration

Level A

Q1. single

Your institution introduces a new online permit application through *ghiseul.ro*. What outcome best reflects digital transformation, not just digitization?

- A. Citizens can apply, pay, and track approvals fully online without visiting the office
- B. Citizens fill out forms online but must print and deliver them in person

- C. Staff receive applications by email and process them manually
- D. The website displays downloadable forms

Q2. single

The National Authority for Digitalization promotes the Governamental Cloud. Why is this significant for public institutions?

- A. It allows secure, standardized data exchange between institutions, reducing duplication and costs
- B. It requires all staff to learn coding
- C. It focuses mainly on buying new servers.
- D. It aims to reduce transparency in data sharing

Q3. multi-select

Your manager asks why your office should adopt digital signatures. Which arguments show understanding of the benefits?

- A. Legal recognition equivalent to handwritten signatures
- B. Faster workflow and reduced paper usage
- C. Enhanced traceability and security
- D. Increased administrative burden compared to paper

Q4. single

The institution considers implementing a chatbot for citizen inquiries. What is the first step before implementation?

- A. Identify the most frequent questions and test answers for clarity and accuracy
- B. Purchase the software immediately
- C. Replace all human interactions with automation
- D. Use generic content without verifying accuracy

Q5. single

A training session introduces “public value through digital tools.” Which statement best illustrates this concept?

- A. Digital tools improve access, fairness, and transparency for citizens
- B. Digital tools serve primarily to cut costs
- C. Digital tools replace staff decisions entirely
- D. Digital tools focus only on aesthetics and design

Q6. multi-select

When planning a small digital reform, what ensures sustainability?

- A. Clear objectives linked to citizen outcomes
- B. Staff involvement from design to evaluation
- C. Public communication of progress and feedback
- D. Frequent tool changes to show innovation.

Q7. single

A central institution adopts an app for reporting service issues. What demonstrates proper monitoring of digital services?

- A. Regularly reviewing response times and publishing reports on solved cases
- B. Focusing only on collecting user email addresses without assessing service performance
- C. Promoting the app on social media without evaluating impact

D. Limiting the app's use to IT staff only

Q8. multi-select

An institution collects data from several digital systems. What ensures responsible use of data?

- A. Use data only for the declared administrative purpose
- B. Apply anonymization where personal data is involved
- C. Keep documentation on data sources and update frequency
- D. Share all data publicly for transparency

Q9. single

When evaluating the need for new digital tools, which principle comes first?

- A. Start from citizen or user needs, not from available technologies
- B. Choose the newest tool to appear innovative
- C. Adopt what neighboring institutions use
- D. Focus only on tools that have already been purchased

Q10. single

Your institution joins a national digitalization project externally funded. Which contribution ensures long-term institutional benefit?

- A. Align project goals with existing processes and ensure post-project maintenance capacity
- B. Focus only on spending the full budget as on the timeline
- C. Depend entirely on external consultants
- D. Limit staff participation to technical teams only

Q11. single

If you identify a need to enhance your digital competency in online collaboration, which learning opportunity would you engage with first?

- A. Ignore it until mandatory
- B. Enroll in a free self-paced online course offered by INA or partner institution
- C. Attend a peer learning workshop with colleagues
- D. Read a general book unrelated to work

Level B

Q1. multi-select

Your ministry plans to automate several back-office processes. Which combination of measures ensures responsible implementation?

- A. Assess potential ethical and social impacts before rollout
- B. Involve end-users and staff in design and testing
- C. Establish monitoring indicators for transparency and performance
- D. Replace all manual processes without review

Q2. multi-select

A local authority wants to use AI to prioritize citizen requests. What should leadership guarantee before approval?

- A. Clear, explainable criteria for algorithmic decisions
- B. Oversight mechanisms to detect bias or discrimination
- C. Compliance with GDPR and data protection principles

D. Full automation without human verification

Q3. multi-select

Your institution joins an inter-ministerial initiative on data-driven policymaking. Which governance practice ensures sustainable collaboration?

- A. Agree on shared data standards and access rules
- B. Establish joint accountability for data quality
- C. Use evidence-based dashboards for decision-making
- D. Keep each ministry's data isolated for security

Q4. single

An evaluation of the digital transformation strategy shows uneven progress across departments. What is the most effective leadership response?

- A. Facilitate peer learning sessions and identify structural barriers before adjusting the strategy
- B. Attribute results solely to individual managers
- C. Suspend digital projects until parity is achieved
- D. Redefine KPIs to make results appear uniform

Q5. multi-select

You are asked to present your institution's digital transformation achievements to the National Authority for Digitalization. Which evidence demonstrates real impact?

- A. Reduction in service delivery time or cost verified by data
- B. Improved citizen satisfaction or accessibility indicators
- C. Increased staff digital confidence and reuse of solutions
- D. Number of meetings held about digitalization

Q6. multi-select

A project team proposes outsourcing the management of citizen data to a private vendor. What should be verified before proceeding?

- A. Contractual clauses on data ownership and long-term access
- B. Vendor compliance with national and EU data protection rules
- C. Existence of an internal capacity to supervise the process
- D. Vendor's popularity or marketing reputation

Q7. multi-select

A digital reform project faces resistance from specific institutions. What the best strategy be to foster collaboration?

- A. Co-design solutions with pilot institutions before full rollout
- B. Offer targeted technical and administrative support
- C. Communicate the benefits in terms of citizen outcomes
- D. Enforce adoption through sanctions only

Q8. multi-select

When evaluating the success of digital transformation, which indicators reflect *value creation* rather than *activity*?

- A. Time saved for citizens and institutions
- B. Quality of interinstitutional data exchange
- C. Evidence of improved policy outcomes

D. Number of software licenses purchased

Answers

A1 Digital Literacy			
Level A		Level B	
Q1	A	Q1	A
Q2	A, B	Q2	A
Q3	A	Q3	A, B, C
Q4	A	Q4	A, B
Q5	A, B, C	Q5	A
Q6	A	Q6	A, B
Q7	A, B, D		
Q8	A		
A2. Digital communication and collaboration			
Level A		Level B	
Q1	A	Q1	A
Q2	A, B, C	Q2	A, B, C, D
Q3	A	Q3	A
Q4	A, B, C	Q4	A
Q5	A, B, C	Q5	A
Q6	A	Q6	A, B, C, D
Q7	A	Q7	A, B, C
Q8	A, B, C		
Q9	A		
Q10	A		
Q11	A		
Q12	A		
Q13	A		
A3. Digital content and digital public services			
Level A		Level B	
Q1	A	Q1	A, B, C
Q2	A	Q2	A
Q3	A	Q3	A, B, C
Q4	A	Q4	A
Q5	A	Q5	A
Q6	A	Q6	A
Q7	A, B, C	Q7	A, B, C
Q8	A	Q8	A
Q9	A		
A4. Safe, responsible and sustainable use of resources			
Level A		Level B	
Q1	A, B, C	Q1	A, B, C
Q2	A, B, C	Q2	A, B, C
Q3	A, B, C	Q3	A, B, C

Q4	A, B, C	Q4	A, B, C
Q5	A, B, C	Q5	A, B, C
Q6	A, B, C	Q6	A, B, C
Q7	A, B, C	Q7	A, B, C
Q8	A, B, C	Q8	A, B, C
Q9	B	Q9	A, B, C
Q10	A, B, C	Q10	A, B, C
A5. Problem-solving through digital tools			
Level A		Level B	
Q1	A	Q1	A, B
Q2	A, B, C	Q2	A, B
Q3	A	Q3	A, B
Q4	A, B, C	Q4	A, B, C
Q5	A	Q5	A, B, C
Q6	A, B, C	Q6	C
Q7	A	Q7	B
A6. Digital transformation in public administration			
Level A		Level B	
Q1	A	Q1	A, B, C
Q2	A	Q2	A, B, C
Q3	A, B, C	Q3	A, B, C
Q4	A	Q4	A
Q5	A	Q5	A, B, C
Q6	A, B, C	Q6	A, B, C
Q7	A	Q7	A, B, C
Q8	A, B, C	Q8	A, B, C
Q9	A		
Q10	A		
Q11	B		