

Report on the proposed ICT roles and functions for the Romanian central public administration - based on the eCF -

Connected report accompanying *Output 2* under the TSI project

Technical Support Instrument

Supporting reforms in 27 Member States

TSI component “Romania: Developing a General Digital Competence Framework for Civil Servants”

Disclaimer

This technical report was prepared under the Technical Support Instrument (TSI) component “*Romania: Developing a General Digital Competence Framework for Civil Servants*”, but it is not an official deliverable. Hence, it was developed and provided for informational purposes only and has not undergone internal quality review by the World Bank. It is intended to provide information and should not be treated as a recommendation or endorsement by the World Bank. The findings, interpretations, and conclusions expressed in this report are those of the authors and do not necessarily reflect the views of the World Bank, its Board of Executive Directors, or the governments they represent.

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 Miheș (Senior Public Sector Specialist) and Fanny Weiner (Senior Public Sector Specialist).

The development of this report was led by Marius Dorian Nicolăescu (Senior Public Sector Digitalization Expert), Cătălin Tudor (Professor, Academy of Economic Studies) and Anca Butnaru (Senior Public Sector Expert).

Key inputs were also provided by: Mogens Andersen (Lead International Digitalization Expert), Sabin Chiricescu (Senior Digitalization Expert), Igor Bercu (Senior Digitalization Expert), George Varga (Senior IT Assistant), Dimitrie Miheș (Senior Public Sector Specialist) and Oxana Cașu (Senior Digitalization Expert).

Fanny Weiner (Senior Public Sector Specialist) and Vlad Manoil (Senior Digitalization Specialist) provided valuable insights as peer reviewers.

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

The 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 (Secretary General) 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.

The report also reflects the results of a design process that relied on the close collaboration with the *IT Working Group* consisting of IT experts from the central public administration in Romania. This group was constituted to support the development of various outputs under the TSI project.

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).

Table of contents

1. Introduction	7
1.1. Context of the report	7
1.2. Scope of the report	9
1.3. Rationale for introducing specialized ICT roles in the Romanian public administration job classification system	11
2. Methodological approach and design process	13
3. Proposed classification of ICT roles for the Romanian public administration	16
3.1. Conceptual differentiation between ICT job and ICT role	16
3.2. Proposed list of ICT roles for the Romanian public administration	19
3.3. A public administration reality: allowing ICT role overlap while determining the dominant role.....	24
3.4. Correlation of ICT roles allocation with organization size and complexity of ICT systems	28
4. Proposed classification of ICT jobs	33
5. Proposed levels of responsibility for ICT jobs	40
6. Methodology for mapping ICT jobs and proposing salary levels	43
7. Methodology for mapping ICT roles and ICT jobs to public institutions needs	44
8. Relevance of ICT roles based on the pilot exercise	46
9. At the intersection between general digital competencies and ICT roles: a digital transformation coordinator.....	49
10. Options for implementation of the proposed ICT roles and ICT job classification	51
10.1. Option 1: Centralized expertise model	52
10.2. Option 2: Federated expertise model	53
10.3. Option 3: Hybrid approach	54
11. Recommendations and roadmap for implementation	55
Annex 1 Proposed ICT roles for the Romanian public administration (based on e-CF) and proposed levels of responsibility – for execution-level and managerial level jobs	59
Annex 2 Mapping of competencies and overlapping competences across the proposed ICT roles.....	61
Annex 3. Proposed ICT Roles description, competencies and levels (first 10 more used roles)	71
Annex 4 List of ICT system categories	107
Annex 5 Summary table of ICT systems types.....	109
Annex 6 Proposed methodology for determining the ranking of IT jobs and salary levels.....	111

Figures

Figure 1. EU countries ranked by DESI results for Digital public services for citizens (left) and businesses (right), 2024	7
Figure 2 TSI project intervention logic: Interim Note corresponds to Activity 2, complementing the proposed general digital competency framework	10
Figure 3 Correlation of assessment and design outputs under the TSI project.....	11
Figure 4. The 30 e-CF ICT Professional role profiles	17
Figure 5. Correlation between job and role for ICT specialists	18

Tables

Table 1 ICT Roles for the Romanian public administration.....	20
Table 2 New roles proposed and associated with e-CF competencies	21
Table 3 Roles and associated competencies for System Administrator and Developer	26
Table 4 Examples of dominant roles and other compatible roles	27
Table 5 Proposed classification of public institutions for the purpose of ICT roles allocation.....	28
Table 6 ICT roles by institution size and ICT system complexity	30
Table 7 Proposed roles allocation and role mission per institution size and systems.....	31
Table 8 The ICT job classification system in Austria, federal public service contract-based jobs ...	35
Table 9 Proposed correspondence between ICT job classification and ICT roles.	38
Table 10 Proposed table of correspondence between proposed ICT roles and ICT job classification	38
Table 11 Proposed levels of responsibility for ICT jobs based on SFIA.....	41
Table 12 Matrix category of ICT unit/department and proposed categories of ICT systems	42
Table 13 Matrix category of ICT unit/department and proposed categories of ICT systems	42
Table 14 Proposed phased implementation roadmap.....	56
Table 15 Matrix proposed ICT roles for Romania PA and proposed levels of responsibility for execution positions.....	59
Table 16 Matrix proposed ICT roles for the Romanian public administration PA and proposed levels of responsibility for managerial positions.....	60
Table 17 Correspondence between proposed ICT job classification, professional grades and SFIA levels of responsibility.....	111
Table 18 ICT system type, SFIA levels and coefficient of ICT system complexity.....	111
Table 19 Job ranking coefficients linked to ICT jobs, professional grades, depending on types of institutions and ICT systems.....	112
Table 20 Proposed ICT job importance coefficients	113
Table 21 Determining job ranking coefficients for ICT jobs	113
Table 22 Proposed matrix for determining ICT job salary matrix.....	115

Acronyms

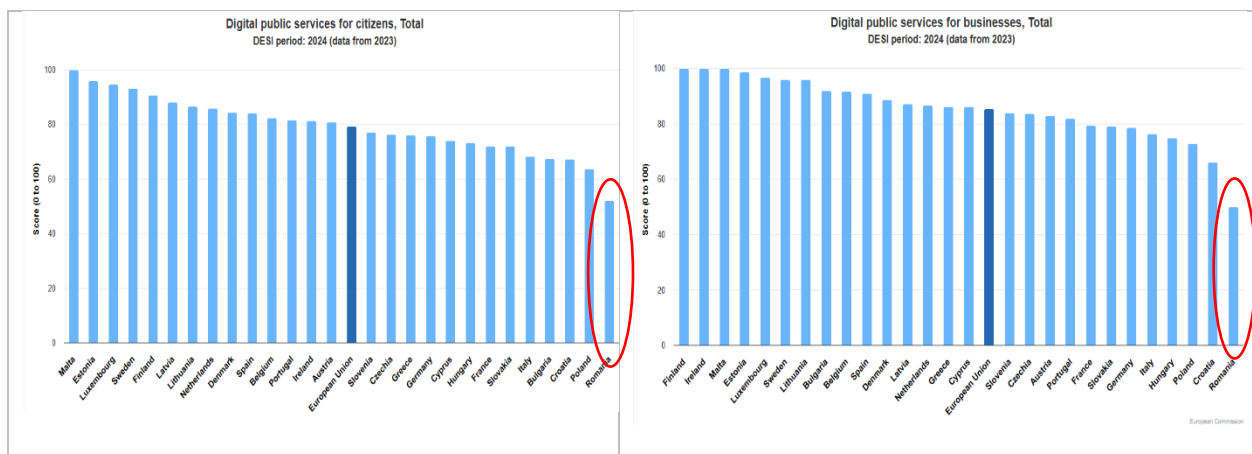
ADR	Authority for Digitalization of Romania
BCP	Business Continuity Plan
BR	Business Recovery
CAD	Codice dell'Amministrazione Digitale (Italian Digital Administration Code)
CDDO	Central Digital and Data Office (United Kingdom)
CDO	Chief Data Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
DESI	Digital Economy and Society Index
DNCS	National Directorate for Cyber Security (Romania)
ECSF	European Cybersecurity Skills Framework
e-CF	European e-Competence Framework
ESCO	European Skills, Competences, Qualifications and Occupations
EU	European Union
GDS	Government Digital Service (United Kingdom)
ICT	Information and Communication Technology
INA	National Institute of Administration
JRC	Joint Research Centre (European Commission)
MEDET	Ministry of Economy, Digitalization, Entrepreneurship and Tourism
MLFYSS	Ministry of Labor, Family, Youth and Social Solidarity
MoF	Ministry of Finance
MoI	Ministry of Internal Affairs
NACS	National Agency for Civil Servants
NRRP	National Recovery and Resilience Plan
RAS	Reimbursable Advisory Services (World Bank instrument)
RTD	Responsabile della Transizione Digitale (Italy – Digital Transition Officer)
SaaS	Software as a Service
SFIA	Skills Framework for the Information Age
SGG	General Secretariat of the Government
SLA	Service Level Agreement
TSI	Technical Support Instrument

1.Introduction

1.1. Context of the report

1. **The role of ICT professionals in Romania's public administration is a key determinant factor for the country's digital transformation ambitions.** The digital transformation of Romania's public administration is advancing rapidly, driven by EU policy objectives, national strategic commitments, and citizen demand for efficient, transparent services. However, digital transformation in Romania is still lagging behind, with Romania consistently placed below EU peers in the digitalization of public services according to the Digital Economy and Society Index (DESI) data (Figure 1). This gap underlines that progress will not come from technology investments alone, but from building the right internal capacity. To support digital transformation, a well-defined structure of IT-specialized roles in the public sector is critical to ensure effective design, deployment, and management of digital public services. ICT roles in government are therefore not just about maintaining systems; they are essential drivers of innovation, security, and service quality. Data analysts, software engineers, cybersecurity experts, and E-Government Specialists form the backbone of a modern state, enabling administrations to anticipate citizen needs, prevent risks, and continuously improve digital service delivery.

Figure 1. EU countries ranked by DESI results for Digital public services for citizens (left) and businesses (right)¹, 2024



Source: European Commission

2. **In Romania, however, ICT expertise remains a scarce resource in the public administration.** The latest DESI report for Romania² notes that many major digital government projects are now being launched. Their success, however, depends on sustained follow-up. Public institutions need adequate resources - funding, project management capacity, and ICT specialists -

¹ Extracted from https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dps_biz&breakdown=total&unit=egov_score&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE.

² European Commission, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future, Short Country Reports: Romania*. Available at: <https://digital-strategy.ec.europa.eu/ro/factpages/romania-2025-digital-decade-country-report>.

to operate and maintain these systems once initial contracts end. However, while the country benefits from a strong pipeline of certified specialists, few of these professionals choose careers in government. A dedicated analysis of the factors impacting public sector ICT specialists was recently developed by the Bank³, underlining that the main challenge is capacity, not technology and that without sustained investment in digital leadership and in-house teams, Romania risks wasting funds on short-term vendor solutions instead of building lasting institutional capability.

3. **While limited ICT expertise in the public sector is indeed a contributing factor, Romania's digitalization challenges reflect deeper structural and institutional factors.** A significant barrier remains the absence of a coherent governance framework with clearly defined authority, decision-making power, and institutional capacity to drive digital transformation across the whole of government. Equally important is the lack of a unified strategic vision and shared technical standards, which leads to fragmented initiatives, inconsistent implementation, duplication of effort, and limited interoperability among public administration systems. Without addressing these systemic shortcomings, individual efforts to improve technical skills or modernise isolated systems will have limited impact on Romania's overall digital performance.

4. **The role of ICT in Romania's public administration needs to shift from a back-office support function to a strategic pillar of governance and digital transformation.** In Romania's public administration, ICT departments have traditionally been perceived as auxiliary support units, primarily responsible for maintaining infrastructure, providing technical assistance, and ensuring operational continuity. However, the acceleration of digital transformation has redefined their role, and ICT is no longer a background function but a strategic enabler of modern governance, essential for designing, implementing, and scaling digital services that meet the needs of citizens and businesses. This paradigm shifts the positions of ICT structures as central actors in policy making and execution, shaping strategic priorities and promoting institutional innovation. They are now expected to contribute to strategic planning, ensure interoperability across systems, adopt emerging technologies, and uphold standards of cybersecurity and data protection. ICT units transitioned from a reactive service model to a proactive role that drives efficiency, transparency, and citizen-centric service delivery. The transformation of ICT from a support function into a core pillar of public administration reflects the broader shift towards digital government, where technology is not perceived as a tool but an essential component of governance and public value creation.

5. **For this, ICT jobs need to shift from generalist jobs (as currently regulated and implemented across most central institutions) towards clearly structured specialist profiles with specific job titles and clear ICT roles attached, that can also be adequately linked to more competitive wages.** This approach would help not only to professionalize the ICT function, but it would also make public sector ICT jobs more attractive to skilled specialists from the private sector.

6. To be effective, the introduction of a new ICT role classification needs to be accompanied by human resources measures to attract and retain qualified talent in the public sector. Classification alone will not address the competitiveness gap with the private sector unless targeted incentives and flexible HR instruments are used to complement it. As highlighted in *Deliverable 8*:

³ World Bank, *Report with recommendations for attracting and retaining ICT staff in the public sector*, delivered in June 2025 under the Reimbursable Advisory Services (RAS) Agreement on Advice to Develop the Government Cloud Platform and to Migrate Selected Public Digital Services to the Cloud (P180766).

*Recommendations for Attracting and Retaining IT Staff in the Public Sector*⁴, these measures should include differentiated salary scales for specialised ICT skills, aligned with market realities. In addition, recruitment processes for ICT positions should be streamlined through fast-track procedures, simplified competitions, or the use of fixed-term expert contracts, enabling institutions to respond more rapidly to critical skills shortages. Non-monetary incentives, such as opportunities for continuous professional development, access to cutting-edge technologies, flexible working arrangements, and clear career progression paths, are equally important for enhancing the attractiveness and sustainability of ICT careers in public administration.

1.2. Scope of the report

7. **This Connected Report on the proposed ICT roles for the Romanian public administration accompanies the official Output 2 delivered under the Technical Support Instrument (TSI) component “Developing a General Digital Competency Framework for Civil Servants in Romania.”** The project supports the National Agency for Civil Servants (NACS), the National Authority for Digitalization of Romania (ADR) and the National Institute of Administration (INA) by developing a proposed framework of digital competencies and recommendations for operationalization. While **Output 2** presents the proposed general digital competency framework applicable across the civil service, this *Connected Report* provides the dedicated analysis and proposals related specifically to specialized ICT roles, including a job classification system – elements that fall outside the scope of the general digital competency framework proposed. In this architecture, the present Connected Report completes the overall model by detailing the potential solutions for developing a specialized ICT workforce in the public administration, ensuring coherence between general digital competencies applicable to all civil servants and the technical, role-specific competencies required to support digital service delivery and system management across institutions.

8. **ICT jobs require specialized digital competencies that go beyond the general digital skills applicable to all civil servants.** Given the strategic importance of ICT roles in modern public administration, the assessments conducted under the TSI project⁵ demonstrated that it was not sufficient to treat these positions merely as illustrative examples of how role-specific competencies could be defined within the general digital competency framework. Instead, the evidence highlighted the need to advance a comprehensive and structured classification of ICT roles themselves, capable of supporting recruitment, career management, remuneration, and targeted professional development.

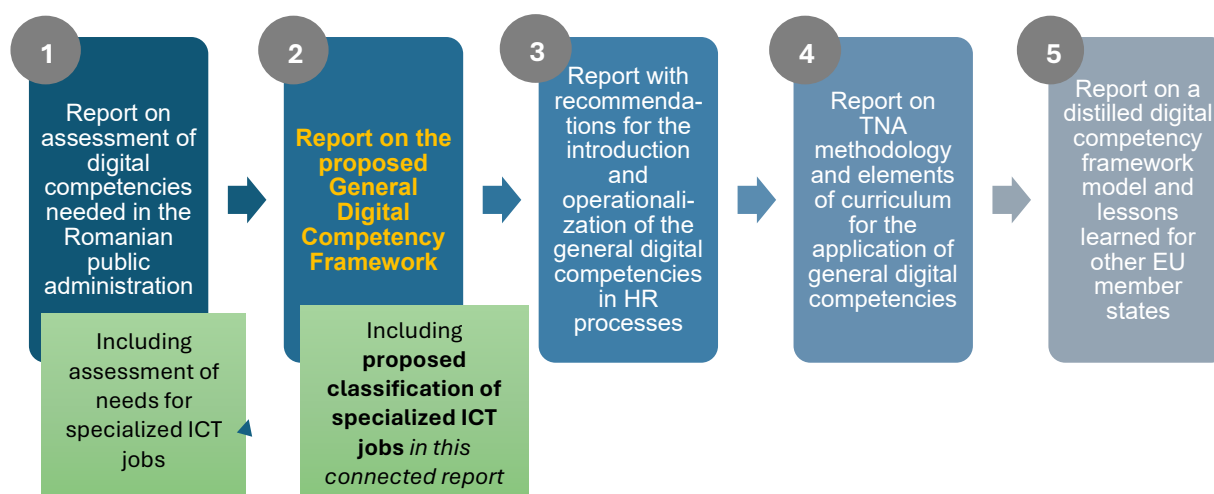
9. **For this reason, a stand-alone *Connected Report* was developed alongside Output 2 to provide the necessary analytical depth and technical justification for a fully-fledged proposal on ICT role and job classification within the Romanian public administration.** This dedicated approach enabled detailed job analysis, alignment with international ICT competency and

⁴ Developed By the World Bank under Reimbursable Advisory Services Agreement on Advice to develop the Government Cloud Platform and to migrate selected public digital services to the Cloud (P180766).

⁵ 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 Developing a General Digital Competency Framework for the Romanian civil service, 2025. Available at: <https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745>.

classification frameworks, and the formulation of differentiated profiles and career pathways, which cannot be adequately captured within a general competency model. The Connected Report therefore complements the general digital competency framework by addressing the distinct workforce segment responsible for designing, maintaining, and governing digital systems, ensuring coherence between broad civil service digital upskilling and the professionalization of Romania's public-sector ICT workforce.

Figure 2 TSI project intervention logic: Interim Note corresponds to Activity 2, complementing the proposed general digital competency framework



Source: Authors' elaboration

10. **The design of ICT roles and classification of ICT jobs need to be firmly underpinned by evidence on both current and future needs of Romania's public administration.** This evidence base was established under **Output 1⁶** developed under the TSI project. That assessment included a review of relevant international strategic and regulatory frameworks, an analysis of EU and international good practices in structuring ICT functions, an assessment of the national legal and organizational context, as well as a job analysis of existing IT-related tasks across civil service roles. In addition, foresight methods were also applied to anticipate emerging requirements in areas such as cybersecurity, data management, interoperability, and the use of emerging technologies. This ensures that the proposed ICT role structure is not limited to current operational needs but also equips the civil service to meet the demands of digital transformation in the years ahead.

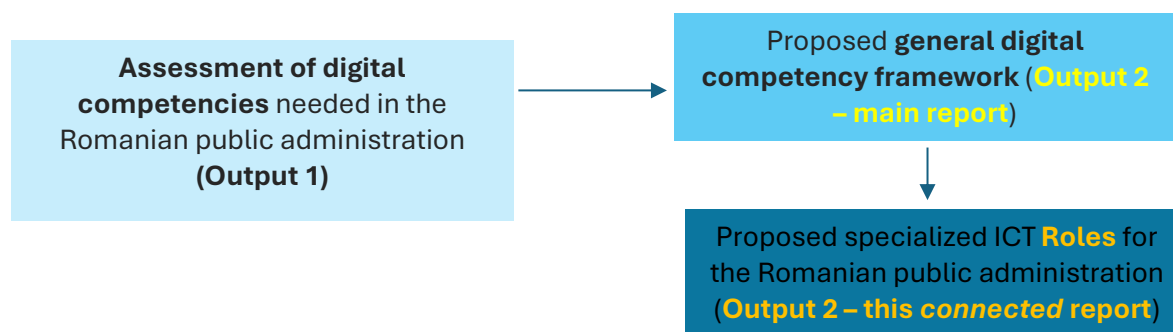
11. **This report proposes a structured framework for specialized ICT roles, developed through dedicated focus groups and in collaboration with the ICT Working Group composed of 10 ICT specialists from the public administration.** The framework offers recommendations for how to structure roles and classify ICT functions in a manner that can support the public sector's

⁶ 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 Developing a General Digital Competency Framework for the Romanian civil service, 2025. Available at: <https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745>.

capacity to develop a modern and resilient digital workforce, capable of delivering secure, user-centric, and interoperable services that align with both current priorities and future demands.

12. **This Connected report on ICT roles complements the main report on the proposed general digital competency framework (Output 2 under the TSI project), focusing on how the specialized ICT roles should be structured.** The proposed general digital competency framework establishes baseline digital skills required across all public servants, whereas the specialized ICT profiles - such as cybersecurity specialists, system developers, E-Government specialists - are essential for designing, implementing, and maintaining digital government services. Together, the two reports create a coherent picture: one ensures that all public employees develop the digital literacy necessary to operate in a modern administration, while the other ensures that roles and jobs are properly designed to allow attracting and retaining highly qualified ICT professionals who can lead and sustain transformation efforts.

Figure 3 Correlation of assessment and design outputs under the TSI project



13. **With the aim to address the key elements needed for the ICT roles classification, this report includes:**

- A proposed structure for the ICT roles tailored to Romania's digital service ecosystem based on institutions' profiles;
- A proposed mapping of ICT roles to an updated job classification for ICT specialists;
- Options for organizational models (centralized, federated, hybrid) for role deployment;
- Options and guidance for role and responsibilities mapping.

14. In addition, the report also outlines a phased roadmap to guide implementation, beginning with role mapping and quick wins, and advancing with a fully professionalized, agile ICT workforce in public administration.

1.3. Rationale for introducing specialized ICT roles in the Romanian public administration job classification system

15. **As outlined in Output 1. Report on the assessment of the digital competencies needed in the Romanian civil service, the current job classification system for the ICT domain remains largely generic.** Jobs are typically designated under broad titles such as "Expert I", "Counsellor", or "Specialist", in line with the national legal framework for civil servants or contract-based staff. While these titles ensure consistency across the administration, they do not convey the specific technical expertise, operational scope, or strategic responsibilities that the digital era demands. As a result,

the system prevents meaningful differentiation and fails to capture the full complexity and diversity of digital roles required in government.

- **The reliance on generic ICT job classifications in Romania's public administration generates several structural challenges, as detailed in Output 1⁷:**
- **Lack of clarity in responsibilities and expectations** - Generic job titles make it difficult to set precise deliverables or link performance to measurable digital outcomes. This hinders both accountability and effective project management.
- **Misalignment with the digital skills market** - In the private sector and international institutions, ICT roles are clearly defined (e.g., *Cybersecurity Analyst, Systems Architect, Business Intelligence Specialist, Data Protection Officer, Cloud Infrastructure Engineer, Digital E-Government specialist, etc.*). Without similar classifications, public administration struggles to attract candidates with up-to-date expertise, as the job profiles do not resonate with professionals' career aspirations or market benchmarks.
- **Challenges in recruitment and retention** - Specialists often perceive these generic positions as undervaluing their qualifications, leading to low interest from highly skilled professionals and high turnover among those hired.
- **Limited opportunities for professional development** - Without well-defined roles, training programs cannot be effectively tailored to the actual skill sets required. This leads to fragmented upskilling efforts and slow adaptation to technological change.
- **Impact on digital transformation** - Ambiguity in roles directly affects Romania's capacity to deliver on strategic e-government objectives, such as interoperable public services, secure digital infrastructure, advanced data analytics for policymaking, AI, and new technologies integration in citizen service delivery. As the digital transformation in the public sector is not just a technical effort, but one of compliance and administrative reengineering, the administration needs e-government experts. They must ensure that digital solutions comply with administrative law principles and state-specific procedural flows, transforming legal requirements into IT technical specifications.

16. Transitioning to specialized ICT role definitions would bring significant benefits for Romania's public administration. First, it would enable strategic workforce planning, as clearly defined roles make it possible to align staffing needs with the government's digital strategy and long-term initiatives. Second, it would generate higher operational efficiency by matching specific competencies to precise technical tasks, reducing duplication of effort and improving project delivery timelines. Third, it would foster better collaboration and cross-agency coordination, since standardized roles across institutions would allow ICT professionals to share expertise, tools, and processes more effectively. This, in turn, would facilitate the creation of cross-sector working groups of ICT specialists, supporting knowledge-sharing, solution reuse, cost reduction, and improved adoption of ICT systems and platforms. Finally, specialized ICT roles would strengthen alignment with EU digital standards, enabling Romania to engage more effectively in cross-border initiatives such as the European Digital Government ecosystem, the Single Digital Gateway, and EU-wide cybersecurity frameworks.

⁷ For more details, please see WB (2025), *Report on the assessment of the digital competencies needed in the Romanian public administration*, available at <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099071725093059745/p506325-5d25a447-aa60-4b9e-aad0-a7193167bc98>.

2. Methodological approach and design process

17. **The proposed ICT roles and ICT job classification framework in this report builds directly on the analytical work conducted under the TSI project under Output 1**, which provided the empirical foundation for both the structure and content of the model. Key features from Output 1 and assessment pillars are briefly mapped in the box below, along with key findings and recommendations.

I. Top-Down legal and strategic mapping

Rationale of the assessment:

- The design of the public administration ICT roles needs to ensure alignment with EU and national policy and legal instruments, including national commitments in the area of digitalization, the National Cybersecurity Strategy, Law 242/2022 on interoperability and other legislation (as mapped under Output 1), ADR digital maturity framework, and institutional strategic plans 2025–2028.

Key findings:

- Specialized technical expertise is required:

IT specialists in Romania’s public administration need advanced competencies to plan, develop, and manage digital infrastructures, protect sensitive data, and implement EU regulatory standards. Specialized technical expertise in the public sector will reduce reliance on external vendors, mitigate vendor lock-in risks, and strengthen sovereign control over critical digital systems and infrastructure. Key domains include cybersecurity, AI development, cloud computing, and big data analytics.

- ICT specialists also have regulatory-driven responsibilities:

EU legislation directly shapes ICT roles. For example: under the Cyber Resilience Act, ICT staff must implement security-by-design principles in software and digital systems; under the Interoperable Europe Act, ICT teams must maintain semantic interoperability standards to enable cross-border data exchange across EU institutions.

- ICT specialists’ roles need to be aligned with EU frameworks:

The e-CF and ECSF frameworks provide structured foundations for defining ICT roles and competencies.

- Differentiation of competencies for ICT specialists:

IT specialists require advanced technical skills distinct from the general digital literacy required of all civil servants, and different again from the policy and leadership skills needed by managers and digital leaders.

- Specialized and emerging areas:

Future ICT roles should encompass expertise in emerging technologies (e.g., blockchain, advanced biometrics, digital twins) and cross-cutting fields like data governance and AI ethics to meet evolving EU and international standards.

II. Bottom-Up institutional assessment

Rationale:

The methodology included a comprehensive mapping of existing ICT functions as captured in the Public Sector Pay Law 153/2017 against the e-CF role profiles. This exercise highlighted both overlaps and gaps, allowing the team to determine which areas could be adapted directly from European standards and which required further customization for Romania's context.

A job analysis exercise was also conducted, covering also relevant ICT jobs from the sample institutions.

To refine this mapping, focus groups and working sessions were held with ICT specialists across central institutions, who assessed coverage of the 41 competence areas defined in e-CF.

Key findings:

- Current coverage of competencies

Institutions currently cover only 30–40% of required ICT competences, with low specialization. Less than half of the 41 e-CF competence areas are present across institutions.

There is heavy reliance on outsourcing for complex tasks (e.g., application design, system architecture), often without in-house capacity to manage vendors. This ad-hoc outsourcing highlights the need for strategic workforce planning to balance internal vs. external resources.

- The e-CF and ECSF provide a comprehensive foundation for defining ICT roles, with detailed skills, responsibilities, and proficiency levels.

A competency-based approach would improve workforce planning, recruitment, and professional development.

Focus groups showed some preference for consolidating all ICT professionals under a broad title like “ICT Specialist”, while still differentiating roles through detailed descriptions.

- Role structuring

Role definitions will use e-CF/ECSF categories, with ESCO occupations and skills as additional references.

Roles should also reflect system complexity and department size, with corresponding levels of responsibility.

Each ICT position should be limited to 3–4 defined roles for clarity and manageability.

- Institutional mandates and governance

A central authority should define, oversee, and monitor ICT roles across institutions, especially for critical systems. Terminology and role assignment should be standardized across the administration.

- Career pathways and retention

Clearly defined career paths, professional certifications, and targeted training are needed for ICT staff.

Salary structures must be revised to remain competitive with the private sector, supporting retention of highly skilled professionals.

III. International Benchmarking

Rationale:

- Drawing the line between general digital competencies and specialized ICT roles should be informed by mature models of ICT roles classification. Beyond eCF and ECSF, a specific classification of ICT roles was analyzed in Output 1: the **Government Digital and Data Profession Capability Framework** from UK.

Key findings:

- The framework in UK encompasses 7 broad role groups (or domains) of digital/data/ICT work:
 - Architecture roles
 - Chief digital & data roles
 - Data roles
 - IT operations roles
 - Product & delivery roles
 - Quality assurance / testing (QAT) roles
 - Software development roles
 - User-centred design roles
- Each role group contains a number of specific roles. For example: in Architecture, roles include Business Architect, Data Architect, Enterprise Architect, Network Architect, Security Architect, Solution Architect, Technical Architect • In Data, roles include Analytics Engineer, Data Analyst, Data Engineer, Data Ethicist, Data Governance Manager, Data Scientist, Machine Learning Engineer, etc.
- The framework is maintained and governed by the Government Digital Service (GDS), working with the Central Digital and Data Office (CDDO). It is also updated regularly to reflect technological advancements, evolving good practices, and feedback from digital professionals across the UK civil service.
- The structure of the framework was recently updated (2025) and can solidly inform similar role and job classifications for ICT specialists.

IV. Foresight exercise on future roles

Rationale:

- The ICT roles should also be relevant for future digital transformation efforts. As part of a dedicated foresight exercise, the Bank team worked with international experts from the JRC and Prospectiva to anticipate emerging public sector digital skills needed and roles (e.g. AI policy, predictive governance, citizen participation platforms, blockchain, digital ethics governance, integrated foresight tools).

Key findings:

- By 2032, Romania's public administration will require a mix of strategic, operational, and technical digital roles: (1) ICT-intensive: cybersecurity analysts, cloud engineers, AI governance experts, (2) ICT-enhanced: digital transformation officers, smart city managers, (3) ICT-dependent: service designers, user experience experts, data analysts.
- High-demand roles will include AI/NLP engineers, cloud and edge computing specialists, IoT engineers, blockchain architects, cybersecurity and data protection specialists, and geospatial data scientists. Sector-specific needs were identified, such as health data system architects, privacy officers, and AI-driven analytics experts for digital health.
- In the future, citizen-facing roles will be even more relevant from a digital perspective, to ensure accessibility, inclusion, and trust in digital services – through dedicated roles such as: citizen engagement specialists, digital inclusion officers, hybrid service coordinators, digital ombudsmen, multilingual support experts, and blockchain public outreach officers.

Source: WB (2025), *Report on the assessment of the digital competencies needed in the Romanian public administration*, available at <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099071725093059745/p506325-5d25a447-aa60-4b9e-aad0-a7193167bc98>.

18. In addition, the design process relied on an iterative technical process of collaboration with the ICT Working Group that provided evidence on how ICT roles can be formulated building

on eCF. Four working group meetings of the ICT working group were conducted as part of the design phase, between February and June 2025. Through an interactive process, the ICT working group worked on selecting a core set of 10 ICT roles for the central public administration, drawing on two relevant frameworks that cover specialized ICT competencies: the European e-Competence Framework (e-CF) that classifies 41 competences for the ICT professionals⁸ (e-CF) and the European Cybersecurity Skills Framework (ECSF)⁹ frameworks. The initial 10 roles discussed in the working group were prioritized according to the complexity of ICT systems and the types of institutions. The group also differentiated between core ICT roles, essential for operational activities, and non-core or emerging roles linked to innovation and transformation. Then the set was expanded to additional relevant roles. In addition, experts provided feedback on the proposed classification of ICT systems, which included the following categories: S0 – Critical ICT systems, S1 – Very large ICT systems, S2 – Large ICT systems, S3 – Medium ICT systems, and S4 – Small ICT systems.

19. **The working group sessions also facilitated exchanges with experts who had led digital transformation efforts in Denmark and Moldova.** These case studies provided valuable input for the design process, showing that digital transformation requires not only the clear definition of ICT roles and differentiated salary structures, but also strong alignment with strategic initiatives. They also highlighted the importance of a comprehensive digital transformation strategy with dedicated funding and a clear implementation plan, ensuring that digital measures are closely linked to institutional capacity-building efforts¹⁰.

3. Proposed classification of ICT roles for the Romanian public administration

3.1. Conceptual differentiation between ICT job and ICT role

Making a clear distinction between ICT roles and ICT jobs is essential for the design of ICT functions in Romania's public administration. While national legislation defines jobs and job titles primarily for classification, pay, and HR management purposes, roles provide a more precise description of the actual competences, tasks, and responsibilities that ICT professionals perform. Without this distinction, institutional workforce planning, recruitment, and training remain anchored in generic titles that obscure the real skills required for digital transformation.

20. **A role represents a structured set of tasks, responsibilities, and competences that describe what an ICT professional is expected to deliver.** Roles define “what needs to be done” and “what skills are required” without reference to a specific organization or staff member. Roles are defined in professional frameworks such as the e-CF, which specifies the knowledge, skills, and proficiency levels required¹¹. Examples of ICT roles include Database Administrator, Cybersecurity Specialist, or ICT Support Officer. Roles provide the level of detail necessary to capture the technical

⁸ <https://itprofessionalism.org/professionalism/e-competence-framework/>.

⁹ <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>.

¹⁰ The presentations of the two case studies are delivered as separate documents.

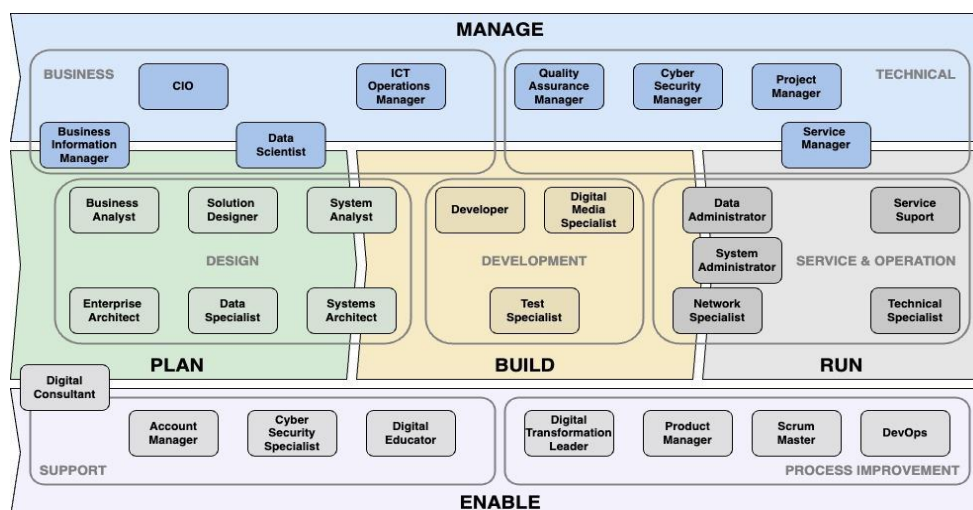
¹¹ <https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf>.

and functional diversity of digital work in government, and they can be used consistently across institutions regardless of local organizational charts.

For the definition of roles, the European e-Competence Framework (e-CF) serves as the primary reference. The European e-Competence Framework (e-CF) classifies 40 competencies for the ICT professionals. 30 ICT Professional Role Profiles were identified by the European Committee for Standardization (CEN).¹²

The e-CF identifies five key processes (planning, building, running, enabling, and managing), as shown in Eroare! Fără sursă de referință., consultations highlighted that key digital skills would cover:

Figure 4. The 30 e-CF ICT Professional role profiles¹³



21. **A job (or position) is the actual position in the organigram of an institution determined based on the job classification under the national legislation.** The position is linked to a specific employment arrangement, professional career structure and salary level. The applicable job classification depends on whether the position is part of the civil service system or the contract-based staff system. The *job title* (also called the *function title*) is the formal label attached to a position and is determined by the Administrative Code and the Framework Pay Law 153/2017. Jobs are therefore legal and organizational constructs, designed for HR management, and may or may not explicitly reflect the underlying ICT role being performed. For example, many ICT professionals in the central public administration are formally employed under generic job titles such as Counsellor (which is a generic civil service job title).

22. **A single ICT job may encompass one or several roles, depending on institutional needs and resource constraints.** For instance, a job/position formally classified as Counsellor may in practice cover both the ICT System Administrator and the ICT Support Officer roles. This mismatch highlights why it is important to distinguish between jobs and roles: job titles serve administrative and pay-related purposes, while roles capture the competences and responsibilities required for

¹²https://standards.cencenelec.eu/dyn/www/f?p=205:29:0:::FSP_ORG_ID,FSP_LANG_ID:1218399,25&cs=1C0456547BD827F5A977AD2936836C8DA#1

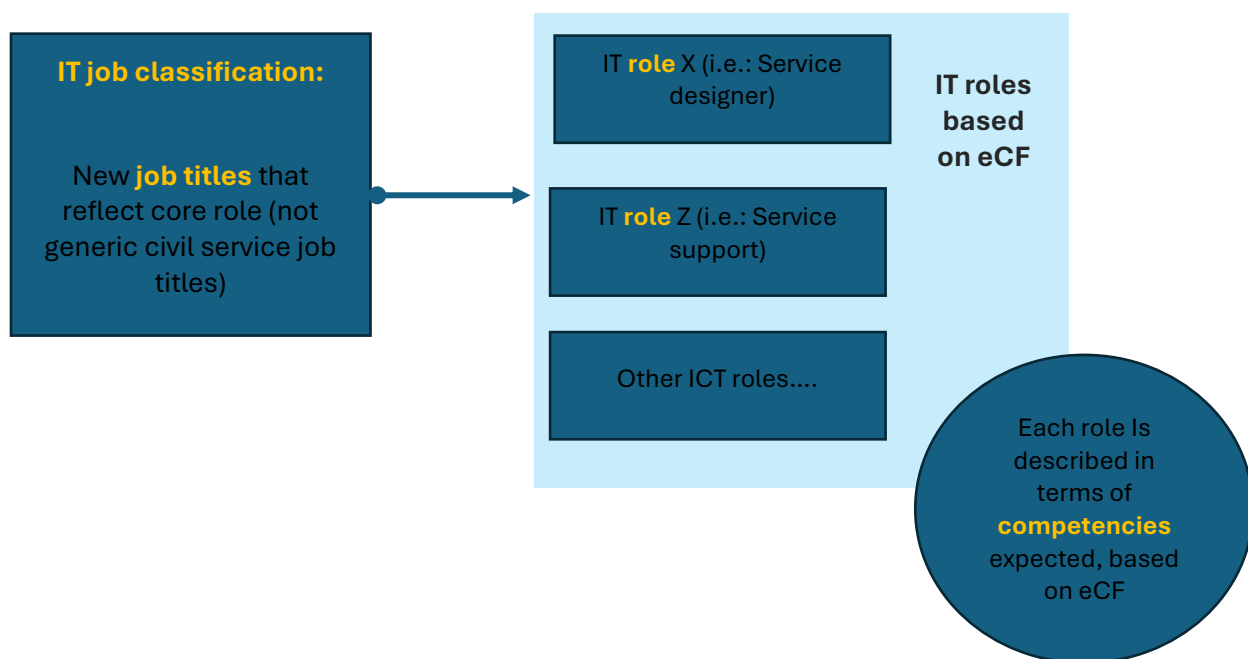
¹³ Also presented in Output 1. More details in: <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099071725093059745/p506325-5d25a447-aa60-4b9e-aad0-a7193167bc98>.

digital transformation. Mapping roles onto jobs ensures that workforce planning, training, and career pathways reflect actual work performed, not just formal titles.

23. **Conceptual differentiation between ICT job and ICT role.** Certain e-CF roles must be interpreted through the lens of “e-government” specificities, not only or merely the digital transformation in general. E-government specialists are professionals who apply regulatory frameworks such as the Interoperable Europe Act or the AI Act in the context of the institution’s internal organization, they are bridging the IT expertise with the regulatory specificities of the functioning of the public sector.

24. **For Romania’s public administration, this analysis points to the need for a revamped job classification system for ICT specialists, with updated job titles that go beyond the current generic labels.** Such a system should explicitly encompass a specific set of ICT roles, defined on the basis of the European e-Competence Framework (e-CF) and validated through expert input and institutional consultations. By aligning job titles with clearly designed ICT role profiles, the administration can ensure that recruitment, workforce planning, and training reflect the real competences required for digital transformation, rather than relying on outdated classifications that obscure the skills and responsibilities of ICT professionals.

Figure 5. Correlation between job and role for ICT specialists



3.2. Proposed list of ICT roles for the Romanian public administration

25. **The proposed list of ICT roles for the Romanian public administration was built upon the e-CF 3.0 (EN 16234-1) but tailored to the specific requirements of the public administration.** Consultations and workshops were held with representatives from central public institutions, leading to an adaptation of the e-CF framework to the public administration needs. Through these structured consultations and working sessions involving ICT experts from relevant central public institutions, the e-CF framework was calibrated and adapted to ensure its strategic relevance, practical applicability, and sustainability in the local context.

26. **The e-CF classifies 30 ICT professional roles according to the technical, operational, and strategic functions needed to plan, build, run, and manage information systems.** Each role is defined by a structured set of competences drawn from the framework's 41 standard competences, covering areas such as architecture design, service delivery, information security, and business analysis. Competences are described at five proficiency levels (e-1 to e-5), ranging from entry-level practitioners to strategic leaders who shape governance frameworks and enterprise-wide decisions.

27. **E-CF competences are expressed at one or more of five proficiency levels (e-1 to e-5),** which describe the depth of expertise, degree of autonomy, and level of influence:

- **e-1:** Entry-level professionals who apply basic knowledge and skills under close supervision.
- **e-2:** Practitioners with moderate experience, capable of delivering well-defined tasks with some autonomy.
- **e-3:** Senior professionals with advanced expertise, able to work independently, solve complex problems, and influence team outcomes.
- **e-4:** Highly experienced professionals who ensure quality, advise on solutions, and influence organizational priorities.
- **e-5:** Strategic-level experts who initiate and lead innovation, define governance frameworks, and shape enterprise-wide decisions.

28. **The design of ICT roles for Romania's public administration combined a selective adaptation of the e-CF with the integration of additional roles from complementary frameworks,** ensuring both relevance to national needs and alignment with European standards.

29. **Out of all 30 ICT roles from eCF, 20 are recommended to be included in the list of proposed ICT roles, and 4 are new roles.** These latter additional roles are drawn from other frameworks (e.g. the European Skills, Competences, Qualifications and Occupations (ESCO)¹⁴, the Government Digital and Data Profession Capability Framework in UK (DDaT)¹⁵) and defined nationally to reflect Romania's digital transformation needs. One of the new roles, the ICT specialist role, includes specific tasks defined in other e-CF roles, but not very specific for the public administration from Romania (DevOps Expert, Digital Media Specialist, Product Owner, Project Manager, Scrum Master, Service Manager). When compared against the 30 e-CF ICT role profiles, the draft list of 25 roles proposed for the Romanian public administration omits some roles (Account Manager, Training Specialist, Quality Assurance Manager). Certain updates were also integrated to

¹⁴ <https://esco.ec.europa.eu/en>.

¹⁵ <https://ddat-capability-framework.service.gov.uk/>.

ensure AI specialization is also covered, taking into account relevant ongoing initiatives, such as the development of AI profiles by the European Committee for Standardization (CEN)¹⁶.

30. **The 25 proposed ICT Roles are presented below. Their comprehensive description, including the list of proposed competencies and associated levels is included in Annex 3.**

Table 1 ICT Roles for the Romanian public administration

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

31. **Some of the ICT roles in the proposed list that are not part of the e-CF are nonetheless justified by the specific focus on digital service delivery in the public sector.** While the e-CF provides a solid foundation for defining technical ICT competences, it does not fully capture the disciplines required for **user-centered service delivery**. Digital transformation in government increasingly depends on roles that combine technical expertise with design, research, and product management skills - areas that have only recently emerged in the public sector. Building internal capacity in these competencies is essential to ensure that digital services are not only technically

¹⁶ <https://www.cencenelec.eu/news-events/news/2025/workshop/2025-04-16-arisa/>.

sound but also accessible, inclusive, and trusted by citizens. Consequently, outside the framework of competences proposed by e-CF, most public institutions that provide services to citizens or to other stakeholders (such as other public institutions or the private sector) need to define roles specifically focused on service provision, such as:

- **Product Manager role:** Leads a cross-functional team to ensure digital services are designed and implemented in a way that is iterative, fluid and collaborative, and which centres user needs alongside organizational goals.
- **User Researcher role:** Plans, designs and carries out research activities to build deep understanding of the people who use government services.
- **Service Designer role:** Designs the experience for government services based on the evidence of user needs and organizational goals.
- **E-Government Specialist role:** Designs and implements digital government solutions based on user needs, policy goals, and institutional capacity to ensure secure, interoperable, and effective public services.

32. **Although these three roles themselves are not explicitly defined in the e-CF framework, certain competences associated with these roles are covered by e-CF profiles**, as shown in Table 2. They are increasingly relevant in the context of digital government, where the expansion of the Government Cloud and the growing reliance on Software-as-a-Service (SaaS) require public institutions to develop user-centered service delivery capacities. Including such roles in the classification of ICT roles for the public administration ensures that digital services are designed and managed not only from a technical perspective but also with a focus on accessibility, usability, and citizen experience.

Table 2 New roles proposed and associated with e-CF competencies

Role	Associated e-CF competencies	Main responsibilities
Product Manager	A.4 Product/Service Planning E.2 Project & Portfolio Management E.4 Relationship Management E.7 Business Change Management A.3 Business Plan Development	Leads cross-functional teams in developing digital public services. Ensures solutions are developed iteratively, agile, and user-centered. Aligns organizational objectives with the design and delivery of services. Prioritizes requirements and resources to maximize public impact. Monitors success indicators and the overall impact of digital services.
User Researcher	B.1 Requirements Analysis E.4 Relationship Management D.10 Information & Knowledge Management E.6 Quality Management	Plans and conducts qualitative and quantitative research to understand users. Builds user profiles and user journeys for public services. Tests prototypes and services with real users. Translates research data and

		insights into actionable recommendations. Ensures services reflect the real experience of end users.
Service Designer	A.4 Product / Service Planning B.1 Requirements Analysis E.5 Process Improvement E.4 Relationship Management E.6 Quality Management D.10 Information and Knowledge Management	Designs the end-to-end experience of public services. Integrates user research evidence with institutional goals. Defines and visualizes processes and service flows, documenting digital administrative workflows and associated information models; Coordinates interface and interaction design with development and UX teams.
E-Government Specialist	A.4 Product / Service Planning B.1 Requirements Analysis B.4 Solution Deployment E.5 Process Improvement E.7 Business Change Management E.4 Relationship Management D.10 Information and Knowledge Management	Analysis of administrative processes and definition of functional and non-functional requirements for digital services. Translation of legal and public policy requirements into functional specifications for the other ICT experts, including the assessment of the organisational and institutional impact of implemented ICT solutions. Ensures alignment of digital solutions throughout the lifecycle of digital solutions with e-government principles, including interoperability, the “once only” principle, and “digital by default” with an accent on the EU and national strategic framework (e.g., e-Gov Public Policy), and integrating the EU financing principles and regulatory framework.
ICT Specialist¹⁷	A.1. IS and Business Strategy Alignment A.3. Business Plan Development A.6. Application Design B.1. Application Development B.2. Component Integration B.3. Testing	Support delivery of digital projects (requirements, documentation, sprint activities, testing, deployment) Assist DevOps and operations teams with configuration, monitoring, troubleshooting

¹⁷ This role manages specific tasks defined in other eCF roles, but not very specific to the public administration in Romania (DevOps Expert, Digital Media Specialist, Product Owner, Project Manager, Scrum Master, Service Manager). When defining a position for this role, at most five competencies should be selected, along with the corresponding responsibilities.

B.4. Solution Deployment D.10. Information and Knowledge Management C.1. User Support C.2. Change Support C.4. Problem Management D.2. ICT Quality Strategy Development E.2. Project and Portfolio Management E.4. Relationship Management E.6. ICT Quality Management	Define, build and optimise data models Apply standards methods and tools for measuring and reporting on wide set of relevant performance indicators (response time, availability, safety, integrity) Facilitate collaboration with IT departments of subordinate agencies Support ICT governance, cybersecurity compliance, standardisation and interoperability Contribute to service management processes (incident, problem, change) Provide user support and help improve digital services Support digital communication tasks when required Provide guidance on search engine optimisation (SEO) Test and resolve any technical, usability and accessibility issues Help team improve and take responsibility for their actions to deploy agile values, principles and practices Direct, organize, plan and monitor activities Coordinate, record and ensure quality compliance Ensure the project helps to support the organisation's wider goals Comply with ethical guidelines and legal requirements.
--	---

Potential need for an *AI Manager* role

33. **Introducing an *AI Manager* role (role 26) could represent a timely and strategic opportunity for public administrations seeking to govern the adoption of artificial intelligence in a coherent and responsible manner.** As AI solutions increasingly influence core public services and decision-making processes, there is a growing need for a role that bridges technology, policy, ethics, and organisational priorities in AI technologies. The AI Manager would provide strategic oversight of AI initiatives, ensuring alignment with institutional objectives, legal frameworks, and public value, while avoiding fragmented or ad-hoc deployments.

34. **Within the proposed role structure, the AI Manager is not intended to replace specialised technical roles, but to coordinate and orchestrate them.** Developers, including

those specialised as AI Developers or Machine Learning Engineers, would remain responsible for building, training, and maintaining AI systems. The AI Manager would instead ensure that these technical activities are coherent, interoperable, and aligned with broader governance requirements, including data governance, risk management, transparency, and compliance with emerging AI regulation. In this sense, the role acts as a horizontal integrator across multiple competences rather than a simple defined technical position.

35. **From an organisational perspective, the AI Manager role may also be functionally integrated with or substituted by an expanded CIO role.** In some institutions, the CIO could assume explicit responsibility for AI governance and strategy, provided that sufficient authority, expertise, and capacity are in place. In larger or more complex organisations, a dual-CIO model could be considered, where one CIO oversees general ICT operations, while a second CIO or equivalent senior role focuses specifically on AI, data, and advanced digital technologies. This approach allows institutions to scale their governance structures according to maturity and risk exposure.

36. **Overall, the introduction of an AI Manager role, either as a standalone position or embedded within senior IT leadership, supports a more structured, accountable, and strategic approach for AI adoption.** It strengthens coordination across technical and non-technical roles, reduces fragmentation, and helps ensure that AI technologies are deployed effectively, trustworthily, and aligned with public sector values.

3.3. A public administration reality: allowing ICT role overlap while determining the dominant role

37. **A job/position held by an individual within an institution can reflect a dominant role that defines the position's main mission and may also combine multiple roles depending on the institution's dimension, digital maturity, and profile.** It is already a common practice in the public sector to have multiple roles for one position, even if they are not adequately mapped and reflected in the job description. This should also be possible in the future. For example, in a small institution with only two ICT staff, a single position may need to combine the Systems Administrator, Service Support, and Security Specialist roles. In a large ministry, by contrast, each of these roles would typically correspond to a distinct position, allowing for greater specialization.

38. **This distinction is crucial because it enables institutions of different sizes to map their needs consistently against a common role model (e-CF), while still adapting the structure of positions to their actual capacity.** In practice, the role provides the standard definition, while the position provides the organizational reality, sometimes one-to-one, sometimes combining several roles into a single post, according to the conceptual differentiation presented in section 3.2.

39. **Despite the distinct responsibilities assigned to each role, a certain degree of skill overlap is both possible and necessary.** Many ICT competences are transferable across roles, and this overlap creates flexibility in how tasks can be distributed within institutions. Such flexibility is particularly important in smaller organizations, where limited staff capacity often requires individuals to take on multiple responsibilities. For example:

- System Administrators and Technical Specialists share tasks such as component integration, system testing, and troubleshooting.

- Software Developers also engage in testing, deployment, and integration, similar to administrators.
- Technical Support Staff perform diagnostics and issue resolution, overlapping with other roles.
- Information Security Specialists contribute to ICT governance in addition to risk assessment and compliance.

40. The example in Box 2 below focused on two selected roles: Systems Administrator and Developer.

Box 2 Example of role compatibility: System Administrator and Developer

Example of role compatibility: System Administrator and Developer

The Systems Administrator role is primarily operational and infrastructure oriented. The main tasks focus on maintaining, installing, upgrading, and securing the organization's ICT systems. This involves diagnosing and resolving hardware or software problems, ensuring that installations and upgrades cause minimal disruption, and complying with security procedures to maintain system integrity. Even where competences overlap with other roles, such as *Component Integration* (B.2) or *Testing* (B.3), the emphasis is on deployment, system reliability, and adherence to organizational standards rather than on creating new functionality.

The Developer role, by contrast, is design and build focused. Its tasks revolve around creating, engineering, and integrating software components, following user experience guidelines, and ensuring security is embedded in the design phase. While it also shares competences like *Component Integration* (B.2) and *Testing* (B.3), the developer's perspective is from the point of view of software creation and quality assurance. Developers also produce documentation (B.5) and provide advanced technical support related to the components they build, often resolving issues before and after testing to ensure smooth deployment.

Even for the shared competence C.4 - Problem Management, the context and focus are different:

- For a **Systems Administrator**, C.4 is about scheduling installation work to minimize disruption, diagnosing and solving hardware/software problems, and maintaining system continuity.
- For a **Developer**, C.4 is about providing advanced technical support for the components they build and resolving issues before and after testing to ensure the software meets requirements.

Therefore, the Systems Administrator and Developer roles can be compatible for a single position only in specific organizational contexts, usually where the ICT environment is small, resources are limited, or the operational model intentionally combines infrastructure and development responsibilities for a specific application. They are most compatible when:

- **The institution is small or has a lean ICT team.** In small public institutions with only a few ICT staff, it's common for one person to manage both system operations (installations, upgrades, security) and in-house development or customization of applications.
- **The role is focused on integrated solutions.** In contexts where an application is built and hosted in-house, the same person might develop features and maintain the underlying infrastructure, mainly the software component. For example, a custom document management system that requires regular software solution updates and monitoring activities, and on-premise server administration (storage and RAM allocation, back-ups, operating system updates, etc.).
- **Workload and complexity are moderate.** If the number of systems, applications, and users is relatively low, the technical workload for each function might not justify separate full-time positions.
- **The organization uses DevOps practices.** In a DevOps setup, roles intentionally combine development (coding, integration) with operational responsibilities (deployment, monitoring, problem resolution), meaning the competencies of both e-CF roles naturally merge.
- **The systems are tightly coupled with in-house applications** If the infrastructure and the developed software are interdependent and require frequent coordinated changes, one person having both skill sets can improve efficiency and reduce communication gaps.

41. **The tables below illustrate both the common and the distinct competences associated with the two roles discussed above.** The use of these tables mapping roles and competences, proficiency levels, and tasks to each ICT role is essential for ensuring clarity and consistency in role definition. They make explicit which competences are unique to a role and which are shared with others, helping institutions identify areas of compatibility, potential overlap, and opportunities for flexibility in assigning responsibilities.

42. **A detailed mapping of role compatibilities based on associated competencies is included in Annex 2.**

Table 3 Roles and associated competencies for System Administrator and Developer

SYSTEMS ADMINISTRATOR		
Competences	Levels	Main tasks
B.2. Component Integration	e2-e4	Investigate, diagnose and solve system related problems
B.3. Testing	e1-e4	Install and upgrades software
C.2. Change Support	e2-e3	Test upgrades
C.4. Problem Management	e2-e4	Schedule installation work, to minimize disruption
E.8. Information Security Management	e2-e4	Diagnose and solve hardware or software problems
		Comply with organization procedures to ensure integrity and security of the system
DEVELOPER		
Competences	Levels	Main tasks
B.1. Application Development	e1-e3	Develop engineer and integrate components
B.2. Component Integration	e2-e4	Follow user experience guidelines
B.3. Testing	e1-e4	Aware of and address known security vulnerabilities, applying security by design
B.5. Documentation Production	e1-e3	Shape documentation
C.4. Problem Management	e2-e4	Provide advanced, component technical support
		Resolve issues prior to and following testing

43. **While it should be possible to combine tasks and responsibilities from several ICT roles, it is essential that a dominant role anchors a given ICT position.** The dominant role represents the core mission and primary responsibilities of the position. It sets the main direction for the role holder's work, determines the most critical competences, and defines the contribution of the position to the organization's digital objectives. For example, in a position described as "Systems Administrator with security responsibilities," the dominant role of Systems Administrator makes clear that the primary mission is to ensure systems are running, secure, and up to date. Security competences are added as complementary, but they do not overshadow the main accountability.

44. **Having a dominant role is important because it provides clarity and consistency in expectations, avoids confusion about priorities, and ensures accountability**, since performance can be evaluated against the leading role rather than a mix of unrelated tasks. It also supports career development and training, as the dominant role anchors the professional pathway and allows the employee to grow within a recognized profile, even if they perform tasks that cut across other roles.

45. **At the same time, it is equally important that no critical task depends on a single individual.** Relying on one person creates a single point of failure: if that person becomes unavailable due to illness, leave, or unexpected departure, essential services may be disrupted. To ensure continuity, every key task should have at least two people capable of carrying it out. While one position may have the dominant role for that task, another should also be trained and competent to perform it when needed. This ensures resilience during staff absence, supports smooth operations during holidays, and allows employees to take time off or pursue development opportunities without risking service delivery. It also promotes knowledge sharing and skill transfer, strengthening the institution's overall capacity.

46. **By combining the concept of a dominant role with the principle of task redundancy, public institutions can achieve both clarity and resilience.** This approach ensures that roles are well-defined and strategically aligned, while operations remain robust, flexible, and resilient to disruptions.

47. **Examples of role compatibility matrix adapted to the public administration is proposed in the table below.** These examples demonstrate the flexibility of the approach: each public institution can define role allocations customized to its systems and the number of ICT positions available, while still ensuring that the recommended roles are covered according to organisational size and system complexity.

Table 4 Examples of dominant roles and other compatible roles

Dominant role	Examples of compatible roles
Developer as dominant	Test Specialist - a developer who also handles integration and quality testing. Solution Designer - a developer who translates requirements and designs solutions in smaller projects. Developer - a developer who also manages Continuous Integration / Continuous Delivery pipelines and deployment tasks.
Systems Administrator as dominant	Network Specialist - unified infrastructure role covering servers and networks (common in small institutions). Information Security Specialist - sysadmin who also enforces security controls and patching. Technical Specialist - sysadmin who takes on advanced troubleshooting and maintenance.
Information Security Specialist as dominant	Systems Administrator - security plus system administration responsibilities. Network Specialist - cybersecurity with direct responsibility for network security. Service Support - in smaller teams, the security officer also acts as an advisor to end-users.
Data Administrator as dominant	Data Scientist - data custodian who also delivers analytics and insights (common in organizations without dedicated analytics units). Data Specialist - an administrator who also implements governance and quality management. Developer - data admin who develops scripts and tools for ETL or automation

Service Support as dominant	Technical Specialist - helpdesk staff who also troubleshoot and repair hardware/software. Service Manager - in small organizations, a support lead who also defines SLAs. Systems Administrator - a support person who manages basic system tasks.
Network Specialist as dominant	Systems Administrator - integrated infrastructure support. Information Security Specialist - a network expert who also enforces security. Technical Specialist - network role combined with advanced technical troubleshooting.
CIO / ICT Operations Manager as dominant	Project Manager - CIO who directly leads strategic projects. Service Manager - CIO who also oversees service delivery. Enterprise Architect - CIO with strategic architecture responsibilities.

3.4. Correlation of ICT roles allocation with organization size and complexity of ICT systems

48. **The number and type of ICT roles an institution needs is influenced not only by its size, but also by the complexity of its systems and the criticality of the services it provides.** A small organization that manages simple, non-essential systems may require only a few multi-role ICT professionals, while a larger institution running complex or critical platforms will need dedicated specialized roles to ensure resilience, security, and continuity. For this reason, ICT staffing models cannot be based only on headcount linked to organizational size. They must also take into account the technical complexity of operations, the importance of uninterrupted service delivery, and the scale of digital transformation required.

49. **Some key factors to be taken into account for the classification of IT roles is organization size (which is expected to be correlated with its mandate) and the complexity of the ICT systems, as reflected in the table below and in Annexes 4 and 5.**

Table 5 Proposed classification of public institutions for the purpose of ICT roles allocation

Type of institution	Characteristics
Small institutions	Size: Up to 50 employees Systems: Fewer than 5, non-critical Staffing: Typically, 2 multi-role ICT professionals Support: External consultants for specialized needs Roles Combined: One person may handle system administration, support, and basic development
Medium institutions	Size: Up to 100 employees Systems: Up to 15, mostly non-critical Staffing: At least 6 ICT professionals: - 1 System Administrator - 1-2 Developers/Support Engineers - 1 Information Security Specialist - 1-2 Technical Support/Operations staff
Large Institutions/ critical IT systems	Size: Over 100 employees Systems: More than 15, including critical systems Staffing: Minimum of 10 dedicated ICT professionals: Separate roles for: - System Administration, - Software Development,

- Information Security, and
- Tiered Technical Support

Additional Needs: Critical systems require dedicated specialists for monitoring, incident response, and compliance auditing

50. **In small institutions, where fewer than five systems are typically in place and most are non-critical, ICT staff are expected to be adaptable and multi-skilled.** With usually no more than two multi-role professionals covering the entire ICT function, a single role - such as a System Administrator - may encompass a wide range of duties, including user support, system configuration, troubleshooting, and even basic development. For specialized needs such as cybersecurity audits or advanced integration, these institutions often rely on external consultants or services. One person covers multiple domains to keep the organization running.

51. **In medium institutions, ICT functions should diversify.** A System Administrator, for instance, will focus more specifically on maintaining and upgrading infrastructure, with less overlap into development or front-line support. Other colleagues may take responsibility for application development, technical support, or information security, reducing the need for one person to cover everything. In this context, the same role becomes more defined but still retains flexibility to cover gaps when needed. Collaboration between roles is more structured, and responsibilities start to align with recognized professional profiles.

52. **In large institutions, the responsibilities of each ICT role become highly specialized.** A System Administrator will focus strictly on infrastructure, ensuring continuity, scalability, and compliance with security standards. Separate teams of developers, security specialists, and technical support staff provide clear functional boundaries. For critical systems, additional specialists may be required for monitoring, incident response, and compliance auditing. In this setting, roles are deep and narrow, with each professional dedicated to a specific area of responsibility, ensuring resilience, high performance, and regulatory compliance.

53. **Beyond the size of the institution, several other factors can significantly influence the required number and type of ICT staff, such as:**

- **System complexity plays a central role.** Institutions that manage complex databases, integrate multiple applications, or deliver external-facing digital services must maintain a larger pool of backend specialists and security professionals. The complexity of interconnected systems raises both the volume of work and the level of expertise needed to maintain stability and reliability.
- **Service criticality is another decisive factor.** Where ICT systems support essential services - such as citizen-facing platforms, public safety applications, or healthcare information systems - institutions cannot afford downtime. This requires additional staff dedicated to redundancy, real-time monitoring, and incident response. The higher the stakes, the more personnel are needed to guarantee resilience and compliance with service-level requirements.
- **Change management and transformation initiatives also drive staffing needs.** Organizations engaged in frequent updates, modernization efforts, or large-scale digital transformation projects must reinforce their teams with project managers, DevOps engineers, and quality assurance testers. These roles are critical to ensure that new technologies are integrated smoothly, risks are managed, and innovations deliver value without disrupting existing services.

54. The progression illustrated in the table below shows how ICT roles in the public administration can evolve with institutional size: from a small but essential core team to a balanced medium-sized unit, and ultimately to a fully specialized ICT department capable of sustaining mission-critical systems.

Table 6 ICT roles by institution size and ICT system complexity

ICT Roles by institution size and systems		
Small	Medium	Large /Critical(strategic) systems
Information Security Specialist	Information Security Specialist	Information Security Specialist
Network Specialist	Network Specialist	Network Specialist
Systems Administrator	Systems Administrator	Systems Administrator
Technical Specialist	Technical Specialist	Technical Specialist
	Business Analyst	Business Analyst
	Business Information Manager	Business Information Manager
	Chief Information Officer (CIO)	Chief Information Officer (CIO)
	Database Administrator (DBA)	Database Administrator (DBA)
	Data Specialist	Data Specialist
	Developer	Developer
	Enterprise Architect	Enterprise Architect
	Systems Analyst	Systems Analyst
	Systems Architect	Systems Architect
	Test Specialist	Test Specialist
		Data Scientist
		Digital Transformation Leader
		ICT specialist
		ICT Operations Manager
		Information Security Manager
		Product Manager
		Service Designer
		Service support
		Solution Designer
		User Researcher
		E-Government Specialist

55. The table below presents the proposed ICT roles for Romania's central public administration, structured according to institutional type and system complexity. It illustrates which roles are most relevant for small, medium, and large institutions (including those managing critical ICT systems), while also providing a concise description of each role's mission.

Table 7 Proposed roles allocation and role mission per institution size and systems

Institution Type					Mission
Nr.	Role title	Small	Medium	Large/ Critical ICT system	
1	Business analyst		x	x	Analyses the information and the processes needed to support business plans. Formulates functional and non-functional requirements of the business organization and advises on the lifecycle of the information solutions. Evaluates the impact in terms of change management.
2	Business information manager		x	x	Aligns the Information System to the business strategy within their area/domain. Ensures continuous enhancement whilst accounting for user requirements, service quality and budgetary constraints.
3	Chief Information Officer (CIO)		x	x	Ensures the alignment of the Information Systems strategy with the business strategy. Provides leadership for the implementation and development of the organizations architecture and applications.
4	Database administrator (DBA)		x	x	Administer and monitor data management systems and ensures design, consistency, quality and security.
5	Data scientist			x	Finds, manages and merges multiple data sources and ensures consistency of datasets. Identifies the mathematical models, selects and optimizes the algorithms to deliver business value through insights. Communicates patterns and recommends ways of applying data.
6	Data specialist		x	x	Ensures asset protection through the provision of clean, consistent, quality assured data. Maintains the integrity of data, stores and searches data and supports presentation of data analysis.
7	Developer		x	x	Ensures building and implementing of ICT applications. Contributes to low-level design. Writes code to ensure optimum efficiency and functionality and user experience.
8	Digital Transformation Leader*			x	Drives cultural change and builds digital capability to deliver innovative business models and processes.
9	Enterprise architect		x	x	Maintains a holistic perspective of the organization strategy, processes, information, security and ICT assets. Links the mission, strategy and business processes to the ICT strategy. Ensures project choices are integrated consistently, efficiently and in a

					sustainable manner according to the enterprise's digital standards.
10	E-Government Specialist			x	Designs and implements digital government solutions based on user needs, policy goals, and institutional capacity to ensure secure, interoperable, and effective public services.
11	ICT specialist			x	Manage specific tasks defined in other eCF roles, but not very specific for the public administration from Romania (DevOps Expert, Digital Media Specialist, Product Owner, Project Manager, Scrum Master, Service Manager)
12	ICT Operations Manager			x	Implements and maintains a designated part of an ICT operation ensuring that activities are conducted in accordance with organizational rules, processes and standards. Plans changes and implements them in accordance with organizational strategy and budget. Risk manages and ensures the effectiveness of the ICT infrastructure.
13	Information security manager			x	Defines the information security strategy and manages implementation across the organization. Embeds proactive information security protection by assessing, informing, alerting and educating the entire organization.
14	Information security specialist	x	x	x	Defines, proposes and implements necessary information security techniques and practices in compliance with information security standards and procedures. Contributes to security practices, awareness and compliance by providing advice, support, information and training.
15	Network specialist	x	x	x	Manages and operates a networked information system, solving problems and faults to ensure defined service levels. Monitors and improves network performances and security.
16	Product manager			x	Ensure that digital products and services create the greatest public value by bringing together user needs, policy goals, and technological innovation.
17	Service designer			x	Design and optimize digital services that are simple, accessible, and user-focused, while ensuring they meet policy objectives, legal requirements, and organizational capabilities
18	Service support			x	Provides user support and troubleshoots ICT problems and issues. The primary objective is to enable users to maximize their productivity through efficient and secure use of ICT equipment or software applications.
19	Solution designer			x	Proposes and designs solutions in line with technical architecture which fit business requirements and support change.
20	Systems administrator	x	x	x	Installs software, configures and upgrades ICT systems. Administers day-to-day operations to satisfy continuity of service, recovery, security and performance needs.

21	Systems analyst		x	x	Ensures the technical design and contributes to the implementation of new and/or enhanced software provision. Provides solutions for the improvement of organizational efficiency and productivity.
22	Systems architect		x	x	Designs, integrates and implements complex technical ICT solutions ensuring procedures and models for development are current and comply with common standards. Monitors new technology developments and applies if appropriate. Provides technological design leadership.
23	Technical specialist	x	x	x	Effectively maintains customer hardware/software. Responsible for delivering timely and effective repairs to ensure optimal system performance and superior customer satisfaction.
24	Test specialist		x	x	Ensures delivered or existing products, applications or services comply with technical and user needs and specifications. For existing systems, applications, innovations and changes; diagnoses failure of products or services to meet specification.
25	User researcher			x	Generate deep, evidence-based insights into the needs, behaviours, and experiences of citizens and public sector users, ensuring that digital services are inclusive, accessible, and truly effective

56. **The Digital Transformation Leader role is strategic and positioned at the intersection of technology and organisational change.** Unlike purely technical ICT roles, this role requires a strong understanding of how digital technologies can reshape public services, combined with the ability to lead organisational processes, manage stakeholders, and promote innovation. A Digital Transformation Leader may not require deep technical expertise but must demonstrate solid knowledge of digital tools, platforms, and trends, enabling informed decisions and effective collaboration with ICT specialists. Their primary mission is to guide institutions through the design and implementation of digital strategies, ensuring that technology adoption is aligned with policy objectives, user needs, and institutional capacity.

57. **Key responsibilities of digital transformation leaders include shaping digital roadmaps, fostering a culture of innovation, identifying opportunities for process optimisation, and ensuring that digital initiatives deliver tangible value for citizens** and public administration. By bridging the gap between ICT experts and decision-makers, the Digital Transformation Leader ensures that digital transformation is not only technically feasible but also sustainable, inclusive, and impactful.

4. Proposed classification of ICT *jobs*

58. **As presented in Output 1, ICT jobs across the public administration are usually classified as generic civil service jobs (referent, counsellor, expert, director).** This limits opportunities for ensuring a vertical path for professional development for ICT professionals. The current job classification doesn't accurately reflect ICT skills needed, instead creating an impression of a mere technical support role rather than a standalone profession. In the absence of specialized

ICT public jobs, the institutional status of ICT professionals in the public sector (whether employed as civil servants or contract staff) is diminished, the general perception being that of “computer technicians”.

59. **Developing a dedicated ICT job classification, such as “cybersecurity specialist” instead of the generic “superior counsellor,” would allow differentiating ICT professionals from general civil service jobs** (like counsellor, expert). A dedicated job classification system would professionalize the sector by clearly defining ICT jobs, their associated roles and responsibilities that would then be consistent across institutions. At present, the main HRM databases¹⁸ don’t allow a clear mapping of ICT professionals or distinguish between ICT subdomains. Creating specialized ICT jobs would make possible to inventory occupied and vacant ICT positions, ensure visibility on institutional needs, and align workforce planning with national and European priorities such as the Governmental Cloud and the Digital Decade.

60. **The definition of specialized ICT jobs, should ensure alignment with the e-CF domains** (Plan, Build, Run, Enable, Manage). This organization of several ICT jobs based on broad e-CF domains can also be observed in other public administrations, for example:

- UK (DDaT Framework), which categorizes roles into the following public functions: Delivery, Data, Security, and Management¹⁹.
- Italy uses the UNI 11506 / UNI 11621 standards (aligned with e-CF) to define ICT professional profiles²⁰. These profiles may be linked to public administration jobs: CIO, Business Analyst, Developer, ICT Security Specialist, and Service Manager.²¹

61. **For the Romanian public administration, ICT jobs could be classified as either as civil service jobs with dedicated career structures or as contract-based positions with flexible pay arrangements.** If they remain in the civil service, they need a distinct career path, grading structure, and salary levels tailored to ICT professions, rather than being absorbed under generic job titles such as “Counsellor” or “Specialist.”

62. **International experience shows that several administrations have already created tailored classification systems for ICT staff, where job titles correspond to specialised ICT roles, like in Austria.** At federal level, Austria maintains a unified federal public service pay system but allows narrowly defined exceptions through special contracts (*Sonderverträge*) under the Contract Staff Act²². These contracts, requiring ministerial approval, enable deviations from standard pay rules in order to attract and retain scarce expertise in fields where public wages cannot match the private sector - such as ICT professionals, certain medical professions etc. For ICT jobs, the RIVIT system was introduced as a separate classification and salary system because the general public service pay scales proved uncompetitive. It sets out eight grades with defined steps, linked to specific ICT families such as security, architecture, software engineering, administration, and support.

¹⁸ NACS database on public sector jobs – SENEOSP and the Database of the Ministry of Labor on the wage data for public sector jobs

¹⁹ <https://ddat-capability-framework.service.gov.uk/>.

²⁰ <https://www.digitalsme.eu/ecompetence-framework-italy-sets-example/>

²¹ https://www.agid.gov.it/sites/agid/files/2024-06/piano_triennale_per_linformatica_nella_pa_2024-2026.pdf

²² Austrian Federal law consolidated: Complete legal provisions for the Contractual Employees Act 1948, version of 20 August 2025 available at: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008115>.

Table 8 The ICT job classification system in Austria, federal public service contract-based jobs²³

RIVIT group	IT jobs	Grading within job family	Corresponding ICT roles
1	Security Architect & Senior Analyst		Information Security Analysis, Information Security Engineering, Security Consulting, Security Architecture, ICT Auditor
	IT Manager		IT Project Management, Product Management, ICT Portfolio Management, Support Management, Incident Management, Supplier Management, Demand Management, Innovation Management, Change Management, Quality Assurance Management, License Management, Process Management
2	System Architect	Senior	Database Architecture, Network Architecture, Cloud Architecture, IOT Architecture, Enterprise Architecture, Telecommunication Architecture
	Software Architect		Software Architecture, Test Architecture, Quality Assurance Architecture
	Security Architect & Regular Analyst		Information Security Analysis, Information Security Engineering, Security Consulting, Security Architecture, ICT Auditor
	IT Manager		IT Project Management, Product Management, ICT Portfolio Management, Support Management, Incident Management, Supplier Management, Demand Management, Innovation Management, Change Management, Quality Assurance Management, License Management, Process Management
3	System Engineer	Senior	Network Engineering, Data Engineering, Security Engineering, Cloud Engineering, Deployment Engineering, IOT Engineering, Telecommunication Engineering
	Software Engineer		Big Data Engineering, Artificial Intelligence Engineering, Business Intelligence Engineering, Robotics Engineering
	Software Developer		Database Development, UI Design, UX Design, Cloud Development, Security Software Development, Backend Development, Frontend Development, Fullstack Development
	IT Analyst		Data Analysis, Data Science, Business Analysis, Data Warehouse Analysis, Process Analysis, Security Analysis, System Analysis, Business Intelligence Analysis, Requirements Engineering, In-house Consulting, Solution Architecture, ICT Controlling, ICT Auditor

²³ Information available at: https://www.sicherheitsverwaltung.gv.at/Dein_Weg_Rivit.html

	System Architect	Regular	Database Architecture, Network Architecture, Cloud Architecture, IOT Architecture, Enterprise Architecture, Telecommunication Architecture
	Software Architect		Software Architecture, Test Architecture, Quality Assurance Architecture
	Agile Coach		Agile Coach
4	System Engineer	Regular	Network Engineering, Data Engineering, Security Engineering, Cloud Engineering, Deployment Engineering, IOT Engineering, Telecommunication Engineering
	DevOps		DevOps Engineering
	Software Engineer		Big Data Engineering, Artificial Intelligence Engineering, Business Intelligence Engineering, Robotics Engineering
	Software Developer		Database Development, UI Design, UX Design, Cloud Development, Security Software Development, Backend Development, Frontend Development, Fullstack Development
	Product Owner		Product Owner
	IT Manager	Junior	IT Project Management, Product Management, Supplier Management, Demand Management, License Management, Process Management
5	Administrator	Senior	Network Administration, IOT Administration, Database Administrator, Cloud Administration, System Security Administration, Network Security Administration
	IT Support		Service Desk Management, Help Desk Management, Technical Support, Customer Support, Desktop Support, ICT Support, Special Support, Onsite Support
	Test Engineer	Regular	Usability Test Engineering, Network Test Engineering/Platform Test Engineering, Test Automation Engineering, Manual Test Engineering, Software Tester, Test Library Specialisation
	IT Analyst		Data Analysis, Data Science, Business Analysis, Data Warehouse Analysis, Process Analysis, Security Analysis, System Analysis, Business Intelligence Analysis, Requirements Engineering, In-house Consulting, Solution Architecture, ICT Controlling, ICT Auditor
	Scrum Master		Scrum Master
6	Administrator	Regular	Network Administration, IOT Administration, Database Administrator, Cloud Administration, System Security Administration, Network Security Administration
	System Engineer	Junior	Network Engineering, Data Engineering, Security Engineering, Cloud Engineering, Deployment Engineering, IOT Engineering, Telecommunication Engineering

	Software Engineer		Big Data Engineering, Artificial Intelligence Engineering, Business Intelligence Engineering, Robotics Engineering
	IT Analyst		Data Analysis, Data Science, Business Analysis, Data Warehouse Analysis, Process Analysis, Security Analysis, System Analysis, Business Intelligence Analysis, Requirements Engineering, In-house Consulting, Solution Architecture, ICT Controlling, ICT Auditor
7	IT Support	Regular	Service Desk Management, Help Desk Management, Technical Support, Customer Support, Desktop Support, ICT Support, Special Support, Onsite Support
	Test Engineer	Junior	Usability Test Engineering, Network Test Engineering/Platform Test Engineering, Test Automation Engineering, Manual Test Engineering, Software Tester, Test Library Specialisation
8	IT Support	Junior	Service Desk Management, Help Desk Management, Technical Support, Customer Support, Desktop Support, ICT Support, Special Support, Onsite Support

63. **For Romania, a similar approach could be adopted - either through a revamped civil service job classification for ICT or, where necessary, through contract-based arrangements** that mirror labor market conditions. While civil service positions provide stability, continuity, and a strong link to national HR management frameworks, they are less flexible in adapting to rapid technological changes and competitive pay levels. For more specialized ICT roles - such as cybersecurity experts, cloud architects - contract-based jobs may be preferable, as they allow institutions to recruit talent at salaries closer to private-sector benchmarks and to define responsibilities with greater precision. This flexibility is critical to attract professionals with cutting-edge expertise, reduce reliance on outsourcing, and ensure that Romania's public administration can deliver secure, modern, and innovative digital services.

64. **A set of six core ICT functions (jobs) are proposed below, building on the e-CF domains** (Plan, Build, Run, Enable, Manage). Each function brings together a cluster of e-CF competences and can have specific ICT roles attached to it. The six proposed specialists ICT functions/jobs are:

- i. **ICT Manager** corresponding to e-CF cluster Plan and Manage.
- ii. **ICT Architect** corresponding to e-CF cluster Plan
- iii. **Cybersecurity** specialist for the Enable and Manage e-CF clusters.
- iv. **ICT Service Delivery and Support** specialist for the Run cluster of e-CF.
- v. **ICT Service Management /E-government specialist** for the group Manage from e-CF.
- vi. **ICT Development and Data** specialist corresponding to Build and Development e-CF clusters.

65. **For clarity and consistency, each ICT function in public administration should be anchored by one or more dominant roles that define its core purpose.** These roles act as the reference point for assigning staff to a function, given the qualifications and competencies expected for the dominant role, for example:

- Strategic and leadership roles (CIO, Enterprise Architect, Digital Transformation Leader) are categorized under the **ICT Manager function**.
- Architectural design and integration roles (Enterprise Architect, Systems Architect, Solution Designer) fall under the **ICT Architects function**.
- Operational infrastructure and support roles, including Systems Administrator, Network Specialist, and Service Desk, fall under the **ICT Service Delivery & Support specialist function**.
- Development and data roles (Developer, Data Scientist, Solution Designer) are grouped under the **ICT Development & Data specialist function**.
- Process and service management roles (such as Service Manager, Business Analyst, E-Government Specialist) can shape the **ICT Service Management and E-Government Specialist function**.
- Security roles (e.g., CISO, Cybersecurity Specialist) can determine the **Cybersecurity professional function**.

66. The table below proposes the dominant ICT roles for each of the six proposed ICT jobs/functions.

Table 9 Proposed correspondence between ICT job classification and ICT roles.

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

Table 10 Proposed table of correspondence between proposed ICT roles and ICT job classification

ICT Role ICT public function	ICT Leader	ICT Architect	Cybersecurity specialist	ICT Service Delivery and Support specialist	ICT Service Management and E-Government specialist	ICT Development and Data Management Specialist
Business Analyst	-	-	-	-	•	0

Business Information Manager	•	-	-	-	0	-
Chief Information Officer (CIO)	•	-	-	-	-	-
Database Administrator (DBA)	-	-	-	-	0	•
Data Scientist	-	-	-	-	0	•
Data Specialist	-	-	-	-	0	•
Developer	-	-	-	-	0	•
Digital Transformation Leader	•	-	-	-	0	-
Enterprise Architect		•	-	-	0	-
E-Government Specialist	-	•	-	-	0	0
ICT Operations Manager	•	-	-	0	-	-
ICT Specialist	-	-	-	•	0	0
Information Security Manager	•	-	0	-	-	-
Information Security Specialist	-	-	•	0	-	-
Network Specialist	-	-	-	•	0	-
Product Manager	0	-	-	-	•	-
Service Designer	-	•	-	-	0	0
Service Support	-	-	-	•	-	-
Solution Designer	-	•	-	-	0	0
Systems Administrator	-	-	-	•	-	0
Systems Analyst	-	-	-	-	•	0
Systems Architect	-	•	-	-	-	0
Technical Specialist	-	-	-	•	0	-
Test Specialist	-	-	-	•	0	-
User Researcher	-	-	-	-	•	0

Legend: • Dominant role, 0 Secondary role, - No corresponding function. Red Roles are not defined in e-CF

67. **The matrix above shows how roles are grouped into the six functions (the ESCO framework defines them as “job titles”).** One of these functions caters to management civil servants, while the other five are specialized ICT public functions to complement the execution functions of class I, as specified in the Administrative Code. In this context, any position within an organization’s chart that includes at least one ICT role for civil servants or contractual staff may be linked to one of the specialized ICT functions.

68. **Public institutions could appoint a Chief Information Officer (CIO) who will be responsible for developing and implementing the vision and strategy.** The CIO will also collaborate with other directors and business leaders to align ICT technology with organizational objectives. In large and very large institutions, and sometimes also in medium-sized ones, ICT directors may be appointed for specific subdomains, often selected from the public ICT Manager function (such as Chief Information Security Officer - CISO, Chief Data Officer - CDO, etc.). These directors will report to and be subordinate to the Chief Information Officer - CIO.

5. Proposed levels of responsibility for ICT jobs

69. **For the Romanian public administration, and building also on relevant international experience, ICT functions should also be defined in connection with the seven levels of responsibilities included in Skills Framework for the Information Age (SFIA)²⁴.** These are presented in Table 11, extended with levels 8 and 9 for top strategic management C-suite roles (CIO, CSO, CDO, CTO, and related deputies).

70. **SFIA emphasizes specific, measurable skills connected to technical or managerial tasks,** such as project management (PRMG) or risk management (BURM). The e-CF, on the other hand, defines broader competences that integrate these various skills. For example, the e-CF competence Information Security Specialist is a unified concept that encompasses multiple SFIA skills (Information security, Offensive cyber operations, Penetration testing, Security operations, Threat intelligence, Vulnerability assessment, Vulnerability research). This shows how a single competence is built from a collection of skills, reflecting the complexity of the real world.

71. **The relationship between e-CF and SFIA can best be understood as the intersection of roles and the level of responsibility.** The e-CF defines roles by specifying their mission, scope of activity, and the competences required to perform them. In contrast, SFIA establishes the level of responsibility at which those roles are exercised, describing the degree of autonomy, influence, and complexity associated with professional practice.

72. **In practical implementation, this means that a single ICT role, as assigned to an ICT job, may be performed at different SFIA levels depending on the institutional context.** For instance, the role of Developer may correspond to SFIA Level 2 when carried out under supervision, to Level 3 when the professional operates independently as a practitioner, and to Levels 4-5 when the individual assumes more advanced responsibilities such as system design or team coordination. Similarly, the role of Systems Administrator may align with Level 3 for routine administrative tasks but rise to Level 5 where the position involves managing complex, mission-critical environments. Other management and strategic roles, such as Chief Information Officer (CIO) align most closely with SFIA Level 7, and in extended models can be mapped to Levels 8 or 9 to reflect enterprise-wide or national leadership functions.

²⁴ The global skills and competency framework for the digital world, available at: <https://sfia-online.org/en>.

73. **This distinction has particular relevance for the Romanian public administration, allowing the mapping of ICT jobs and roles depending on institution size and ICT system complexity.** The same role may be positioned at a lower SFIA level in a small institution, where an ICT professional often operates with limited autonomy, modest infrastructure, and multiple overlapping responsibilities. By contrast, the identical role may correspond to a higher SFIA level in a ministry, where systems are more complex, responsibilities are specialized, and the professional has greater authority and influence. In this way, the combination of roles and SFIA levels makes it possible to describe ICT positions consistently across institutions while recognizing the different scales of responsibility at which they are performed.

Table 11 Proposed levels of responsibility for ICT jobs based on SFIA

Level	Characteristics of the level:
Level 1 - Follow	Performs routine tasks under close supervision, follows instructions, and requires guidance to complete their work. Learns and applies basic skills and knowledge.
Level 2 - Assist	Provides assistance to others, works under routine supervision, and uses their discretion to address routine problems. Actively learns through training and on-the-job experiences
Level 3 - Apply	Performs varied tasks, sometimes complex and non-routine, using standard methods and procedures. Works under general direction, exercises discretion, and manages own work within deadlines. Proactively enhances skills and impact in the workplace.
Level 4 - Enable	Performs diverse complex activities, supports and guides others, delegates tasks when appropriate, works autonomously under general direction, and contributes expertise to deliver team objectives.
Level 5 - Ensure, advise	Provides authoritative guidance in their field and works under broad direction. Accountable for delivering significant work outcomes, from analysis through execution to evaluation.
Level 6 - Initiate, influence	Has significant organizational influence, makes high-level decisions, shapes policies, demonstrates leadership, promotes organizational collaboration, and accepts accountability in key areas.
Level 7 - Set strategy, inspire, mobilize	Operates at the highest organizational level, determines overall organizational vision and strategy, and assumes accountability for overall success.
Management levels	
Level 6m - Deputy ICT Director	These levels are for ICT management roles in medium ICT organization or management roles reporting to ICT strategic management roles in large ICT units or strategic ICT units.
Level 7m - ICT Director	
Level 8m - deputy ICT strategic management	These levels are for ICT strategic management roles (C-suite roles) and their deputies. CIO - Chief Information Officer CSO - Chief Security Officer
Level 9m - ICT strategic management	
	CDO - Chief Data Office CTO - Chief Technical officer

Source <https://sfia-online.org/en/sfia-9/responsibilities> and Authors

74. **The definition of levels of responsibility is particularly important for differentiating ICT jobs across institutions and according to the complexity of the ICT systems they manage.** Not all public institutions face the same digital challenges: while some operate small-scale

administrative platforms, others oversee mission-critical systems such as national registries, government cloud infrastructure, or cybersecurity operations. By linking job levels to system size and complexity, it becomes possible to distinguish between routine operational roles and positions that require advanced expertise, leadership, and accountability. This differentiation ensures that ICT professionals are assigned responsibilities that match both their skill levels and the strategic importance of the systems they manage, while also providing a sound basis for tailored career structures, training opportunities, and salary scales.

75. **As a foundation, a general correlation table is proposed between ICT unit size and type of ICT system managed.** The following table - matrix shows which system categories can be managed by an ICT Unit category.

Table 12 Matrix category of ICT unit/department and proposed categories of ICT systems

Category of ICT Unit	S0: Critical ICT systems	S1: Very large ICT systems	S2: Large ICT systems	S3: Medium ICT systems	S4: Small ICT systems
Strategic/special ICT Unit (e.g. DNSC, Cyberint)	Yes	Yes	Yes	Yes	Yes
Very large and large ICT Unit (e.g. MoF ICT Unit, MoI ICT Unit, proposed CIO Unit Justice Sector)	Yes	Yes	Yes	Yes	Yes
Medium ICT Unit		Exceptional	Exceptional	Yes	Yes
Small ICT Unit				Exceptional	Yes

76. **For this matrix, medium and small ICT Units can manage “exceptional” systems such as:**

- ICT systems that are standard software (ERP, HR, etc.) could be provided as SaaS, and there is a comprehensive SLA with the provider for Business Continuity Plans (BCP) and/or Business Recovery (BR) for ICT systems.
- Specific (business) software that are installed on e-government cloud (sectoral cloud) and there are comprehensive SLA for BCP and BR and other roles (e.g. mandatory Business Analyst for Large ICT systems, mandatory Product Owner for Very large ICT systems).

77. **Building on this foundation, the matrix below illustrates the proposed levels of responsibility for each given category of ICT system.**

Table 13 Matrix category of ICT unit/department and proposed categories of ICT systems

Level of responsibility	S0: Critical ICT systems	S1: Very large ICT systems	S2: Large ICT systems	S3: Medium ICT systems	S4: Small ICT systems
Level 1 - Follow	Yes	Yes	Yes	Yes	Yes
Level 2 - Assist	Yes	Yes	Yes	Yes	Yes
Level 3 - Apply	Yes	Yes	Yes	Yes	Yes
Level 4 - Enable	Yes	Yes	Yes	Yes	

Level 5 - Ensure, advise	Yes	Yes	Yes
Level 6 - Initiate, influence	Yes	Yes	
Level 7 - Set strategy, inspire, mobilize	Yes	Yes	
Management level			
Level 6m - Deputy ICT Director	Yes	Yes	Yes
Level 7m - ICT Director	Yes	Yes	Yes
Level 8m - deputy ICT strategic management	Yes	Yes	
Level 9m - ICT strategic management	Yes	Yes	

6. Methodology for mapping ICT jobs and proposing salary levels

78. **The classification of ICT jobs implies not only the design of specific jobs and formulation of job titles, but also the construction of a career system to support attraction and salary progression, in close correlation with the level of responsibility.** For this, it is essential to apply a clear methodological framework that allows the differentiation of ICT professionals, balancing fairness and competitiveness. Salaries should be differentiated according to several key factors:

- the specialized ICT function for the public sector,
- expertise level (including three tiers: junior, regular, senior, and expert,
- level of responsibility (determined according to SFIA criteria),
- institutional size (small, medium, large, very large, and critical), and
- the relative importance of the role within the public institution (expressed as a *coefficient* – but this is not a recommended pay coefficient).

79. **The methodology proposed in this report in Annex 6 is meant to inform the calibration of ICT professional grades, but also future allocation to pay grades.** This methodology will need to be aligned with the technical process expected to be conducted by the Ministry of Labor in the preparation of the salary system reform for all public sector jobs, as envisaged under milestone 420 of NRRP²⁵.

80. **The methodology in Annex 6 proposes a structured approach for differentiating and ranking specialized ICT jobs according to levels of professional responsibility rather than job titles alone.** It begins by mapping each ICT function and seniority level to the internationally recognized SFIA responsibility framework, which defines the maximum level of accountability associated with each role. These responsibility levels are then weighted according to the size and

²⁵ This is a reform process benefitting from World Bank support. The reform is expected to be adopted by June 2026.

criticality of the ICT systems managed (small, medium, large, very large, or critical), acknowledging that identical roles can carry very different levels of complexity, risk, and strategic importance depending on the institutional context.

81. **The model further recognizes functional differences by incorporating an additional weighting factor reflecting the strategic importance of distinct ICT roles.** This differentiation highlights positions with system-wide governance, architectural leadership, cybersecurity protection, and digital transformation responsibilities versus primarily operational or support functions, building on international public-sector ICT classification practices. The combination of SFIA responsibility levels, system-complexity coefficients, and functional-importance weights generates a relative job-ranking coefficient that enables consistent comparison of ICT roles across institutions and seniority levels.

82. **The resulting coefficients are strictly illustrative and analytical tools intended for job ranking and benchmarking, they should not be interpreted as the pay levels proposed by the Bank team.** They demonstrate how ICT roles could be objectively compared in terms of responsibility and institutional impact, but they do not constitute proposals for grading structures, career pathways, or remuneration levels. Any official translation of this methodology into binding classification or wage arrangements must be developed separately through policy dialogue and consultation with key authorities – notably the Ministry of Economy, Digitalization, Entrepreneurship and Tourism (MEDET), ADR, NACS, and the Ministry of Labor, Family, Youth and Social Solidarity (MLFYSS) – and aligned with Romania’s broader public administration job classification reforms.

7. Methodology for mapping ICT roles and ICT jobs to public institutions needs

83. **The proposed ICT roles and ICT jobs need to be aligned with the institutional realities of Romania’s public administration. This section outlines the methodology designed for that purpose.** The preceding sections presented the classification of ICT roles, their consolidation into broader ICT jobs and the definition of professional grades, correlated with institutional type and ICT system complexity. These proposals now require systematic mapping to the actual needs and capacities of public institutions. The methodology provides a structured approach to ensure that the proposed framework is operational and relevant in practice.

84. **This first step will establish a baseline of institutional size, digital service demand, investment capacity, and reliance on external providers.** This ensures results that can be compared across different categories (small/medium/large institutions).

Step 1 - Data collection at institutional level (Organization survey)

Each participating institution completes a standardized questionnaire capturing:

- *Workforce profile (total employees, ICT staff by service area: support, development, infrastructure).*
- *Digital service delivered by institution (number of citizen-facing applications, unique users across citizens, public, and private institutions).*
- *IT investment trends (budget allocations for infrastructure, development, software maintenance, and other ICT services, over the past three years).*
- *Externalized ICT service by type (support, cybersecurity, development, infrastructure, etc.).*

Step 2 will capture how ICT staff perceive their current workload distribution, identify under-utilized competences, and document career aspirations.

Step 2 - Data collection at individual ICT staff level (Specialist survey)

Each ICT professional completes a complementary survey, including:

- *Position title and role in the institution (management/non-management, number of staff supervised if applicable).*
- *Role mapping: Selection of up to 3 roles from the 25 proposed list that apply to individual activities performed in the institution, with estimation of time spent (in percentages – the sum is up to 100%).*
- *Task mapping: Selection of up to 6 tasks from the corresponding list from the selected roles that apply to individual activities performed in the institution, with estimation of time spent (in percentages – the sum is up to 100%).*
- *Competence self-assessment: Selection of up to three competences from the competence set that staff possess and would like to apply more extensively, even if not currently required.*

Professional development interest: Ranking of the selected competences in order of career development priority.

Step 3 - Mapping tasks to competences, roles, identification of dominant role

Using the proposed framework:

- *Tasks selected in Step 2 are mapped to the corresponding competences and their associated proficiency levels.*
- *Competences identified are cross-referenced with the standard role profiles to determine which roles align most closely with each staff member's current position.*
- *A dominant role is identified per staff member (reflecting their primary mission), with optional complementary roles if multiple competences extend beyond a single role profile.*

Step 4 - Institutional role validation, gap analysis and ICT job allocation (including professional grade)

This step analyses whether institutions have the right balance of roles and competencies to support their digital service portfolio and criticality level.

At the institutional level, aggregated data is compared with the recommended ICT roles proposed for small, medium, and large institutions.

- *Identify gaps (missing roles, under-represented competences), overlaps (same tasks assigned to too few staff, creating single points of failure), and mismatches (roles defined generically as "Expert" but actually covering specialized e-CF functions).*
- *Evaluate whether at least two staff members cover each critical competence, ensuring continuity during absences.*
- *Determine allocation of ICT jobs and professional grades*

Step 5 - Reporting and recommendations for workforce planning

A consolidated report is produced for each institution, showing:

- *Workforce structure (current vs. recommended roles).*
- *Competence coverage map (which competences are well covered, which are missing).*
- *Role alignment (actual vs. required roles per institution size).*

- *Professional development Interests (analyse competences selected by staff but not currently utilized).*

85. **The methodological steps proposed are critical for transforming the proposed ICT job classification from a conceptual framework into a practical workforce-planning tool grounded in institutional reality.** By combining organizational data with individual staff mapping, the approach ensures that ICT roles and grades are not assigned abstractly or uniformly across the public administration but are calibrated to real levels of digital service delivery, system complexity, investment capacity, and dependence on external providers. This enables institutions of different sizes and profiles to apply the framework consistently while still reflecting their specific operational contexts, reducing the risk of over- or under-classification of ICT roles.

86. **The multi-step process also creates a direct evidence base for identifying skills gaps, overlapping responsibilities, and institutional vulnerabilities.** Aggregating role and task data across staff allows institutions to assess whether critical competences are sufficiently covered, whether key functions depend on single individuals, and whether current job titles genuinely correspond to specialized ICT profiles. This supports targeted decisions on recruitment, upskilling, redeployment, and internal career development, ensuring that limited human resource investments address the most pressing risks and transformation priorities.

87. **Finally, the consolidated institutional reporting enables the methodology to directly support strategic workforce planning and reform implementation.** By linking actual staffing structures to recommended role distributions and professional grades, institutions gain a clear roadmap for building sustainable ICT capacity over time. The outputs provide a shared factual basis for dialogue between institutions and central authorities when shaping recruitment plans, learning programs, and future adjustments to classification frameworks, ensuring that ICT workforce development is coherent, defensible, and aligned with Romania's broader digital transformation objectives.

8. Relevance of ICT roles based on the pilot exercise

88. **As described in the methodological approach for Output 2, a piloting exercise was designed as a fully integrated test of both components of the TSI work – the proposed general digital competency framework and the specialized ICT role and job classification model.** During October-November, the pilot was implemented across a representative sample of jobs from three key public institutions, covering core business functions, support services, and ICT departments. This allowed the team to validate how general digital competencies apply to non-ICT roles while, in parallel, testing the relevance, differentiation, and calibration of ICT role profiles against real technical ICT positions and workloads. The pilot methodology, detailed in Output 2, combined structured interviews, task and competency mapping, proficiency-level rating, and role alignment exercises. A full description of the pilot design and tools, together with a comprehensive analysis of results for both the general competency framework and the ICT roles, is presented in Output 2 (Annex 2), which serves as the main reference for the empirical evidence underpinning the recommendations set out in this *Connected Report on ICT roles*.

89. **The piloting of the proposed ICT roles across three public sector organizations confirms that the role framework is conceptually strong, easy to apply, and capable of capturing the diversity and complexity of ICT functions.** Despite significant differences in size, mandate, and

technical maturity among the institutions involved in the pilot, the proposed role taxonomy - based on the e-CF - proved immediately recognizable. Existing tasks could be accurately mapped to roles such as Network Specialist, Information Security Specialist, Systems Administrator, Technical Specialist, Business Analyst, even in organizations with minimal digital capacity. This demonstrates that the framework is intuitive, aligns with real job responsibilities, and significantly improves clarity compared to the generic civil service titles currently in use.

90. **At the same time, the pilot revealed structural capacity gaps that had been already noted in Output 1 under the TSI project. Institutions operating currently cover less than 50% of the minimum roles recommended for their category.** Even institutions managing large or critical ICT systems, which require advanced roles in architecture, testing, operations management, and data management, cover less than half of the minimum roles required for their mandate, often missing essential internal capacities such as systems administration, testing or software development. Taken together, these findings indicate that the role framework highlights real staffing and capability deficits, rather than misalignment between the proposed roles and institutional needs.

91. **The pilot indicates that some of the foundational ICT roles - particularly those linked to daily operations - are to a certain extent present across institutions and generally well understood.** Roles such as Network Specialist, Information Security Specialist, Technical Specialist, Systems Administrator and Service Support align closely with current responsibilities and were mapped with relative ease during the pilot. This suggests that institutions already possess a baseline operational ICT capacity oriented toward maintaining infrastructure, handling incidents and ensuring continuity of routine digital services.

92. **At the same time, the assessment highlights a more limited presence of roles that support system development, digital service design, enterprise and system architecture, testing, user-centric design, and data management.** Functions such as Systems Analyst, Developer, Test Specialist, Data Specialist, Business Analyst, or ICT Operations Manager are often missing or only partially covered, even where institutional mandates would benefit from stronger in-house capability. Likewise, advanced and strategic roles, including Enterprise Architect, Business Information Manager, Systems Architect, or roles dedicated to product or service design are only rarely present. Their absence is not unusual in administrations where ICT functions have historically focused on support, but it does indicate that current structures may not be fully equipped to manage more complex or integrated digital environments.

93. **A consistent pattern emerging across all piloted organizations is the limited scope of current ICT work.** In most cases, ICT staff focus predominantly on first-level support - troubleshooting incidents, resolving user requests, and handling basic hardware or communication issues. Because of this operational burden, roles requiring deeper technical, architectural, analytical, or development expertise are either absent or fulfilled informally, without clear allocation of responsibilities. Additionally, the absence of redundancy means that most technical roles are performed by a single individual. This situation poses a high risk to business continuity, knowledge retention, and the resilience of digital public services.

94. **The pilot also shows that in many cases, individual staff members cover multiple roles simultaneously, which is recommended also in the current report, but should be pursued while still allowing role specialization.** At the same time, in some cases the lack of redundancy means that some critical functions depend on a single person. These patterns suggest that while existing operational roles provide a functional core, the overall mix of roles remains incomplete for

institutions aiming to modernize their digital services, govern complex systems or reduce reliance on external providers.

95. **Despite these limitations, the pilot confirms that the proposed set of ICT roles is applicable without requiring conceptual modification.** The role descriptions correspond closely to the responsibilities observed during the pilot, covering both the operational tasks already present in institutions and the more advanced functions required for future digitalization efforts. This alignment suggests that the role model itself does not require conceptual revision; rather, the main challenge lies in how roles are distributed, staffed and phased in across institutions with different levels of digital maturity.

96. **Instead, the pilot provided evidence that more effort is needed to develop strategies for implementation.** The findings show that operationalizing the ICT role set will require clear guidance, tailored to different organizational contexts, and a phased, capacity-building approach. Smaller ICT units, which typically operate with limited staffing, will need to combine several roles within the same position as a practical necessity. By **contrast**, institutions managing more complex or large-scale digital systems will need to progressively introduce the missing roles, broaden their technical functions, and expand team capacity over time. This staged approach allows the framework to be adopted realistically, ensuring that institutions can gradually align with the full role model while responding to their current capabilities and constraints.

97. **The pilot also demonstrates the need for more attention to supporting roles that are critical for high-quality digital services** - such as Business Analyst, Test Specialist, E-Government Specialist, Product Manager, and User Researcher. These roles ensure that digital solutions are well designed, tested, user-centered, and aligned with policy objectives.

98. **Strengthening ICT roles and capacity requires a phased and proportionate approach that reflects the varying levels of institutional complexity across the administration.** A first step could be to clarify and re-label existing ICT responsibilities using the new role taxonomy proposed under the TSI project, ensuring that current tasks are accurately reflected in job profiles. Building on this foundation, institutions can begin introducing the missing core roles that are appropriate for their category, for example, Systems Administrator or Technical Specialist in smaller organizations, and Systems Analyst, Developer or Test Specialist in medium-sized ones. As systems grow in scale or criticality, institutions may then expand into more advanced roles related to architecture, data governance and ICT operations management. In more mature environments, it becomes feasible to develop strategic roles such as Digital Transformation Leader, Product Manager or Business Information Manager, which help anchor digitalization within broader organizational objectives.

99. **A second priority is to improve redundancy within ICT teams.** The pilot found that many critical roles are carried out by only one specialist, creating operational and continuity risks. Institutions should therefore aim for at least two people to cover core functions such as systems administration, network operations, information security and technical support. Even partial overlap between roles can considerably strengthen resilience.

100. **In addition to core technical roles, the pilot highlighted the need to reinforce several support and cross-functional profiles that are essential for high-quality digital services.** These include Business Analysts, who can define requirements and reduce reliance on external vendors; Test Specialists, who ensure that systems meet users needs and required technical specifications before system roll-out; and E-Government Specialists and User Researchers, who help align digital services with user needs. Product Managers and Business Information Managers also play an important role in ensuring that digital services deliver value and remain consistent with

organizational priorities. Although these roles are less visible in current structures, they are necessary for sustainable digitalization.

101. **The pilot reconfirmed the need for a dedicated *digital transformation leadership role* positioned at the intersection of general digital competencies and specialized ICT functions but firmly rooted in the coordination architecture of the civil service management system – potentially at the level of General Secretary or Deputy General Secretary.** Across the piloted institutions, the exercise consistently highlighted gaps between ICT operational capacity, fragmented project ownership, and existing coordination of digital initiatives. Output 1 under the TSI project had also underlined that even when technical ICT roles are present to varying degrees, responsibility for aligning digital investments with policy priorities, service reform, and organizational change is often diffuse or informal. The pilot evidence therefore supports the creation of a formalized managerial role tasked with providing strategic direction, cross-departmental coordination, and institutional accountability for digital transformation – a function that complements specialized ICT leadership while anchoring digital governance at the highest administrative level where system-wide authority and integration capacity already exist.

102. **A further area for development concerns the broader governance environment in which ICT roles operate.** Institutions would benefit from formalizing medium-term ICT strategies, establishing clearer governance and decision-making structures, and adopting enterprise architecture principles. Strengthening cybersecurity policies and data governance frameworks, including interoperability standards, would also create the conditions needed for advanced ICT roles to function effectively and for digital initiatives to scale.

103. **Finally, at the sector level that oversees numerous subordinate entities, ICT coordination and collaboration can provide significant advantages.** In such contexts, roles such as Enterprise Architect, ICT Operations Manager or Information Security Manager may be more feasible and effective when organized centrally rather than replicated in each entity. By coordinating priorities, sharing technical expertise, and aligning systems and data standards, institutions can avoid fragmentation and ensure interoperability across services. Joint planning enables integrated digital solutions, reduces investment duplication, and improves cybersecurity. Moreover, a common governance framework supports faster decision-making, consistent implementation of digital policies, and the development of shared platforms that benefit the entire sector and the citizens.

9. At the intersection between general digital competencies and ICT roles: a *digital transformation coordinator*

104. **The need for a dedicated Digital Transformation Coordinator role emerges from the growing complexity of digital reform in the public administration.** Digital transformation can no longer be carried forward solely through specialized ICT structures or through general managerial roles acting independently. Effective implementation requires a civil service managerial function positioned at the intersection between ICT expertise and mainstream public-sector leadership – capable of bridging specialized technical domains with policy, service delivery, and organizational

management. This role responds directly to the pilot findings, which showed fragmentation between ICT operational capacity, strategic digital governance needs, and the responsibilities of general management across institutions.

105. The Digital Transformation Coordinator is therefore conceived as a senior managerial civil service role integrating two complementary dimensions of competence:

- (i) On one hand, the role must possess advanced general digital competencies in some areas, particularly at proficiency levels B and C, with Level C in the Digital Transformation competency area (Area 6) and in Digital Leadership and Governance (Area 7) - capturing leadership responsibilities for coordinating digital strategy, change management, and cross-institutional processes.
- (ii) On the other hand, the role requires a solid functional understanding of specialized ICT roles and job profiles, including ICT architecture, cybersecurity, digital service development, and operations management, as proposed in the ICT role classification framework.

106. While this position does not substitute technical ICT management roles, it enables informed strategic oversight, alignment with business priorities, and coherent integration of ICT delivery into broader institutional objectives.

107. At the institutional and system levels, this role anchors the digital transformation agenda within mainstream public sector leadership. The Digital Transformation Coordinator ensures that digital initiatives are not treated as isolated technical projects but as core instruments of service reform, administrative simplification, data governance, and process modernization. The pilot highlighted persistent risks where digital initiatives rely excessively on external providers, or remain disconnected from operational priorities. A senior internal coordinator with appropriate managerial authority mitigates these risks by providing continuity, institutional accountability, and strategic coherence across ICT units, core business departments, and executive management.

108. This proposed role aligns closely with international practice, particularly the Italian model of the “Responsabile della Transizione Digitale (RTD)” established under the Italian Digital Administration Code (CAD)²⁶. In Italy, the RTD is legally mandated as a managerial function responsible for coordinating digitization across administrations, including strategic planning, digital service development, interoperability, cybersecurity oversight, accessibility, and cross-government cooperation²⁷.

109. In the Romanian civil service, the Digital Transformation Coordinator role could be mapped to existing senior managerial positions, most naturally to General Secretaries or Deputy General Secretaries. These positions already hold cross-cutting coordination responsibilities and institutional authority, making them well suited to assume digital transformation leadership functions. **Output 2** of the TSI project further supports this approach by proposing dedicated managerial digital competencies with elevated proficiency expectations (Levels B and C)

²⁶ Details on the Italian example are included also in Output 1 developed under the TSI project. 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 Developing a General Digital Competency Framework for the Romanian civil service, 2025. Available at: <https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/099071725093059745>.

²⁷ <https://www.agid.gov.it/sites/agid/files/2024-06/Vademecum%20nomina%20RTD%20e%20UTD%20in%20forma%20associata.pdf>.

for these senior roles, particularly within the Digital Leadership and Governance competency area. Embedding the transformation coordination function within such established roles ensures consistency with current grading structures, avoids creating isolated digital posts, and strengthens institutional ownership of reform.

110. Effective operationalization of this role nevertheless requires targeted capacity building. The dual competency profile – combining advanced digital leadership skills with informed understanding of ICT roles and digital policy instruments – cannot be assumed automatically from existing managerial backgrounds. A tailored learning pathway is therefore necessary to equip incumbents with the specific competencies needed for the role. In this regard, a subsequent TSI project “*Competency-Based Staff Management in Romania’s public administration*” implemented with INA and NACS is designed to develop a targeted learning program precisely for digital transformation coordinating roles. The program will translate the digital leadership competencies defined under Output 2 into structured curricula, practical learning modules, and applied leadership development activities to ensure that Digital Transformation Coordinators are fully prepared to steer reform agendas effectively across Romania’s public administration.

111. The Digital Transformation Coordinator should be differentiated from the e-CF role of Digital Transformation Manager, given their scope and function. For improved coordination on digital transformation, the Digital Transformation Coordinator should be a senior civil-service governance role, embedded in top management responsible for providing strategic direction, cross-institutional coordination, and overall accountability for the digital transformation agenda. This role focuses on aligning policy, organizational reform, workforce development, and ICT investments, ensuring coherence between business units and ICT departments, and interfacing central authorities and external partners. By contrast, the Digital Transformation Manager included in the list of ICT roles proposed in this report is a specialized role, typically situated within ICT or digital delivery units, responsible for the hands-on management of specific digital programs and projects, including technical coordination, supplier management, timelines, budgets, and system implementation. This role relies predominantly on specialized ICT management and technical competencies, rather than on the cross-government leadership and coordination competencies that define the Digital Transformation Coordinator.

112. The e-Government specialist is the one who operationalizes the Coordinator's vision. While the Coordinator has a strategic (leadership) role, the e-Government specialist has a mixed expertise needed to design public services that are "digital by design" but also legally compliant. Acting as an ICT-oriented role within the digital delivery chain, the e-Government Specialist works closely with business analysts, architects, developers to define functional requirements, digital workflows and information models, and to ensure that legal and administrative rules are correctly embedded in system design, data structures and service logic throughout the ICT solution lifecycle.

10. Options for implementation of the proposed ICT roles and ICT job classification

113. The implementation of the proposed ICT roles and ICT job classification in the Romanian public administration can follow different governance arrangements. International practice shows three main models: centralized service centres, federated in-house expertise, and

hybrid approaches. Each model has distinct advantages and challenges in terms of efficiency, interoperability, flexibility, and workforce management. The following section sets out three possible options for Romania: a centralized expertise model, a federated expertise model, and a hybrid model that combines elements of both.

114. **The governance arrangements proposed below complement the detailed recommendations that were already developed by the Bank in its recent report on *Recommendations for attracting and retaining ICT staff in the public sector*²⁸, delivered to ADR in June 2025 under the Reimbursable Advisory Services (RAS) Agreement on Advice to Develop the Government Cloud Platform.**

10.1. Option 1: Centralized expertise model

115. **This option involves the development of specialized teams in a national shared ICT service centre.** Creating a national shared ICT service centre as a central hub for expertise is a proven governance model that improves the recruitment and retention of ICT specialists in the public sector. A National Shared ICT Services Centre is a unique organizational structure at the government level that unites specialized ICT teams in key areas and provides common services for all public institutions. Instead of each ministry, agency, or institution hiring and managing ICT staff separately, which can lead to fragmentation and duplication, the Shared Service Centre consolidates expertise and offers standardized, scalable, and more efficient services.

116. **In this setup, recruitment processes can be faster and more professional because technical evaluations are handled by specialized experts within the shared service.** Additionally, implementing the proposed unified competency framework in ICT enables the development of transparent and competitive salary structures.

117. **The Shared Service Center can be organized around specific services, depending on needs, which can group various ICT roles:** ICT architecture and interoperability, cybersecurity, application development and digital services for institutions upon request or of national interest, infrastructure and government cloud management, ICT support and services (centralized helpdesk), data analysis, etc. Public institutions could benefit from services provided by the Shared Service Center, upon request or as needed.

118. **Beyond financial mechanisms, the centralized model introduces additional flexibility** in workforce management, including options for remote or hybrid work across the national territory, temporary secondments between regions, and adaptable work schedules, all of which broaden the attractiveness of public sector ICT roles.

119. **From an organizational perspective, international evidence demonstrates the effectiveness of such models.** For example, Germany's ITZBund²⁹ and Austria's BRZ³⁰ have consolidated specialized expertise within shared service centers, enabling efficiency gains,

²⁸ World Bank, *Report with recommendations for attracting and retaining ICT staff in the public sector*, delivered in June 2025 under the Reimbursable Advisory Services (RAS) Agreement on Advice to Develop the Government Cloud Platform and to Migrate Selected Public Digital Services to the Cloud (P180766).

²⁹ <https://www.itzbund.de/DE/dasitzbund/ueberuns/ueberuns.html>.

³⁰ <https://www.brz.gv.at/en/>.

enhanced interoperability, and improved human resource management. Similarly, Estonia's RIA³¹ provides a centralized structure for digital and cybersecurity expertise, which supports the resilience of national digital infrastructure.

120. **Adopting cross-ministry mobility and structured secondments enables digital professionals to move into new roles without leaving government service.** This approach not only supports remote hiring but also extends career options. Simultaneously, Communities of Practice (CoPs) can be set up across key areas such as product management, design, engineering, and data, fostering knowledge sharing and collaborative innovation.

121. **With respect to staff retention, a centralized shared service can ensure clearer career pathways through transparent promotion criteria and mobility opportunities.** By providing an internal portfolio of assignments (internal project marketplace), ICT professionals may diversify their experience without leaving the system, thereby reducing attrition.

122. **Possible advantages of a centralized approach should not be ignored** if it defines a well-articulated national strategy, tested by the experience of other countries with a developed public administration:

- The grouping of ICT specialists at the central level would increase efficiency and generate significant savings nationwide. By concentrating ICT resources in a single centre, costs would be reduced through standardization and the elimination of redundancies.
- Access to ICT roles with rare skills and high levels of expertise would be possible through the recruitment of highly specialized professionals, who are difficult to attract to individual public institutions and smaller-scale organizations. The centre could manage the resources needed for major national interest projects.
- Improving strategic coherence and promoting inter-institutional interoperability would be possible through the unified implementation of national strategies (government cloud, digital identity, unified security standards, etc.).
- Attracting young talents by promoting a work model similar to the private sector would allow the development of modern and flexible work arrangements: remote working, hybrid, and secondments in the territory.

123. **The challenges induced by the centralized expertise model** are related to the high level of initial investments in reorganization, the inherent organizational change, managing resistance to change from public institutions, and minimizing the perception of excessive centralization. Additionally, in such situations, centralization can lead to the risk of a single point of failure, creating critical dependencies with national-level impact if problems occur during implementation.

124. **This first option still allows ICT specialists to be present within each institution, providing first- and second-level user support** and maintaining the connection with specialised teams in the national shared ICT service centre.

10.2. Option 2: Federated expertise model

125. **Under the second option, ICT core roles are embedded in each major public institution.** The federal model assumes that each major public institution (ministry, central agency, autonomous institution) develops and manages its own internal ICT teams, which cover the basic necessary roles: ICT management, system architecture, cybersecurity, infrastructure

³¹ <https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority>.

administration, application development, and user support. The overall coordination is carried out through government policies and standards, but the implementation and daily operation of ICT services remain at the level of each institution.

126. **In this approach, the definition of workforce planning will fall under the responsibility of a central institution with clearly defined prerogatives in this regard (MEDAT / ADR / SGG),** which will implement the framework of competencies and ICT roles at the national level. In this case, the need for ICT specialists in each public institution will be analyzed by this central authority, which will decide into which category of public institutions it will be classified, based on the systems it manages, and will determine which ICT roles will be necessary and what functions need to be defined. Common ICT roles for public institutions could be maintained in specialized departments. The highly specialized ICT roles that require high-level positions in the public ICT hierarchy should be maintained, in this approach, at the level of the specialists' centre and used in the implementation of large projects.

127. **The advantages of using such a model are linked to:** (1) flexibility and adaptation to the needs of each institution, which will be able to size and manage its own ICT department based on roles aligned with real needs, (2) a faster response to incident resolution or local requirements, without waiting for a response from the Shared Services centre depending on the priority assigned (increasing the institution's resilience in emergency situations), (3) increased autonomy for ICT management through direct control of the budget and allocated resources.

128. **The challenges induced by the federal approach relate to the risk of fragmentation,** which can lead to isolated solutions that are difficult to integrate, duplication of efforts and resources (multiple institutions may invest resources in implementing similar solutions), and difficulties in recruiting and retaining experts with highly specialized ICT roles.

10.3. Option 3: Hybrid approach

129. **The third option focuses on ensuring centralized leadership with decentralized implementation capacity.** The hybrid model combines the advantages of centralization and federalization of expertise at the central level, with strategic leadership and key competencies (architecture, interoperability, cybersecurity, ICT policies, data management). Institutionally, large ministries and agencies have their own ICT teams for implementation and daily operations, under the coordination of the central authority (MEDAT / ADR / SGG).

130. **This model is not disruptive; instead, it offers a balanced approach that maintains strategic coherence while allowing for autonomy.** Policies, standards, and critical infrastructure are centrally managed to ensure consistency, security, and, with proper coordination, interoperability. Nevertheless, institutions have the flexibility to customize implementations according to their own procedures and sector-specific needs (health, education, finance).

131. **This approach depends on clear coordination and governance structures.** It is crucial to establish explicit processes for setting standards, prioritizing projects, and assigning responsibilities. Without a robust governance framework, the model may become either overly centralized or too fragmented.

132. **Unlike the centralized model, the hybrid model involves greater complexity in human resource management.** This complexity is caused by the need to harmonize and coordinate

between the central level and the institutional level, involving additional investments in governance mechanisms (reporting systems, collaboration platforms).

133. **The options above can be combined within the Romanian public administration by applying sector-specific approaches**, such as distinct models for autonomous sectors like the Justice sector or the Ministry of Internal Affairs.

11. Recommendations and roadmap for implementation

134. **Romania needs to transition from generic roles in the ICT departments of public administration institutions to a unified description of the ICT role requirements**, using a common understanding based on the skill set for each role. Raising the visibility of ICT roles held by public servants or contractual staff is a key step in establishing a clear professional identity, moving beyond general titles like counsellor, inspector, or referent, at both institutional and national levels.

135. **Romania can adopt a customized ICT skills framework based on the e-CF standard, adapted to national realities and the specifics of public administration**. Prioritizing the clarification of ICT roles based on competencies, defining specific public functions for the ICT sector within public administration, consequently establishing a salary grid aligned with private sector standards, and ensuring comparable professional capacities are essential options for transforming the administrative framework in the upcoming period.

136. **Identifying a leading institution to oversee legislative initiatives and implement one of the proposed models is crucial for putting this report's recommendations into action**. MEDAT and ADR should serve as the primary entities responsible for promoting the new ICT role and job classification system and adopting the methodology for introducing this new classification.

137. **In defining how ICT functions should be staffed within the public administration, two main options can be preliminarily considered, in correlation also with the implementation model selected (chapter 7):**

I. **Option 1 – Mixed approach by role type**

Under this model, regular ICT positions (such as system administration, basic support, or routine maintenance) are carried out by civil servants, while specialized roles (such as cybersecurity experts, solution architects, or system architects) are filled by contractual staff. This separation allows the administration to maintain stability in core functions while bringing in specialized expertise where needed.

II. **Option 2 – Fully mixed approach**

In this scenario, both civil servants and contractual staff can occupy all types of ICT roles. This model enhances flexibility, enabling the administration to attract and retain talent more easily. Contractual staff can also collaborate with the private sector at the same time, creating opportunities for knowledge transfer and alignment with industry practices.

138. **Both options have advantages and limitations.** The first ensures continuity and institutional stability while reserving flexibility for specialized positions. The second provides maximum adaptability and opens the door to closer cooperation with the private sector, but requires careful governance to avoid conflicts of interest and ensure long-term institutional capacity.

139. **The pilot exercise also highlighted that the main adjustments needed for ICT roles relate to implementation strategy rather than role definitions.** The pilot points to the need for clear guidance on how to phase in the proposed roles over time, how to combine roles in smaller ICT units, and how to organize advanced functions at the sector or shared-service level where appropriate. Strengthening support and cross-functional roles – such as Business Analysts, Test Specialists, E-Government Specialists, Product Managers and User Researchers – will also be important for improving the quality, user-centeredness and reliability of digital public services. In parallel, the development of ICT strategies, governance arrangements, architecture principles and data/security frameworks will be necessary to create an enabling environment in which both the digital competency framework and the specialized ICT roles can be used effectively as levers for digital transformation.

140. **A phased implementation approach is necessary to ensure realistic, sustainable adoption of the reform package comprising the ICT role and job classification framework, the proposed Digital Transformation Coordinator managerial role, and the General Digital Competency Framework.** Institutions currently operate at very different levels of digital maturity, staffing capacity, and organizational complexity. A gradual rollout allows for initial clarification and formalization of roles, targeted piloting, and step-by-step scaling of staffing, training, and governance arrangements. This staged approach also enables calibration based on evidence, lessons learned from early adopters, and evolving reform priorities, ensuring that both general digital competencies and specialized ICT roles are embedded progressively without creating immediate implementation overload or unrealistic compliance requirements.

Table 14 Proposed phased implementation roadmap

Phase	Key measures
Phase 1 – Foundation and alignment (short term: 0–12 months)	Establish governance and ownership - Formal endorsement of the ICT role framework by the Chancellery, MEDET, NACS, ADR, Ministry of Public Administration and MLYSS. - Appointment of institutional focal points responsible for ICT workforce planning and coordination. - Establishment of a central coordination group to oversee phasing, guidance, and monitoring. Legal adoption of the proposed package Map existing capacities Apply the institutional and specialist surveys to assess: - Current ICT tasks, roles, and staffing. - System criticality and digital service portfolios. - Use of external service providers. Identify gaps, overlaps, and single-point dependencies across institutions. Re-label existing positions - Translate current job titles into the standardized ICT job taxonomy. - Identify “multi-role” positions in small institutions where combining roles is necessary.

	• Validate dominant roles per position using task-to-competence mapping. Define initial standards • Endorse minimum role coverage requirements by institutional category (small / medium / large / critical-system operators). • Approve principles on minimum dual coverage for critical functions (e.g., systems administration, cybersecurity, network operations). Improve governance frameworks • Institutionalize: ○ Medium-term ICT strategies. ○ Enterprise architecture standards. ○ Cybersecurity and interoperability frameworks. • Link ICT role planning to national digital strategies and EU alignment reporting.
Phase 2 – Staffing stabilization and redundancy (medium to long term: 2–4 years)	Fill in missing core roles • Prioritize establishment of operational and project-support roles: ○ Systems Administrator ○ Technical Specialist ○ Network Specialist ○ Cybersecurity Specialist ○ Systems/Business Analyst ○ Developer / Test Specialist ○ Data Management Specialist ○ E-government Specialist Introduce Digital Transformation Coordinators at managerial level. Training and certification • Launch competency-based training programs aligned with the proposed ICT roles and SFIA role expectations, and • Develop certification or micro-credential pathways for ICT and digital-transformation roles via INA and ADR, using blended learning models. Update job descriptions • Rewrite ICT job descriptions nationally using the standardized role profiles. • Embed competence expectations and required proficiency levels. • Align recruitment criteria and selection tests with the new profiles (with practical case tasks for technical roles). Recruit targeted profiles • Launch competitive campaigns for scarce roles • Utilize flexible staffing mechanisms: public–private mobility, secondees, project contracts where permitted. Build role redundancy • Ensure minimum two-person coverage for critical ICT functions in medium and large institutions. • Cross-train adjacent roles to prevent operational dependency on single individuals. Reduce external dependency • Gradually insource core functions: ○ Business analysis ○ Testing and quality assurance

	○ Data governance Retain outsourcing only for infrastructure operations, peak workloads and major systems developments.
Phase 4 – Consolidation and optimization (long term: 3–5 years) role specialization	Gradually separate combined roles in larger institutions. ● Enable sector-level pooling ● In sectors with multiple subordinate agencies, create shared ICT hubs for: ○ Enterprise architecture ○ Cybersecurity operations ○ Data governance ○ Platform management ● Promote cross-institution team models for high-cost expertise. Performance monitoring ● Use dashboard reporting to track: ○ Role coverage ratios. ○ Proficiency progression (via training completion and assessment). ○ Reduction of single-point dependency risks. ○ Shifts from outsourcing to internal provision. Framework updating ● Review ICT roles every 2-3 years in light of: ○ Emerging technologies (AI, data platforms, cybersecurity). ○ Changes in service portfolios. ○ EU competency framework updates. Evidence-based adjustments ● Use workforce data and pilot-style task mapping to refine: ○ Role definitions. ○ Seniority thresholds. Specialty training pathways.

141. **Effective implementation requires coordinated leadership across key public-sector stakeholders.** The Center of Government (through the Prime Minister’s Chancellery and related coordination structures) has a central role in setting reform priorities, ensuring cross-ministerial coherence, and anchoring the ICT roles as a priority for the digital transformation policy agenda. MEDET provides strategic policy leadership on digital transformation and public service modernization, ensuring alignment between workforce planning and national digital priorities. NACS is responsible for integrating digital competencies and ICT roles into recruitment, career management, and HRM regulations, while ADR ensures alignment with national digital standards, interoperability frameworks, cybersecurity policies, and technology governance. ADR should also gain a more prominent role in the management of the HRM system for ICT professionals. The Ministry of Labour aligns job classification and remuneration frameworks with the evolving public sector job classification grading and pay reform. Together, this institutional ecosystem forms the governance backbone necessary to translate the reform package into a coherent and sustainable implementation roadmap across the Romanian public administration.

Annex 1 Proposed ICT roles for the Romanian public administration (based on e-CF) and proposed levels of responsibility – for execution-level and managerial level jobs

Execution-level ICT roles

Table 15 Matrix proposed ICT roles for Romania PA and proposed levels of responsibility for execution positions.

e-CF role profile	Level 1 Follow	Level 2 Assist	Level 3 Apply	Level 4 Enable	Level 5 Ensure, advise
Business Analyst					Yes
Database Administrator (DBA)		Yes	Yes	Yes	Yes
Data Scientist		Yes	Yes	Yes	Yes
Data Specialist		Yes	Yes	Yes	Yes
Developer		Yes	Yes	Yes	Yes
Enterprise Architect					Yes
E-Government Specialist				Yes	Yes
ICT Operations Manager					Yes
ICT Specialist					Yes
Information Security Specialist		Yes	Yes	Yes	Yes
ICT Specialist		Yes	Yes	Yes	Yes
Network Specialist	Yes	Yes	Yes	Yes	Yes, as team lead
Product Manager					Yes
Service Designer					Yes

e-CF role profile	Level 1 Follow	Level 2 Assist	Level 3 Apply	Level 4 Enable	Level 5 Ensure, advise
Service Support	Yes	Yes	Yes	Yes	
Solution Designer				Yes	Yes
Systems Administrator		Yes	Yes	Yes	Yes
Systems Analyst			Yes	Yes	Yes
Technical Specialist				Yes	Yes
Test Specialist		Yes	Yes	Yes	Yes - team lead in large ICT Units
User Researcher				Yes	Yes

Proposed managerial ICT roles

Table 16 Matrix proposed ICT roles for the Romanian public administration PA and proposed levels of responsibility for managerial positions.

e-CF role profile	Level 5 Ensure, advise	Level 6 Initiate, influence	Level 7 Set strategy, inspire, mobilize	Management levels
Business Analyst	Yes	Yes		
Business Information Manager		Yes	Yes	
Chief Information Officer (CIO)				All levels 6 and 7 for ICT Director 8 and 9 for CIO
Digital Transformation Leader		Yes	Yes	
Enterprise Architect	Yes	Yes		
E-Government Specialist	Yes	Yes		
ICT Operations Manager				All levels 6 and 7 for ICT Operational manager 8 and 9 for CTO
ICT Specialist	Yes	Yes		
Information Security Manager				All levels 6 and 7 for Information Security manager 8 and 9 for CSO - see ECSF
Product Manager		Yes	Yes	

Official Use Only

e-CF role profile	Level 5 Ensure, advise	Level 6 Initiate, influence	Level 7 Set strategy, inspire, mobilize	Management levels
Service Designer	Yes	Yes		
Systems Architect		Yes	Yes	

Annex 2 Mapping of competencies and overlapping competences across the proposed ICT roles

SYSTEMS ADMINISTRATOR		
Competences	Levels	Main tasks
B.2. Component Integration	e2-e4	Investigate, diagnose and solve system related problems
B.3. Testing	e1-e4	Install and upgrades software
C.2. Change Support	e2-e3	Test upgrades
C.4. Problem Management	e2-e4	Schedule installation work, to minimize disruption
E.8. Information Security Management	e2-e4	Diagnose and solve hardware or software problems
		Comply with organisation procedures to ensure integrity and security of the system

DEVELOPER		
Competences	Levels	Main tasks
B.1. Application Development	e1-e3	Develop engineer and integrate components
B.2. Component Integration	e2-e4	Follow user experience guidelines
B.3. Testing	e1-e4	Aware of and address known security vulnerabilities, applying security by design
B.5. Documentation Production	e1-e3	Shape documentation
C.4. Problem Management	e2-e4	Provide advanced, component technical support
		Resolve issues prior to and following testing

SERVICE SUPPORT

Competences	Levels	Main tasks
C.1. User Support	e1-e3	Identify and diagnose issues and problems
C.2. Change Support	e2-e3	Categorize and record reported queries and provide solutions
C.3. Service Delivery	e1-e3	Support problem identification
C.4. Problem Management	e2-e4	Advise users on appropriate course of action
		Monitor issues from start to resolution
		Escalate, if needed, unresolved problems to a higher level of support
		Provide essential online security advice and support

TECHNICAL SPECIALIST		
Competences	Levels	Main tasks
C.2. Change Support	e2-e3	Identify software and hardware problems and repair
C.3. Service Delivery	e1-e3	Perform regular maintenance on hardware and software components
C.4. Problem Management	e2-e4	Install cables and configures hardware and software
E.3. Risk Management	e2-e4	Document system addresses and configurations
E.6. ICT Quality Management	e2-e4	Run diagnostic programs or use test equipment to locate source of problems
		Communicate effectively with end users and customer management
		Maintain security and functionality through application of program temporary fixes

INFORMATION SECURITY SPECIALIST		
Competences	Levels	Main tasks
A.7. Technology Trend Monitoring	e3-e5	Evaluate information security risks, threats and consequences and take appropriate action
A.9. Innovating	e4-e5	Provide information security training and education
D.1. Information Security Strategy Development	e4-e5	Provide technical validation of security tools, implement, configure and manage appropriate tools
D.3. Education and Training Provision	e2-e3	Contribute to the definition of and actively promote information security standards and procedures throughout the ICT and ICT user communities
E.3. Risk Management	e2-e4	Identify and remediate security vulnerabilities

		Audit security vulnerability
		Monitor security developments to ensure the continued efficiency and effectiveness of information security processes and controls
		Proactively evaluate new threats and counter potential information security incidents
		Implements security techniques on all or part of an application, process, network or system within area of responsibility

NETWORK SPECIALIST		
Competences	Levels	Main tasks
A.6. Application Design	e1-e3	Ensure communication performance, recovery, and security needs meet agreed service agreement standards
B.2. Component Integration	e2-e4	Contribute to define network design policies, philosophies and criteria
B.4. Solution Deployment	e1-e3	Investigate, diagnose and solve network problems
C.4. Problem Management	e2-e4	Use network management system tools to determine network load and model performance statistics
E.8. Information Security Management	e2-e4	Maintain awareness of relevant legislation affecting network security
		Configure network to protect against security threats
		Monitor network to identify and address traffic bottle necks

DATABASE ADMINISTRATOR		
Competences	Levels	Main tasks
B.1. Application Development	e1-e3	Apply standards methods and tools for measuring and reporting on wide set of relevant performance indicators (response time, availability, safety, integrity)
B.2. Component Integration	e2-e4	Produce data set procedures and instructions for other analysts or administrators
C.2. Change Support	e2-e3	Monitor and maintain data management systems
D.10. Information and Knowledge Management	e3-e5	Ensure the integrity and security of existing data management systems
E.8. Information Security Management	e2-e4	Identify, investigate and correct problems or incidents related to data management systems
		Provide training, support, advice and guidance on data set issues to other information system practitioners

BUSINESS ANALYSTS		
Competences	Levels	Main tasks
A.1. IS and Business Strategy Alignment	e4-e5	Contribute to the preparation of the organisation's business plan
A.3. Business Plan Development	e3-e5	Analyse business requirements and design related processes
D.10. Information and Knowledge Management	e3-e5	Support Digital Transformation, identifying areas for improvement in business processes
D.11. Needs Identification	e3-e5	Provide possible ICT solutions compliant with the ICT strategy
E.5. Process Improvement	e3-e4	Develop business cases related to the proposed solutions
		Analyse required information and documents
		Develop plan for continuity of operations

DATA SPECIALIST		
Competences	Levels	Main tasks
A.6. Application Design	e1-e3	Define, build and optimise data models
D.10. Information and Knowledge Management	e3-e5	Proactively protect confidentiality and security of data
E.6. ICT Quality Management	e2-e4	Ensure data lifecycle support
E.8. Information Security Management	e2-e4	Curate and archive data
		Advise on appropriate data analytic methodology
		Ensure data quality and integrity
		Maintain data quality and compliance to legal standards

DIGITAL TRANSFORMATION LEADER		
Competences	Levels	Main tasks
A.3. Business Plan Development	e3-e5	Shape and deliver a digital strategy
A.5. Architecture Design	e3-e5	Develop awareness and education to improve digital capability
A.9. Innovating	e4-e5	Demonstrate the benefits of digital transformation implementation
E.7. Business Change Management	e3-e5	Advise and support on a 'digital by design' approach
E.9. Information Systems Governance	e4-e5	Lead cultural change required to facilitate digital strategy
		Lead and mobilise key organisation influencers to implement digital transformation

BUSINESS INFORMATION MANAGER		
Competences	Levels	Main tasks
A.1. IS and Business Strategy Alignment	e4-e5	Manage the information and communication technology development focused on user needs
A.3. Business Plan Development	e3-e5	Prepare for changes to the Information System influenced by technology updates or user needs
E.4. Relationship Management	e3-e4	Formalise, consolidate and drive the development of the IS configuration
E.7. Business Change Management	e3-e5	Evaluate the relevance of the Information Systems to users
E.9. Information Systems Governance	e4-e5	Liaise between the user community and the IS infrastructure
		Translate user requirements into functional specifications

CHIEF INFORMATION OFFICER		
Competences	Levels	Main tasks
A.1. IS and Business Strategy Alignment	e4-e5	Enable the company's digital strategy
A.3. Business Plan Development	e3-e5	Define and implement ICT strategy and ICT governance
E.2. Project and Portfolio Management	e2-e5	Ensure the reliability, confidentiality, security and integrity of Information Systems
E.4. Relationship Management	e3-e4	Ensure the quality and management of ICT customer-supplier relationships in particular contracts
E.9. Information Systems Governance	e4-e5	Define and ensure compliance with Service Level Agreements
		Ensure that ICT change management processes are implemented

ENTERPRISE ARCHITECT		
Competences	Levels	Main tasks
A.1. IS and Business Strategy Alignment	e4-e5	Align digital and ICT strategies and planning with the organisation's business goals
A.3. Business Plan Development	e3-e5	Anticipate future business needs and plan for how architecture will support/enable it
A.5. Architecture Design	e3-e5	Streamline business processes, functions, procedures and workflows and apply a consistent implementation approach

A.7. Technology Trend Monitoring	e3-e5	Manage stakeholder engagement in the development of new processes and systems and verifies feasibility
E.8. Information Security Management	e2-e4	Conduct post-implementation reviews to evaluate benefits accrued from new processes and systems
		Build and maintain standards and enterprise architecture model and principles, for example process mapping
		Evaluate the impact of changes within the ecosystem of the organisation (including political, technical, social, regulatory, legal) on the enterprise architecture

ICT OPERATIONS MANAGER		
Competences	Levels	Main tasks
D.9. Personnel Development	e2-e4	Coordinate and manage staff
E.2. Project and Portfolio Management	e2-e5	Direct, organize, plan and monitor activities
E.3. Risk Management	e2-e4	Negotiate the objectives and resources
E.6. ICT Quality Management	e2-e4	Manage the departmental budget
E.8. Information Security Management	e2-e4	Establish and monitor management information
		Analyse and propose solutions for continuous productivity improvement
		Manage the implementation and monitoring of IS quality assurance and security
		Communicate with internal business departments and project owners

INFORMATION SECURITY MANAGER		
Competences	Levels	Main tasks
A.7. Technology Trend Monitoring	e3-e5	Define the information security strategy and standards
D.1. Information Security Strategy Development	e4-e5	Contribute to the development of the organisation's security policy
E.3. Risk Management	e2-e4	Manages security audits
E.8. Information Security Management	e2-e4	Evaluate risks, threats and consequences
E.9. Information Systems Governance	e4-e5	Establish and manage prevention, detection, correction and remediation plans
		Inform and raise awareness among general management and across all ICT users and professionals
		Conduct information security operations

SERVICE MANAGER		
Competences	Levels	Main tasks
A.2. Service Level Management	e3-e4	Define Service requirements
C.3. Service Delivery	e1-e3	Negotiate SLA / OLA
C.4. Problem Management	e2-e4	Manage solution operation
D.8. Contract Management	e2-e4	Provide service delivery
D.9. Personnel Development	e2-e4	Maintain and contribute to the creation of the department budget
		Manage staff development

SYSTEMS ANALYST		
Competences	Levels	Main tasks
A.5. Architecture Design	e3-e5	Analyse existing systems and business models
B.5. Documentation Production	e1-e3	Recommend resolutions and improvements
B.6. ICT Systems Engineering	e3-e4	Provide integrated solutions
E.6. ICT Quality Management	e2-e4	Provide consolidate findings on components or processes
		Author technical performance requirements
		Ensure security by design
		Maps and documents interfaces between legacy and new systems

SYSTEMS ARCHITECT		
Competences	Levels	Main tasks
A.5. Architecture Design	e3-e5	Specify and implement the architecture of complex ICT solutions
A.7. Technology Trend Monitoring	e3-e5	Lead development and integration of components
A.9. Innovating	e4-e5	Lead and/ or conduct system integration
B.2. Component Integration	e2-e4	Ensure incorporation of security by design
B.6. ICT Systems Engineering	e3-e4	Analyse technical and business requirements

		Develop and maintain a comprehensive record of usability requirements
--	--	---

TEST SPECIALIST

Competences	Levels	Main tasks
B.2. Component Integration	e2-e4	Select and develop integration testing techniques to ensure the system meets requirements.
B.3. Testing	e1-e4	Design and customize integration tests, identify open issues.
B.4. Solution Deployment	e1-e3	Organise test plans and procedures for white and black box testing at unit, module, system and integration levels.
B.5. Documentation Production	e1-e3	Establish procedures for result analysis and reporting.
E.3. Risk Management	e2-e4	Design and implement defect tracking and correction procedures
		Write test program to assess software quality
		Develop tools to increase test effectiveness

SOLUTION DESIGNER

Competences	Levels	Main tasks
A.6. Application Design	e1-e3	Examine and interpret business requirements
A.9. Innovating	e4-e5	Establish solution intent
D.10. Information and Knowledge Management	e3-e5	Align solution with technical architecture
D.11. Needs Identification	e3-e5	Identify potential technical design risks
		Supervise the built in quality
		Operate within the budgetary framework to validate the financial impact of design decisions
		Identify opportunities for innovation
		Plan technology roadmaps

DATA SCIENTIST

Competences	Levels	Main tasks
A.7. Technology Trend Monitoring	e3-e5	Represent business challenges through mathematical models

A.9. Innovating	e4-e5	Collect, understand, clean, analyse, integrate and investigate internal and external data to achieve the mission
D.10. Information and Knowledge Management	e3-e5	Create and test hypothesis
D.11. Needs Identification	e3-e5	Uncover data correlations/relationships in support of measurement and predication
E.1. Forecast Development	e3-e4	Identify the right visualisation models depending on the business challenges and the data sets
		Address data security through active preventative strategies
		Select and optimise algorithms using data science tools
		Comply with ethical guidelines and legal requirements

ICT specialist ³²		
Competences (a selection of maximum five to be selected for a position)	Levels	Main tasks (in accordance with selected competences)
A.1. IS and Business Strategy Alignment	e4-e5	Support delivery of digital projects (requirements, documentation, sprint activities, testing, deployment)
A.3. Business Plan Development	e3-e5	Assist DevOps and operations teams with configuration, monitoring, troubleshooting
A.6. Application Design	e1-e3	Define, build and optimise data models
B.1. Application Development	e1-e3	Apply standards methods and tools for measuring and reporting on wide set of relevant performance indicators (response time, availability, safety, integrity)
B.2. Component Integration	e2-e4	Facilitate collaboration with IT departments of subordinate agencies
B.3. Testing	e1-e4	Support ICT governance, cybersecurity compliance, standardisation and interoperability
B.4. Solution Deployment	e1-e3	Contribute to service management processes (incident, problem, change)
D.10. Information and Knowledge Management	e3-e5	Provide user support and help improve digital services
C.1. User Support	e1-e3	Support digital communication tasks when required
C.2. Change Support	e2-e3	Provide guidance on search engine optimisation (SEO)
C.4. Problem Management	e2-e4	Test and resolve any technical, usability and accessibility issues

³² Manage specific tasks defined in other eCF roles, but not very specific for the public administration from Romania (DevOps Expert, Digital Media Specialist, Product Owner, Project Manager, Scrum Master, Service Manager)

D.2. ICT Quality Strategy Development	e4-e5	Help team improve and take responsibility for their actions to deploy agile values, principles and practices
E.2. Project and Portfolio Management	e2-e5	Direct, organize, plan and monitor activities
E.4. Relationship Management	e3-e4	Coordinate, record and ensure quality compliance
E.6. ICT Quality Management	e2-e4	Ensure the project helps to support the organisation's wider goals
		Comply with ethical guidelines and legal requirements

Annex 3. Proposed ICT Roles description, competencies and levels (first 10 more used roles)

e-CF role profile	Description	Competencies and e-CF levels
Developer	<u>Mission:</u> Ensures building and implementing of ICT applications. Contributes to low-level design. Writes code to ensure optimum efficiency and functionality and user experience. <u>Summary:</u> Designs and/ or codes components to meet solution specifications. <u>Main tasks:</u> Develop engineer and integrate components Follow user experience guidelines Aware of and address known security vulnerabilities, applying security by design Shape documentation Provide advanced, component technical support Resolve issues prior to and following testing	<u>Application Development</u> Interprets the application design to develop a suitable application in accordance with customer needs. Adapts existing solutions by e.g. porting an application to another operating system. Codes, debugs, tests and documents and communicates product development stages. Selects appropriate technical options for development such as reusing, improving or reconfiguration of existing components. Optimises efficiency, cost and quality. Validates results with user representatives, integrates and commissions the overall solution. Level 1 Acts under guidance to develop, test and document applications. Level 2 Systematically develops and validates applications. Level 3 Acts creatively to develop applications and to select appropriate technical options. Accounts for others development activities. Optimizes application development, maintenance and performance by employing design patterns and by reusing proved solutions. Level 4 - Not applicable Level 5 - Not applicable <u>Component Integration</u> Integrates hardware, software or sub system components into an existing or a new system. Complies with established processes and procedures such as, configuration management and package maintenance. Takes into account the compatibility of existing and new modules to ensure system integrity, system interoperability and information security. Verifies and

tests system capacity and performance and documentation of successful integration.

Level 1: Not applicable

Level 2: Acts systematically to identify compatibility of software and hardware specifications. Documents all activities during installation and records deviations and remedial activities

Level 3: Accounts for own and others actions in the integration process. Complies with appropriate standards and change control procedures to maintain integrity of the overall system functionality and reliability.

Level 4: Exploits wide ranging specialist knowledge to create a process for the entire integration cycle, including the establishment of internal standards of practice. Provides leadership to marshal and assign resources for programs of integration.

Level 1: Not applicable

Testing

Constructs and executes systematic test procedures for ICT systems or customer usability requirements to establish compliance with design specifications. Ensures that new or revised components or systems perform to expectation. Ensures meeting of internal, external, national and international standards; including health and safety, usability, performance, reliability or compatibility. Produces documents and reports to evidence certification requirements.

Level 1 Performs simple tests in strict compliance with detailed instructions.

Level 2 Organises test programs and builds scripts to stress test potential vulnerabilities. Records and reports outcomes providing analysis of results.

Level 3 Exploits specialist knowledge to supervise complex testing programmes. Ensures tests and results are documented to provide input to subsequent process owners such as designers, users or maintainers.

Accountable for compliance with testing procedures including a documented audit trail.

Level 4 Exploits wide ranging specialist knowledge to create a process for the entire testing activity, including the establishment of internal standard of practices.

Provides expert guidance and advice to the testing team.

Level 5 - Not applicable

Documentation Production

Produces documents by integrating information and maintaining compliance with relevant requirements.

Selects the appropriate style and format by determining the media type and presentation mode of the documentation. Creates templates for document-management systems. Ensures that documentation complies with customers', technical and ICT application development process needs and that existing documents are valid and up to date. Provides support for the development of interactive documents.

Level 1 Uses and applies standards to define document structure.

Level 2 Ensures that documentation is complete, correct and provided in a suitable place and format.

Level 3 Adapts the level of detail to meet the needs of the targeted population.

Level 4 - Not applicable

Level 5 - Not applicable

Problem Management

Manages the life cycle of incidents and problems.

Identifies and resolves the root cause of incidents. Takes a proactive approach to avoidance or identification of root cause of ICT problems. Deploys a knowledge system based on recurrence of common errors. Resolves or escalates incidents. Optimises system or component performance.

Level 1 - Not applicable

		Level 2 Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution. Level 3 Exploits specialist knowledge and in-depth understanding of the ICT infrastructure and problem management process to identify failures and resolve with minimum outage. Makes sound decisions in emotionally charged environments on appropriate action required to minimise business impact. Rapidly identifies failing component, selects alternatives such as repair, replace or reconfigure. Level 4 Provides leadership and is accountable for the entire problem management process. Schedules and ensures well trained human resources, tools, and diagnostic equipment are available to meet emergency incidents. Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. Constructs escalation processes to ensure that appropriate resources can be applied to each incident. Level 5 - Not applicable
Cybersecurity (Information Security) Specialist	Summary: Ensures the implementation of the organisation's information security policy by the secure and appropriate use of ICT resources. Mission: Defines, proposes and implements necessary information security techniques and practices in compliance with information security standards and procedures. Contributes to security practices, awareness and compliance by providing advice, support, information and training. Tasks: Evaluate information security risks, threats and consequences and take appropriate action	<u>Technology Trend Monitoring</u> Investigates latest ICT technological developments to establish understanding of evolving technologies. Encourages and explores internal and external sources (including e.g. research activities, patents, start-up activities, digital communities) for innovative ideas and opportunities. Devises innovative solutions for the adoption or integration of existing or new technology and/or ideas into existing products, applications or services or for the creation of new ones. Level 1 - Not applicable Level 2 - Not applicable Level 3 Detects signs of change to provide supervision and analysis of current and trend-setting ICT technological developments. Establishes relationships with relevant communities. Level 4 Validates new and emerging technologies, coupled with expert understanding of the business, to

Provide information security training and education
 Provide technical validation of security tools, implement, configure and manage appropriate tools
 Contribute to the definition of and actively promote information security standards and procedures throughout the ICT and ICT user communities
 Identify and remediate security vulnerabilities
 Audit security vulnerability
 Monitor security developments to ensure the continued efficiency and effectiveness of information security processes and controls
 Proactively evaluate new threats and counter potential information security incidents
 Implements security techniques on all or part of an application, process, network or system within area of responsibility

envision and articulate solutions for the future. Creates the organisation wide trend monitoring processes.
 Level 5 Plans and leads an organisational structure and support system for systematic technology watch. Advises and influences strategic decisions envisioning and articulating future ICT solutions.

Innovating

Devises creative solutions for the provision of new concepts, ideas, products or services. Deploys novel and open thinking to envision exploitation of technological advances to address business / society needs or research direction.

Level 1 - Not applicable

Level 2 - Not applicable

Level 3 - Not applicable

Level 4 Applies independent thinking and technology awareness to lead the integration of disparate concepts for the provision of unique solutions.

Level 5 Provides strategic leadership for the introduction of new concepts. Guides innovation approaches and leads the cultural change to innovation.

Information Security Strategy Development

Defines and makes applicable a formal organisational strategy, scope and culture to maintain safety and security of information from external and internal threats. Analyses the business and technology strategy alongside trends in the threat landscape to anticipate potential vulnerabilities and risk mitigation requirements. Tracks legal, regulatory and social expectations involving the security of services and sensitive data. Provides the foundation for Information Security Management, including role identification and accountability. Uses defined standards to create objectives for information integrity, availability, and data privacy.

Level 1 - Not applicable

Level 2 - Not applicable

Level 3 - Not applicable

Level 4 Exploits depth of expertise and leverages external standards and best practices
Level 5 Provides strategic leadership to embed information security into the culture of the organization

Education and Training Provision

Defines and implements ICT training policy to address organisational skill needs and gaps. Incorporates these onto internal employee development plans as a tool for enabling career development. Structures, organises and schedules training programs and evaluates training quality through a feedback process and implements continuous improvement. Adapts training plans to address changing demand.

Level 1 -Not applicable

Level 2 Organises the identification of training needs; collates organisation requirements, identifies, selects and prepares schedule of training interventions.

Level 3 Acts creatively to analyse skills gaps; elaborates specific requirements and identifies potential sources for training provision. Has specialist knowledge of the training market and establishes a feedback mechanism to assess the added value of alternative training programmes.

Level 4 -Not applicable

Level 5 -Not applicable

Risk Management

Implements the management of risk across information systems through the application of the enterprise defined risk management policy and procedure. Assesses risk to the organisation's business, including web, cloud and mobile resources. Documents potential risk and containment plans.

Level 1 - Not applicable

Level 2 Understands and applies the principles of risk management and investigates ICT solutions to mitigate identified risks.

Level 3 Decides on appropriate actions required to adapt security and address risk exposure. Evaluates, manages

		and ensures validation of exceptions; audits ICT processes and environment. Level 4 Provides leadership to define and make applicable a policy for risk management by considering all the possible constraints, including technical, economic and political issues. Delegates assignments. Level 5 - Not applicable
Service Support	Summary: Provides remote or onsite diagnosis or guidance to internal or external clients with technical issues. Mission: Provides user support and troubleshoots ICT problems and issues. The primary objective is to enable users to maximize their productivity through efficient and secure use of ICT equipment or software applications. Tasks: - Identify and diagnose issues and problems - Categorize and record reported queries and provide solutions - Support problem identification - Advise users on appropriate course of action - Monitor issues from start to resolution - Escalate, if needed, unresolved problems to a higher level of support - Provide essential online security advice and support	<u>User Support</u> Responds to user requests and issues, recording relevant information. Assures resolution or escalates incidents and optimises system performance in accordance with predefined service level agreements (SLAs). Understands how to monitor solution outcome and resultant customer satisfaction. Level 1 Interacts with users, applies basic product knowledge to respond to user requests. Solves incidents, following prescribed procedures. Level 2 Systematically interprets user problems and identifies solutions and possible side effects. Uses experience to address user problems and interrogates database for potential solutions. Escalates complex or unresolved incidents. Records and tracks issues from outset to conclusion. Level 3 Manages the support process and accountable for agreed SLA. Plans resource allocation to meet defined service level. Acts creatively, and applies continuous service improvement. Manages the support function budget. Level 4 - Not applicable Level 5 - Not applicable <u>Change Support</u> Evaluates, implements and guides the evolution of an ICT solution evaluating changes and their impact. Ensures efficient control and scheduling of software or hardware modifications to prevent multiple upgrades creating unpredictable outcomes. Minimises service disruption as a consequence of changes and adheres to defined service

level agreement (SLA). Ensures consideration and compliance with information security procedures.

Level 1 - Not applicable

Level 2 During change, acts systematically to respond to day by day operational needs and react to them, avoiding service disruptions and maintaining coherence to (SLA) and information security requirements.

Level 3 Ensures the integrity of the system by controlling the application of functional updates, software or hardware additions and maintenance activities. Complies with budget requirements.

Level 4 - Not applicable

Level 5 - Not applicable

Service Delivery

Ensures service delivery in accordance with established service level agreements (SLA's). Takes proactive action to ensure stable and secure applications and ICT infrastructure to avoid potential service disruptions, attending to capacity planning and to information security. Updates operational document library and logs all service incidents. Maintains monitoring and management tools (i.e. scripts, procedures). Maintains IS services. Manages all aspects of service availability.

Level 1 Acts under guidance to record and track reliability data.

Level 2 Systematically analyses performance data and communicates findings to senior experts. Escalates potential service level failures and security risks, recommends actions to improve service reliability. Tracks reliability data against SLA.

Level 3 Plans the schedule of operational tasks. Manages costs and budget according to the internal procedures and external constraints. Identifies the optimum number of people required to resource the operational management of the IS infrastructure.

Level 4 - Not applicable

Level 5 - Not applicable

		<u>Problem Management</u> Manages the life cycle of incidents and problems. Identifies and resolves the root cause of incidents. Takes a proactive approach to avoidance or identification of root cause of ICT problems. Deploys a knowledge system based on recurrence of common errors. Resolves or escalates incidents. Optimises system or component performance. Level 1 - Not applicable Level 2 Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution. Level 3 Exploits specialist knowledge and in-depth understanding of the ICT infrastructure and problem management process to identify failures and resolve with minimum outage. Makes sound decisions in emotionally charged environments on appropriate action required to minimise business impact. Rapidly identifies failing component, selects alternatives such as repair, replace or reconfigure. Level 4 Provides leadership and is accountable for the entire problem management process. Schedules and ensures well trained human resources, tools, and diagnostic equipment are available to meet emergency incidents. Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. Constructs escalation processes to ensure that appropriate resources can be applied to each incident. Level 5 - Not applicable
Technical Specialist	Summary: Maintains and repairs hardware, software and service applications. Mission: Effectively maintains customer hardware/software. Responsible for delivering timely and effective repairs to ensure optimal system	<u>Change Support</u> Evaluates, implements and guides the evolution of an ICT solution evaluating changes and their impact. Ensures efficient control and scheduling of software or hardware modifications to prevent multiple upgrades creating unpredictable outcomes. Minimises service disruption as a consequence of changes and adheres to defined service

performance and superior customer satisfaction. Tasks: - Identify software and hardware problems and repair - Perform regular maintenance on hardware and software components - Install cables and configures hardware and software - Document system addresses and configurations - Run diagnostic programs or use test equipment to locate source of problems - Communicate effectively with end users and customer management - Maintain security and functionality through application of program temporary fixes	level agreement (SLA). Ensures consideration and compliance with information security procedures. Level 1 - Not applicable Level 2 During change, acts systematically to respond to day by day operational needs and react to them, avoiding service disruptions and maintaining coherence to (SLA) and information security requirements. Level 3 Ensures the integrity of the system by controlling the application of functional updates, software or hardware additions and maintenance activities. Complies with budget requirements. Level 4 - Not applicable Level 5 - Not applicable <u>Service Delivery</u> Ensures service delivery in accordance with established service level agreements (SLA's). Takes proactive action to ensure stable and secure applications and ICT infrastructure to avoid potential service disruptions, attending to capacity planning and to information security. Updates operational document library and logs all service incidents. Maintains monitoring and management tools (i.e. scripts, procedures). Maintains IS services. Manages all aspects of service availability. Level 1 Acts under guidance to record and track reliability data. Level 2 Systematically analyses performance data and communicates findings to senior experts. Escalates potential service level failures and security risks, recommends actions to improve service reliability. Tracks reliability data against SLA. Level 3 Plans the schedule of operational tasks. Manages costs and budget according to the internal procedures and external constraints. Identifies the optimum number of people required to resource the operational management of the IS infrastructure. Level 4 - Not applicable Level 5 - Not applicable
---	---

Problem Management

Manages the life cycle of incidents and problems. Identifies and resolves the root cause of incidents. Takes a proactive approach to avoidance or identification of root cause of ICT problems. Deploys a knowledge system based on recurrence of common errors. Resolves or escalates incidents. Optimises system or component performance.

Level 1 - Not applicable

Level 2 Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution.

Level 3 Exploits specialist knowledge and in-depth understanding of the ICT infrastructure and problem management process to identify failures and resolve with minimum outage. Makes sound decisions in emotionally charged environments on appropriate action required to minimise business impact. Rapidly identifies failing component, selects alternatives such as repair, replace or reconfigure.

Level 4 Provides leadership and is accountable for the entire problem management process. Schedules and ensures well trained human resources, tools, and diagnostic equipment are available to meet emergency incidents. Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. Constructs escalation processes to ensure that appropriate resources can be applied to each incident.

Level 5 - Not applicable

Risk Management

Implements the management of risk across information systems through the application of the enterprise defined risk management policy and procedure. Assesses risk to the organisation's business, including web, cloud and mobile resources. Documents potential risk and containment plans.

		Level 1 - Not applicable Level 2 Understands and applies the principles of risk management and investigates ICT solutions to mitigate identified risks. Level 3 Decides on appropriate actions required to adapt security and address risk exposure. Evaluates, manages and ensures validation of exceptions; audits ICT processes and environment. Level 4 Provides leadership to define and make applicable a policy for risk management by considering all the possible constraints, including technical, economic and political issues. Delegates assignments. Level 5 - Not applicable <u>ICT Quality Management</u> Implements ICT quality policy to maintain and enhance service and product provision. Plans and defines indicators to manage quality with respect to ICT strategy. Reviews quality measures and recommends enhancements to influence continuous quality improvement. Level 1 - Not applicable Level 2 Communicates and monitors application of the organisation's quality policy. Level 3 Evaluates quality management indicators and processes based on ICT quality policy and proposes remedial action. Level 4 Assesses and estimates the degree to which quality requirements have been met and provides leadership for quality policy implementation. Provides cross functional leadership for setting and exceeding quality standards. Level 5 - Not applicable
Business Analyst	Mission: Analyses the information and the processes needed to support business plans. Formulates functional and non-functional requirements of the business organisation and advises on the lifecycle	A.1. IS and Business Strategy Alignment Anticipates long term business requirements, influences improvement of the organisation's process efficiency and effectiveness. Determines the IS model and enterprise architecture maintaining consistency with organisational

of the information solutions. Evaluates the impact in terms of change management.

Summary: Analyses the business domain and optimises business performance through technology application.

Main tasks:

Contribute to the preparation of the organisation's business plan

Analyse business requirements and design related processes

Support Digital Transformation, identifying areas for improvement in business processes

Provide possible ICT solutions compliant with the ICT strategy

Develop business cases related to the proposed solutions

Analyse required information and documents

Develop plan for continuity of operations

policy and ensuring a secure environment. Recognises potential risks and business requirements to assure resilience in the alignment of systems and services to the business strategy. Makes strategic IS policy decisions for the enterprise, including sourcing strategies.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Not applicable

Level 4. Provides leadership for the construction and implementation of long term innovative IS solutions.

Level 5. Provides IS strategic leadership to reach consensus and commitment from the management team of the enterprise.

A.3. Business Plan Development

Addresses the design and structure of a business or product plan including the identification of alternative approaches as well as return on investment propositions. Considers the possible and applicable sourcing models. Presents cost benefit analysis and reasoned arguments in support of the selected strategy. Ensures compliance with business risk and technology strategies. Communicates and sells business plan to relevant stakeholders and addresses political, financial, and organisational interests.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Exploits specialist knowledge to provide analysis of market environment etc.

Level 4. Provides leadership for the creation of an information system strategy that meets the requirements of the business (e.g. distributed, mobility-based) and includes risks and opportunities.

Level 5. Applies strategic thinking and organisational leadership to exploit the capability of Information Technology to improve or transform the business.

D.10. Information and Knowledge Management

Identifies information and knowledge relevant to the organisation and develops processes and structures to manage it. Creates information structure to enable the exploitation, optimisation and sharing of information. Understands appropriate tools to be deployed to create, extract, maintain, renew and propagate business knowledge in order to capitalise from the information asset.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Analyses business processes and associated information requirements and provides the most appropriate information structure

Level 4. Integrates the appropriate information structure into the corporate environment.

Level 5. Correlates information and knowledge to create value for the business. Applies innovative solutions based on information retrieved

D.11. Needs Identification

Actively listens to internal/ external customers, articulates and clarifies their needs. Manages the relationship with all stakeholders to ensure that solutions and services are in line with business requirements. Proposes different solutions (e.g. make-or-buy), by performing contextual analysis in support of user centred system design. Advises the customer on appropriate solution choices. Acts as an advocate engaging in the implementation or configuration process of the chosen solution.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Establishes reliable relationships with customers and helps them clarify their needs.

Level 4. Exploits wide ranging specialist knowledge of the customers business to offer possible solutions to business needs. Provides expert guidance to the customer by proposing solutions and supplier.

		Level 5. Provides leadership in support of the customers' strategic decisions. Helps customer to envisage new ICT solutions, fosters partnerships and creates value propositions. E.5. Process Improvement Measures effectiveness of existing or new ICT process approaches (Waterfall, Agile, DevOps etc.). Designs and implements process or technology changes supporting the organization through a continuous learning process. Assesses and addresses risks involved in process change. Level 1. Not applicable Level 2. Not applicable Level 3. Exploits specialist knowledge to research existing ICT processes and solutions in order to define possible innovations. Makes recommendations based on reasoned arguments. Level 4. Provides leadership and authorises implementation of innovations and improvements that will enhance competitiveness or efficiency. Demonstrates to senior management the business advantage of potential changes. Level 5. Not applicable
Data Specialist	Mission: Ensures asset protection through the provision of clean, consistent, quality assured data. Maintains the integrity of data, stores and searches data and supports presentation of data analysis. Summary: Ensures the implementation of the organisations data management policy. Main tasks: Define, build and optimise data models Proactively protect confidentiality and security of data Ensure data lifecycle support Curate and archive data	A.6. Application Design Analyses, specifies, updates and makes available a model to implement applications in accordance with IS policy and user/customer needs. Selects appropriate technical options for application design, optimising the balance between cost and quality. Designs data structures and builds system structure models according to analysis results through modelling languages. Ensures that all aspects take account of interoperability, usability, accessibility and security. Identifies a common reference framework to validate the models with representative users, based upon development models (e.g. iterative approach). Level 1. Contributes to the design and general functional specification and interfaces.

Advise on appropriate data analytic methodology
Ensure data quality and integrity
Maintain data quality and compliance to legal standards

Level 2. Organises the overall planning of the design of the application.

Level 3. Accounts for own and others actions in ensuring that the application is correctly integrated within a complex environment and complies with user / customer needs.

Level 4. Not applicable

Level 5. Not applicable

D.10. Information and Knowledge Management

Identifies information and knowledge relevant to the organisation and develops processes and structures to manage it. Creates information structure to enable the exploitation, optimisation and sharing of information. Understands appropriate tools to be deployed to create, extract, maintain, renew and propagate business knowledge in order to capitalise from the information asset.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Analyses business processes and associated information requirements and provides the most appropriate information structure

Level 4. Integrates the appropriate information structure into the corporate environment.

Level 5. Correlates information and knowledge to create value for the business. Applies innovative solutions based on information retrieved

E.6. ICT Quality Management

Implements ICT quality policy to maintain and enhance service and product provision. Plans and defines indicators to manage quality with respect to ICT strategy. Reviews quality measures and recommends enhancements to influence continuous quality improvement.

Level 1. Not applicable

		Level 2. Communicates and monitors application of the organisation's quality policy. Level 3. Evaluates quality management indicators and processes based on ICT quality policy and proposes remedial action. Level 4. Assesses and estimates the degree to which quality requirements have been met and provides leadership for quality policy implementation. Provides cross functional leadership for setting and exceeding quality standards. Level 5. Not applicable E.8. Information Security Management Manages information and systems security policy accounting for technical, human, organisational and other relevant threats, in line with the ICT and business strategy and reflecting the risk culture of the organisation. Deploys and manages the operational and specialist (for e.g. forensics, threat intelligence and intrusion detection) resources needed to ensure the capacity to manage security incidents, and makes recommendations for the continuous improvement of security policy and strategy. Level 1. Not applicable Level 2. Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non- compliance. Level 3. Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches Level 4. Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements. Level 5. Not applicable
Digital Transformation Leader/e-Government specialist	Mission: Drives cultural change and builds digital capability to deliver innovative business models and processes.	A.3. Business Plan Development Addresses the design and structure of a business or product plan including the identification of alternative approaches as well as return on investment propositions.

Summary: Provides leadership for the implementation of the digital transformation strategy of the organisation.

Main tasks:

Shape and deliver a digital strategy

Develop awareness and education to improve digital capability

Demonstrate the benefits of digital transformation implementation

Advise and support on a 'digital by design' approach

Lead cultural change required to facilitate digital strategy

Lead and mobilise key organisation influencers to implement digital transformation

Considers the possible and applicable sourcing models. Presents cost benefit analysis and reasoned arguments in support of the selected strategy. Ensures compliance with business risk and technology strategies. Communicates and sells business plan to relevant stakeholders and addresses political, financial, and organisational interests.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Exploits specialist knowledge to provide analysis of market environment etc.

Level 4. Provides leadership for the creation of an information system strategy that meets the requirements of the business (e.g. distributed, mobility-based) and includes risks and opportunities.

Level 5. Applies strategic thinking and organisational leadership to exploit the capability of Information Technology to improve or transform the business.

A.5. Architecture Design

Specifies, refines, updates and makes available a formal approach to implement solutions and services, necessary to develop and operate the IS architecture, taking into account the requirements from business, management and data and information infrastructure. Identifies change requirements and the components involved: hardware, software, applications, processes, services, information and technology platform. Takes into account interoperability, reversibility, scalability, usability, accessibility and security, including the need to account for the development and management of vulnerability within existing and emerging technologies. Maintains alignment between business evolution and technology developments and services to ensure capacity of ICT solutions according to SLA.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Exploits specialist knowledge to define relevant ICT technology and specifications to be deployed in the construction of multiple ICT projects, applications or infrastructure improvements.

Level 4. Acts with wide ranging accountability to define the strategy to implement ICT technology compliant with business need. Takes account of the current technology platform, obsolescent equipment and latest technological innovations.

Level 5. Provides strategic leadership for implementing the digital enterprise strategy. Applies strategic thinking to discover and recognize new patterns in data sets and new ICT systems, to achieve business benefits.

A.9. Innovating

Devises creative solutions for the provision of new concepts, ideas, products or services. Deploys novel and open thinking to envision exploitation of technological advances to address business / society needs or research direction.

Level 1. Not applicable

Level 2. Not applicable

Level 3. Not applicable

Level 4. Applies independent thinking and technology awareness to lead the integration of disparate concepts for the provision of unique solutions.

Level 5. Provides strategic leadership for the introduction of new concepts. Guides innovation approaches and leads the cultural change to innovation.

E.7. Business Change Management

Assesses the implications of digital transformation, potential digital disruption and change. Defines the requirements and quantifies the business benefits.

Manages change taking into account structural and cultural issues. Maintains business and process continuity throughout change, monitoring the impact, taking any required remedial action and refining approach.

		Ensures compliance of the digital solution with the administrative regulatory framework and interoperability rules. Analysis of the impact of digitalization on legal and organizational decision-making processes. Level 1. Not applicable Level 2. Not applicable Level 3. Evaluates change requirements and exploits specialist skills to identify possible methods and standards that can be deployed Level 4. Provides leadership to plan, manage and implement significant ICT led business change Level 5. Applies pervasive influence to embed organisational change. E.9. Information Systems Governance Defines, deploys and controls the management of information systems and services and data in line with the business imperatives. Takes into account all internal and external parameters such as legislation and industry standard compliance to influence risk management and resource deployment to achieve balanced business benefit. Level 1. Not applicable Level 2. Not applicable Level 3. Not applicable Level 4. Provides leadership for IS governance strategy by communicating, propagating and controlling relevant processes across the entire ICT infrastructure. Level 5. Defines and aligns the IS governance strategy incorporating it into the organisation's corporate governance strategy. Adapts the IS governance strategy to take into account new significant events arising from legal, economic, political, business, technological or environmental issues.
Product Manager	Mission:	A.4 Product / Service Planning

	Leads cross-functional teams to design, deliver and continuously improve digital public services in a user-centred, iterative and value-driven manner. Summary: Owns the vision, roadmap and lifecycle of digital public services, aligning organisational objectives, public value and user needs. Main tasks: - Lead cross-functional teams in developing digital public services - Ensure iterative, agile and user-centred delivery - Align organisational objectives with service design and delivery - Prioritise requirements and resources to maximise public impact - Define and monitor success indicators and service outcomes	Level 3-4: Defines and manages the vision, scope, and roadmap of digital public services. At higher maturity, leads the full service lifecycle and optimises value delivery across multiple services. <u>E.2 Project & Portfolio Management</u> Level 3-4: Manages delivery of digital services within constraints of scope, time, cost, and quality; at higher levels, coordinates multiple initiatives and balances priorities across a portfolio. <u>E.7 Business Change Management</u> Level 3-4: Drives and supports organizational change resulting from digital service delivery; at higher levels, leads adoption, stakeholder alignment, and benefits realization. <u>E.4 Relationship Management</u> Level 3: Manages relationships with stakeholders across policy, legal, ICT, and operational units to ensure shared understanding and commitment to product goals. <u>A.3 Business Plan Development</u> Level 3: Translates strategic and policy objectives into actionable service plans, value propositions, and success indicators.
User Researcher	Mission: Ensures digital public services are grounded in real user needs, behaviours, and experiences through systematic research. Summary: Plans and conducts qualitative and quantitative research to inform evidence-	B.1 Requirements Analysis Level 3-4: Analyzes, validates, and refines service requirements using both qualitative and quantitative user research. As it matures, it offers expert guidance on defining and validating user-centered requirements. E.4 Relationship Management Level 3: Establishing and sustaining trusted relationships with users, stakeholders, and multidisciplinary teams to

	based service and product design decisions. Main tasks: Plan and conduct qualitative and quantitative user research Build user profiles and user journeys Test prototypes and live services with real users Translate research insights into actionable recommendations Ensure services reflect real end-user experience	collect insights and effectively communicate research findings. D.10 Information and Knowledge Management Level 3: Structuring, documenting, and sharing research data, insights, personas, and user journeys to facilitate evidence-based decision-making and enable reuse across services. E.6 Quality Management Level 3: Contributes to service quality by validating usability, accessibility, and user satisfaction through testing and evaluation activities.
Service Designer	Mission Ensures the design and continuous improvement of end-to-end public services by applying user-centred and evidence-based design methods. Integrates user needs, organisational objectives, and operational constraints to deliver accessible, usable, and coherent digital and hybrid public services that create measurable public value. Summary Designs public services from a holistic perspective, covering user journeys, service touchpoints, processes, and supporting digital solutions. Works closely with policy, legal, business, and ICT stakeholders to translate user research and service insights into service blueprints, process models, and functional requirements. Ensures that public services are understandable, inclusive, accessible, and aligned with institutional goals, while supporting service consistency across channels. Main responsibilities	A.4 Product / Service Planning Level 3: Contributes to the planning and structuring of public services, defining service scope and delivery channels from a user-centered perspective. B.1 Requirements Analysis Level 3: Analyses and refines service requirements based on user research, service design, and stakeholder input. D.10 Information and Knowledge Management Level 3: Structures and documents service knowledge, design artefacts, and insights to support reuse and consistency. E.5 Process Improvement Level 3: Identifies opportunities to simplify and optimize administrative processes through service design methods. E.4 Relationship Management Level 3: Collaborates with stakeholders (policy, legal, ICT, users) to align service design outcomes with organizational needs.

- Plan and conduct service design activities for digital and hybrid public services, using user-centered and participatory design methods.
- Analyze user needs, behaviors, and pain points based on qualitative and quantitative evidence (e.g., user research, service analytics).
- Design end-to-end service journeys, service blueprints, and interaction flows covering front-office and back-office processes.
- Collaborate with User Researchers, Product Managers, and ICT teams to translate service concepts into functional and non-functional requirements.
- Ensure public services are accessible, usable, and inclusive, in line with applicable accessibility standards and good practices.
- Support process optimization by identifying redundancies, bottlenecks, and opportunities for simplification from a service perspective.
- Validate service concepts and prototypes with users and stakeholders, incorporating

E.6 Quality Management

Level 3: Ensures service quality by validating usability, accessibility, and consistency across service channels.

	feedback into iterative improvements. Contribute to service quality monitoring and continuous improvement based on user feedback and performance indicators.	
e-Gouvernement Specialist	Mission: Ensures that the design, implementation, and operation of digital public services align with national and European e-government frameworks, legal and regulatory standards, and interoperability principles. Converts public policies and administrative rules into clear, compliant, and user-focused digital services, supporting institutional consistency and service integration. Summary: Designs, coordinates, and supports the delivery of digital public services by aligning administrative processes, legal requirements, and ICT solutions. Ensures that digital services comply with e-government principles, including <i>digital-by-default</i>, <i>once-only</i>, interoperability, accessibility, and data protection. Acts as a key interface between policy, legal, business, and ICT stakeholders to ensure coherence, sustainability, and reuse across the public administration.	A.4 Product / Service Planning Level 1. Not applicable Level 2. Not applicable Level 3: Contributes to the planning and structuring of digital public services in line with institutional objectives and public value. Supports the definition of service scope, delivery models and success indicators. Level 4. Not applicable Level 5. Not applicable B.1 Requirements Analysis Level 1. Not applicable Level 2. Not applicable Level 3: Translates legal, policy and administrative requirements into functional and non-functional requirements for digital public services. Ensures requirements are complete, consistent and aligned with e-government principles. Level 4. Not applicable Level 5. Not applicable B.4 Solution Deployment Level 1. Not applicable Level 2. Not applicable Level 3: Supports the deployment of digital public services, ensuring alignment with approved

Main tasks:

Contributes to planning and organizing digital public services in accordance with institutional goals and public value.

Assists in defining service scope, delivery methods, and success criteria.

Converts legal, policy, and administrative needs into functional and non-functional requirements for digital services, ensuring completeness, consistency, and alignment with e-government principles.

Supports the deployment of digital services, verifying compliance with specifications, interoperability standards, and operational constraints within public administration.

Analyzes current administrative processes (AS-IS) and designs optimized digital workflows (TO-BE), reducing complexity and administrative burden for users.

Aids organizational change driven by digitalization efforts, and at advanced levels, manages institutional impact and adoption of new digital practices.

Ensures digital services adhere to national e-government frameworks, interoperability standards, data protection regulations, and ICT governance principles in the public sector.

specifications, interoperability requirements and operational constraints within public administration.

Level 4. Not applicable

Level 5. Not applicable

E.5 Process Improvement

Level 1. Not applicable

Level 2. Not applicable

Level 3: Analyses administrative processes (AS-IS) and contributes to the design of optimised digital processes (TO-BE), reducing complexity and administrative burden for users.

Level 4. Not applicable

Level 5. Not applicable

E.7 Business Change Management

Level 1. Not applicable

Level 2. Not applicable

Level 3-4: Supports organizational change resulting from digitalization initiatives. At higher maturity, contributes to managing institutional impact and adoption of new digital working practices.

Level 5. Not applicable

E.4 Relationship Management

Level 1. Not applicable

Level 2. Not applicable

Level 3: Coordinates and maintains effective working relationships with internal stakeholders (policy, legal, IT) and external institutions to ensure coherent service delivery across government.

Level 4. Not applicable

Level 5. Not applicable

	Coordinates and maintains productive relationships with internal stakeholders (policy, legal, IT) and external institutions to deliver coherent services across government. Organizes, documents, and preserves knowledge related to digital public services, administrative workflows, and information models, supporting reuse and consistency across institutions.	
ICT Specialist	Mission: Supports the delivery, operation, and continuous improvement of digital solutions across their lifecycle, ensuring quality, compliance, and interoperability. Summary: A transversal ICT role combining technical execution, service support, quality assurance, and governance support. Main responsibilities: Support delivery of digital projects (requirements, documentation, testing, deployment) Assist DevOps and operations teams (configuration, monitoring, troubleshooting) Define, build and optimize data models Apply standards for measuring and reporting performance indicators Support service management (incident, problem, change)	A.1 IS & Business Strategy Alignment - Level 2–3 A.3 Business Plan Development – Level 2–3 A.6 Application Design – Level 2–3 B.1 Application Development – Level 2–3 B.2 Component Integration – Level 2–3 B.3 Testing – Level 2–3 B.4 Solution Deployment – Level 2–3 C.1 User Support – Level 2–3 C.2 Change Support – Level 2–3 C.4 Problem Management – Level 3 D.2 ICT Quality Strategy Development – Level 2–3 D.10 Information & Knowledge Management – Level 3 E.2 Project & Portfolio Management – Level 2–3 E.4 Relationship Management – Level 3 E.6 ICT Quality Management – Level 3

	Facilitate collaboration with subordinate agencies' IT teams Support ICT governance, cybersecurity compliance and interoperability Provide user support and improve digital services Ensure compliance with ethical and legal requirements	
Network Specialist	<u>Summary:</u> Ensures the alignment of the network, including telecommunication and/or computer infrastructure to meet the organisation's communication needs. <u>Mission:</u> Manages and operates a networked information system, solving problems and faults to ensure defined service levels. Monitors and improves network performances and security. <u>Main tasks:</u> Ensure communication performance, recovery, and security needs meet agreed service agreement standards Contribute to define network design policies, philosophies and criteria Investigate, diagnose and solve network problems Use network management system tools to determine network load and model performance statistics Maintain awareness of relevant legislation affecting network security Configure network to protect against security threats Monitor network to identify and address traffic bottle necks	<u>Application Design</u> Analyses, specifies, updates and makes available a model to implement applications in accordance with IS policy and user/customer needs. Selects appropriate technical options for application design, optimising the balance between cost and quality. Designs data structures and builds system structure models according to analysis results through modelling languages. Ensures that all aspects take account of interoperability, usability, accessibility and security. Identifies a common reference framework to validate the models with representative users, based upon development models (e.g. iterative approach) Level 1: Contributes to the design and general functional specification and interfaces. Level 2: Organises the overall planning of the design of the application. Level 3: Accounts for own and others actions in ensuring that the application is correctly integrated within a complex environment and complies with user / customer needs. <i>Level 4: Not applicable</i> <i>Level 5: Not applicable</i> <u>Component Integration</u> Integrates hardware, software or sub system components into an existing or a new system. Complies with established processes and procedures such as, configuration management and package maintenance. Takes into account the compatibility of existing and new

modules to ensure system integrity, system interoperability and information security. Verifies and tests system capacity and performance and documentation of successful integration.

Level 1: Not applicable

Level 2: Acts systematically to identify compatibility of software and hardware specifications. Documents all activities during installation and records deviations and remedial activities

Level 3: Accounts for own and others actions in the integration process. Complies with appropriate standards and change control procedures to maintain integrity of the overall system functionality and reliability.

Level 4: Exploits wide ranging specialist knowledge to create a process for the entire integration cycle, including the establishment of internal standards of practice. Provides leadership to marshal and assign resources for programs of integration.

Level 5: Not applicable

Solution Deployment

Following predefined general standards of practice carries out planned necessary interventions to implement solutions and services, including installing, securing, upgrading or decommissioning. Configures hardware, software or network to ensure interoperability of system components and debugs any resultant faults, incompatibilities or losses (damage). Engages additional specialist resources if required, such as third-party network providers. Formally hands over fully operational solution to user ICT management, and completes documentation recording all relevant information, including equipment addressees, configuration and performance data.

Level 1: Removes or installs components under guidance and in accordance with detailed instructions.

Level 2: Acts systematically to build or deconstruct system elements. Identifies failing components and establishes root cause failures. Provides support to less experienced colleagues.

Level 3:Accounts for own and others actions for solution provision and initiates comprehensive communication with stakeholders. Exploits specialist knowledge to influence solution construction providing advice and guidance.

Level 4: *Not applicable*

Level 5: *Not applicable*

Problem Management

Manages the life cycle of incidents and problems. Identifies and resolves the root cause of incidents. Takes a proactive approach to avoidance or identification of root cause of ICT problems. Deploys a knowledge system based on recurrence of common errors. Resolves or escalates incidents. Optimises system or component performance.

Level 1: *Not applicable*

Level 2: Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution.

Level 3: Exploits specialist knowledge and in-depth understanding of the ICT infrastructure and problem management process to identify failures and resolve with minimum outage. Makes sound decisions in emotionally charged environments on appropriate action required to minimise business impact. Rapidly identifies failing component, selects alternatives such as repair, replace or reconfigure.

Level 4: Provides leadership and is accountable for the entire problem management process. Schedules and ensures well trained human resources, tools, and diagnostic equipment are available to meet emergency incidents. Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. Constructs escalation processes to ensure that appropriate resources can be applied to each incident.

Level 5: *Not applicable-*

Information Security Management

		Manages information and systems security policy accounting for technical, human, organisational and other relevant threats, in line with the ICT and business strategy and reflecting the risk culture of the organisation. Deploys and manages the operational and specialist (for e.g. forensics, threat intelligence and intrusion detection) resources needed to ensure the capacity to manage security incidents, and makes recommendations for the continuous improvement of security policy and strategy. Level 1: <i>Not applicable</i> Level 2-Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non- compliance. Level 3-Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches Level 4-Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements. Level 5: <i>Not applicable</i>
Systems Administrator	<u>Summary:</u> Administers ICT System components to meet service requirements. <u>Mission:</u> Installs software, configures and upgrades ICT systems. Administers day-to-day operations to satisfy continuity of service, recovery, security and performance needs. <u>Main tasks:</u> Investigate, diagnose and solve system related problems Install and upgrades software Test upgrades Schedule installation work, to minimize disruption	<u>Component Integration</u> Integrates hardware, software or sub system components into an existing or a new system. Complies with established processes and procedures such as, configuration management and package maintenance. Takes into account the compatibility of existing and new modules to ensure system integrity, system interoperability and information security. Verifies and tests system capacity and performance and documentation of successful integration. Level 1: <i>Not applicable</i> Level 2: Acts systematically to identify compatibility of software and hardware specifications. Documents all activities during installation and records deviations and remedial activities. Level 3: Accounts for own and others actions in the integration process. Complies with appropriate standards

Diagnose and solve hardware or software problems
Comply with organization procedures to ensure integrity and security of the system

and change control procedures to maintain integrity of the overall system functionality and reliability.
Level 4: Exploits wide ranging specialist knowledge to create a process for the entire integration cycle, including the establishment of internal standards of practice. Provides leadership to marshal and assign resources for programs of integration.
Level 5: *Not applicable*

Testing

Constructs and executes systematic test procedures for ICT systems or customer usability requirements to establish compliance with design specifications. Ensures that new or revised components or systems perform to expectation. Ensures meeting of internal, external, national and international standards; including health and safety, usability, performance, reliability or compatibility. Produces documents and reports to evidence certification requirements.

Level 1: Performs simple tests in strict compliance with detailed instructions.

Level 2: Organises test programs and builds scripts to stress test potential vulnerabilities. Records and reports outcomes providing analysis of results.

Level 3: Exploits specialist knowledge to supervise complex testing programmes. Ensures tests and results are documented to provide input to subsequent process owners such as designers, users or maintainers.

Accountable for compliance with testing procedures including a documented audit trail.

Level 4: Exploits wide ranging specialist knowledge to create a process for the entire testing activity, including the establishment of internal standard of practices.

Provides expert guidance and advice to the testing team.

Level 5: *Not applicable* -

Change Support

Evaluates, implements and guides the evolution of an ICT solution evaluating changes and their impact. Ensures efficient control and scheduling of software or hardware

modifications to prevent multiple upgrades creating unpredictable outcomes. Minimises service disruption as a consequence of changes and adheres to defined service level agreement (SLA). Ensures consideration and compliance with information security procedures.

Level 1: *Not applicable* -

Level 2: During change, acts systematically to respond to day by day operational needs and react to them, avoiding service disruptions and maintaining coherence to (SLA) and information security requirements.

Level 3: Ensures the integrity of the system by controlling the application of functional updates, software or hardware additions and maintenance activities. Complies with budget requirements.

Level 4: *Not applicable*-

Level 5: *Not applicable*

Problem Management

Manages the life cycle of incidents and problems. Identifies and resolves the root cause of incidents. Takes a proactive approach to avoidance or identification of root cause of ICT problems. Deploys a knowledge system based on recurrence of common errors. Resolves or escalates incidents. Optimises system or component performance.

Level 1: *Not applicable* -

Level 2: Identifies and classifies incident types and service interruptions. Records incidents cataloguing them by symptom and resolution.

Level 3: Exploits specialist knowledge and in-depth understanding of the ICT infrastructure and problem management process to identify failures and resolve with minimum outage. Makes sound decisions in emotionally charged environments on appropriate action required to minimise business impact. Rapidly identifies failing component, selects alternatives such as repair, replace or reconfigure.

Level 4: Provides leadership and is accountable for the entire problem management process. Schedules and ensures well trained human resources, tools, and

		diagnostic equipment are available to meet emergency incidents. Has depth of expertise to anticipate critical component failure and make provision for recovery with minimum downtime. Constructs escalation processes to ensure that appropriate resources can be applied to each incident. Level 5: <i>Not applicable</i> - Information Security Management Manages information and systems security policy accounting for technical, human, organisational and other relevant threats, in line with the ICT and business strategy and reflecting the risk culture of the organisation. Deploys and manages the operational and specialist (for e.g. forensics, threat intelligence and intrusion detection) resources needed to ensure the capacity to manage security incidents, and makes recommendations for the continuous improvement of security policy and strategy. Level 1: <i>Not applicable</i> - Level 2: Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non- compliance. Level 3: Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches Level 4: Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements. Level 5: <i>Not applicable</i>
Database Administrator	<u>Summary:</u> Designs, implements or monitors and maintains data sets, structured (databases) and unstructured (big data). <u>Mission:</u> Administer and monitor data management systems and ensures design, consistency, quality and security.	Application Development Interprets the application design to develop a suitable application in accordance with customer needs. Adapts existing solutions by e.g. porting an application to another operating system. Codes, debugs, tests and documents and communicates product development stages. Selects appropriate technical options for development such as reusing, improving or reconfiguration of existing

Main tasks:

Apply standards methods and tools for measuring and reporting on wide set of relevant performance indicators (response time, availability, safety, integrity)
Produce data set procedures and instructions for other analysts or administrators
Monitor and maintain data management systems
Ensure the integrity and security of existing data management systems
Identify, investigate and correct problems or incidents related to data management systems
Provide training, support, advice and guidance on data set issues to other information system practitioners

components. Optimises efficiency, cost and quality. Validates results with user representatives, integrates and commissions the overall solution.

Level 1: Acts under guidance to develop, test and document applications.

Level 2: Systematically develops and validates applications.

Level 3: Acts creatively to develop applications and to select appropriate technical options. Accounts for others development activities. Optimizes application development, maintenance and performance by employing design patterns and by reusing proved solutions.

Level 4: *Not applicable*

Level 5: *Not applicable*

Component Integration

Integrates hardware, software or sub system components into an existing or a new system. Complies with established processes and procedures such as, configuration management and package maintenance. Takes into account the compatibility of existing and new modules to ensure system integrity, system interoperability and information security. Verifies and tests system capacity and performance and documentation of successful integration.

Level 1: *Not applicable* -

Level 2: Acts systematically to identify compatibility of software and hardware specifications. Documents all activities during installation and records deviations and remedial activities.

Level 3: Accounts for own and others actions in the integration process. Complies with appropriate standards and change control procedures to maintain integrity of the overall system functionality and reliability.

Level 4: Exploits wide ranging specialist knowledge to create a process for the entire integration cycle, including the establishment of internal standards of practice.

Provides leadership to marshal and assign resources for programs of integration.

Level 5: *Not applicable* -

Change Support

Evaluates, implements and guides the evolution of an ICT solution evaluating changes and their impact. Ensures efficient control and scheduling of software or hardware modifications to prevent multiple upgrades creating unpredictable outcomes. Minimises service disruption as a consequence of changes and adheres to defined service level agreement (SLA). Ensures consideration and compliance with information security procedures.

Level 1: *Not applicable* -

Level 2: During change, acts systematically to respond to day by day operational needs and react to them, avoiding service disruptions and maintaining coherence to (SLA) and information security requirements.

Level 3: Ensures the integrity of the system by controlling the application of functional updates, software or hardware additions and maintenance activities. Complies with budget requirements.

Level 4: *Not applicable*-

Level 5: *Not applicable*-

Information and Knowledge Management

Identifies information and knowledge relevant to the organisation and develops processes and structures to manage it. Creates information structure to enable the exploitation, optimisation and sharing of information. Understands appropriate tools to be deployed to create, extract, maintain, renew and propagate business knowledge in order to capitalise from the information asset.

Level 1: *Not applicable*

Level 2: *Not applicable*-

Level 3: Analyses business processes and associated information requirements and provides the most appropriate information structure

Level 4: Integrates the appropriate information structure into the corporate environment.

Level 5: Correlates information and knowledge to create value for the business. Applies innovative solutions based on information retrieved

Information Security Management

Manages information and systems security policy accounting for technical, human, organisational and other relevant threats, in line with the ICT and business strategy and reflecting the risk culture of the organisation. Deploys and manages the operational and specialist (for e.g. forensics, threat intelligence and intrusion detection) resources needed to ensure the capacity to manage security incidents, and makes recommendations for the continuous improvement of security policy and strategy.

Level 1: *Not applicable* -

Level 2: Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non-compliance.

Level 3: Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches

Level 4: Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements.

Level 5: *Not applicable* -

Annex 4 List of ICT system categories

Category	Description
SO. Critical ICT systems	Very large and critical national ICT systems (such as critical cloud infrastructure (data centers, VPN, cybersecurity, servers, storages, virtualization, etc.), critical national registers - basic registers, critical ICT business applications/systems) whose non-functioning (malfunctioning) can cause very large damages (financial, reputation, confidence and/or other collateral damages). The maximum interruption time is 1-2 hours only during very critical events (such as earthquakes, fires, very critical and important upgrades). In normal period there should be no interruption time, that means redundant architecture and maintenance (updates and not critical upgrades) without interruption of production systems. The national PA institutions managing these ICT systems must have comprehensive Business Continuity Plans and BCPs are annually independently audited and quarterly/semiannually tested (or sooner for very critical components). <i>Examples:</i> <i>Infrastructure for National Data Network and Governmental Cloud and Sectorial Clouds (MoF, MoI, MoJ for justice sector, etc.);</i> <i>Critical national registers: Civil Register;</i> <i>Critical applications/systems: Border Control (MoI); Trezor (MoF); SIUI (National Health Insurance House), Meteorological Warning System (Sistem Avertizări Meteorologice - SAM) etc.</i> <i>Portal for Reporting Cybersecurity events www.dnsc.ro</i>
S1. Very large ICT systems	Complex very large national ICT systems (such as data centers, servers and other infrastructure, national register, ICT applications, etc.) that are used by a very large number of internal users, and/or manage G2C applications for a very large number of citizens, and/or manage G2B/G2C applications for a very large number of legal entities. The maximum interruption time can be few (1-2) calendar days. The national PA institutions managing these ICT systems must have detailed Business Continuity Plans and BCPs are annually independently audited and annually tested. Minimum number of internal users: 10,000 Minimum number of citizens for G2C: 1,000,000 Minimum number of legal entities for G2B and/or G2G: 100,000 <i>Examples:</i> <i>Dedicated and specialized data centers and Infrastructure for Public Ministry (prosecutors)</i> <i>National registers: Registry of commercial organizations (Trade Register) and Registry of fiscal code for legal entities (MoF); Street Register and Cadaster (ANCP), etc.</i> <i>IT very large applications: ECRIS (MoJ); Forexebug and others (MoF), SEAP (ADR), etc.</i>
S2. Large ICT systems	National and local ICT systems (such as infrastructure (usually data rooms), servers and other infrastructure, ICT applications, etc.) that are used by many internal users, and/or manage G2C applications for a large number of citizens, and/or manage G2B/G2C applications for many citizens/legal entities. The maximum interruption time can be few (1-2) working days.

	The national and local PA institutions managing these ICT systems must have Business Continuity Plans (including comprehensive ICT Backup and Recovery measures) and BCPs (BRs) are independently audited (preferable annually, but no later than 2 years) and regularly tested (preferable annually, but no later than 2 years). Minimum number of internal users: 500 Minimum number of citizens for G2C: 250,000 Minimum number of legal entities for G2B and/or G2G: 10,000 <i>Examples:</i> <i>Most of these large ICT systems are managed by central administration (usually large ministries/agencies) such as Pension, Social Assistance and others in Social Protection; ICT systems in Education; etc.</i> <i>Bucharest and maybe a couple of other large municipalities (local administration “municipii”) that large ICT systems.</i>
S3. Middle ICT systems	National and local ICT systems (servers and other infrastructure, ICT applications, etc.) that are used by a medium number of internal users, and/or manage G2B/G2C applications for a medium number of citizens/legal entities. The maximum interruption time can be maximum 5 working days. The national and local PA institutions managing these ICT systems must have detailed ICT Backup and Recovery policies and BRs are independently audited (no later than 2 years) and regularly tested (preferable annually, but no later than 2 years). Minimum number of internal users: 100 Minimum number of citizens for G2C: 50,000 Minimum number of legal entities for G2B and/or G2G: 1,000
S4. Small ICT systems	National and local ICT systems that are mainly used by internal users for back office function. The maximum interruption time can be maximum 10 working days. The national and local PA institutions managing these ICT systems must have primitive ICT Backup and Recovery policies and BRs are regularly tested (no later than 2/3 years). Number of internal users: 1-100 Number of citizens for G2C and number of legal entities for G2B and/or G2G are usually small.

Annex 5 Summary table of ICT systems types

ICT system category	Level (national or national and local)	Maximum interruption time	Business Continuity Plan (BCP) / Backup and Recovery policies and measures(BR) <i>Note: BCP includes BR</i>	Minimum number of internal users	Minimum number of citizens for G2C		Minimum number of legal entities for G2B and/or G2G
S0	Critical ICT systems	National	1-2 hours only during very critical periods	Comprehensive BCP and BCP is annually independently audited and quarterly/semi-annually tested (or sooner for very critical components).	These are not relevant for critical ICT systems		
S1	Very large ICT systems	National	1-2 calendar days	Detailed BCP and BCP is annually independently audited and annually tested	10,000	1,000,000	100,000
S2	Large ICT systems	National and local	1-2 working days	BCP (including comprehensive ICT BR measures) and BCP (BR) is independently audited (preferable annually, but no later than 2 years) and regularly tested (preferable annually, but no later than 2 years).	500	250,000	10,000
S3	Middle ICT systems	National and local	maximum 5 working days	Detailed ICT BR policy and BR measures are independently audited (no later than 2 years) and regularly tested (preferable annually, but no later than 2 years).	100	50,000	1,000

S4	Small ICT systems	National and local	maximum 10 working days	Primitive BR and BR is regularly tested (no later than 2/3 years).	1-100	Usual very small figures
-----------	-------------------	--------------------	-------------------------	--	-------	--------------------------

Annex 6 Proposed methodology for determining the ranking of IT jobs and salary levels

Step 1. Establishing the maximum level of responsibility for each ICT job/ function and seniority level: Beginning with mapping the key roles that define specialized ICT functions using SFIA skills^[1], the highest level of responsibility can be attained for each ICT job. The following matrix can be obtained, which sets the maximum SFIA responsibility level for each function and each seniority level:

Table 17 Correspondence between proposed ICT job classification, professional grades and SFIA levels of responsibility

Function / Level of expertise	Junior	Regular	Senior	Expert
ICT Manager			7	8
ICT Architect		4	5	7
Cybersecurity specialist	2	4	6	7
ICT Service Delivery & Support specialist	2	4	5	6
ICT Service Management and E-Government specialist	2	4	5	7
ICT Development & Data Management Specialist	2	4	5	7

^[1] <https://sfia-online.org/en/sfia-9/documentation/access-sfia-9-excel>

Step 2: Based on Table 12 - Matrix of the ICT unit/department and the proposed categories of ICT systems, a coefficient of complexity could be attached for each type of ICT system considered. The coefficient 1 will be maintained for very large ICT systems and critical systems, calculating for other types of ICT systems a coefficient based on the ratio of the maximum level of responsibility allowed (according to the referenced table) and level 7 (the maximum for very large systems). The complexity coefficients in the table below are illustrative.

Table 18 ICT system type, SFIA levels and coefficient of ICT system complexity

ICT system type	Maximum level of responsibility allowed	Coefficient
Small	3	0,4
Medium	4	0,6
Large	5	0,7
Very Large	7	1,0
Critical	7	1,0

Step 3: The coefficient from the previous step could be used to weight it with the maximum level of responsibility, obtaining a matrix for each type of institution considered. The coefficients in the table below are illustrative and should not be considered proposed pay coefficients. They are meant to illustrate difference in responsibility and therefore in job ranking across various ICT jobs based on their allocation to professional grade and type of institution/ICT system.

Official Use Only

Table 19 Job ranking coefficients linked to ICT jobs, professional grades, depending on types of institutions and ICT systems

Responsibility level weighted by function importance	Seniority level			
	Junior	Regular	Senior	Expert
S4: Small ICT systems				
ICT Manager	0,0	0,0	3,0	3,4
ICT Architect	0,0	1,7	2,1	3,0
Cybersecurity specialist	0,9	1,7	2,6	3,0
ICT Service Delivery & Support specialist	0,9	1,7	2,1	2,6
ICT Service Management and E-Government specialist	0,9	1,7	2,1	3,0
ICT Development & Data Management Specialist	0,9	1,7	2,1	3,0
S3: Medium ICT systems				
ICT Manager	0,0	0,0	4,0	4,6
ICT Architect	0,0	2,3	2,9	4,0
Cybersecurity specialist	1,1	2,3	3,4	4,0
ICT Service Delivery & Support specialist	1,1	2,3	2,9	3,4
ICT Service Management and E-Government specialist	1,1	2,3	2,9	4,0
ICT Development & Data Management Specialist	1,1	2,3	2,9	4,0
S2: Large ICT systems				
ICT Manager	0,0	0,0	5,0	5,7
ICT Architect	0,0	2,9	3,6	5,0
Cybersecurity specialist	1,4	2,9	4,3	5,0
ICT Service Delivery & Support specialist	1,4	2,9	3,6	4,3
ICT Service Management and E-Government specialist	1,4	2,9	3,6	5,0
ICT Development & Data Management Specialist	1,4	2,9	3,6	5,0
S1 (S0): Very Large or Critical ICT systems				
ICT Manager	0,0	0,0	7,0	8,0
ICT Architect	0,0	4,0	5,0	7,0
Cybersecurity specialist	2,0	4,0	6,0	7,0
ICT Service Delivery & Support specialist	2,0	4,0	5,0	6,0
ICT Service Management and E-Government specialist	2,0	4,0	5,0	7,0
ICT Development & Data Management Specialist	2,0	4,0	5,0	7,0

Step 4: Weighting the maximum level of responsibility defined on each type of system considered with a coefficient for ICT function importance. This new dimension added to the model will allow differentiation for those specialized ICT public functions that hold the same maximum level of responsibility for the same type of system considered.

In the table above, it can be observed that the level of responsibility for small ICT systems is the same for the roles of ICT architect, Cybersecurity specialist, ICT Service Management and E-Government specialist, and ICT Development & Data Management Specialist. A coefficient that allows for the ranking of the ICT function can make this differentiation, which should be reflected in the salary grid.

Official Use Only

IT job importance coefficients were proposed considering the ranking reflected by other methodological frameworks: in UK, in DDaT Capability Framework – Product Manager, Technical Architect, and Head of ICT are in higher job grades compared to Service Desk roles (<https://ddat-capability-framework.service.gov.uk/>), in France Référentiel des métiers SIC – the roles of 'Information Systems Architect' and 'Information Security Manager' are classified in higher salary brackets compared to 'Support Technician' (<https://www.data.gouv.fr/datasets/referentiel-de-remuneration-des-56-metiers-de-la-filiere-numerique-et-des-systemes-dinformation-et-communication>).

- ICT Manager - position 1 (strategic impact, SFIA level 6–7).
- ICT Architect - second position (defines national ICT infrastructure and interoperability).
- ICT Development and Data Management Specialist - third in the hierarchy (innovation, data, support for data-driven public policies).
- Cybersecurity Specialist - third, possibly fourth (protection, compliance, management of critical risks).
- ICT Service Management and E-Government Specialist - position 5 (management of ICT services, mid-level coordination).
- ICT Service Delivery & Support Specialist – position 6 in the hierarchy (operational, daily support).

Table 20 Proposed ICT job importance coefficients

ICT function	Coefficient
ICT Manager	1,5
ICT Architect	1,4
Cybersecurity specialist	1,3
ICT Service Delivery & Support specialist	1
ICT Service Management and E-Government specialist	1,2
ICT Development & Data Management Specialist	1,3

By applying the importance coefficient from the table to the responsibility levels defined by the size and complexity of ICT systems managed by a public institution, it is possible to construct a matrix that generates a ranking coefficient for each ICT job. This coefficient combines seniority level with the specialized ICT function. For example, an expert-level employee in a public institution managing a medium-sized ICT system, assigned to the ICT function of cybersecurity specialist, would have a responsibility level of 4 (the maximum level for that system). When weighted by the coefficient of 1.3 for the cybersecurity specialist function, the resulting ranking coefficient is 5.2.

Table 21 Determining job ranking coefficients for ICT jobs

Professional grading by the ICT function and seniority level	Seniority level			
	Junior	Regular	Senior	Expert
S4: Small ICT systems				
ICT Manager	0,0	0,0	4,5	5,1
ICT Architect	0,0	2,4	3,0	4,2

Official Use Only

Professional grading by the ICT function and seniority level	Seniority level			
	Junior	Regular	Senior	Expert
Cybersecurity specialist	1,1	2,2	3,3	3,9
ICT Service Delivery & Support specialist	0,9	1,7	2,1	2,6
ICT Service Management specialist and E-Government	1,0	2,1	2,6	3,6
ICT Development & Data Management Specialist	1,1	2,2	2,8	3,9
S3: Medium ICT systems				
ICT Manager	0,0	0,0	6,0	6,9
ICT Architect	0,0	3,2	4,0	5,6
Cybersecurity specialist	1,5	3,0	4,5	5,2
ICT Service Delivery & Support specialist	1,1	2,3	2,9	3,4
ICT Service Management and E-Government specialist	1,4	2,7	3,4	4,8
ICT Development & Data Management Specialist	1,5	3,0	3,7	5,2
S2: Large ICT systems				
ICT Manager	0,0	0,0	7,5	8,6
ICT Architect	0,0	4,0	5,0	7,0
Cybersecurity specialist	1,9	3,7	5,6	6,5
ICT Service Delivery & Support specialist	1,4	2,9	3,6	4,3
ICT Service Management and E-Government specialist	1,7	3,4	4,3	6,0
ICT Development & Data Management Specialist	1,9	3,7	4,6	6,5
S1 (S0): Very Large or Critical ICT systems				
ICT Manager	0,00	0,00	10,50	12,00
ICT Architect	0,00	5,60	7,00	9,80
Cybersecurity specialist	2,60	5,20	7,80	9,10
ICT Service Delivery & Support specialist	2,00	4,00	5,00	6,00
ICT Service Management and E-Government specialist	2,40	4,80	6,00	8,40
ICT Development & Data Management Specialist	2,60	5,20	6,50	9,10

Step 5: Establishing the salary level (in lei) by groups of coefficients and salary steps. Based on the job ranking coefficients, pay intervals can be determined. The ones proposed below are illustrative. They would need to be determined by mapping the proposed ICT jobs and their professional grades onto the single pay grade structure that is developed by the Ministry of Labor as part of the wage system reform process, as envisaged under NRRP milestone 420³³.

³³ The updated deadline for adopting the public sector wage system reform is June 2026.

Table 22 Proposed matrix for determining ICT job salary matrix

Job ranking coefficient interval	Step 1	Step 2	Step 3
0-3	x	X+5%	X+10%
3-6	X+15%	X+25%	X+35%
6-10	X+45%	...	...
10-12	...	...	...