EN

THIS ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX III

to the Commission Implementing Decision on the financing of the multiannual action plan part I in favour of the Regional South Neighbourhood for 2024-2026

Action Document for Support to Digital Transition in the Southern Neighbourhood

MULTIANNUAL ACTION PLAN
This document constitutes the multiannual work programme in the sense of Article 110(2) of the Financial Regulation, and action plan/measure in the sense of Article 23(2) of NDICI-Global Europe Regulation.

1. SYNOPSIS

1.1. Action Summary Table

1. Title **OPSYS** **Basic Act**	Support to Digital Transition in the Southern Neighbourhood Multiannual action plan part I in favour of the Regional South Neighbourhood for 2024-2026 OPSYS business reference: ACT-62466 ABAC Commitment level 1 number: JAD.1398832 Financed under the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe)
2. Economic and Investment Plan (EIP)	Yes Contribution to thematic priority IV Digital
EIP Flagship	Yes (Flagship 7 – Digital transformation, research and innovation)
3. Team Europe Initiative	Yes The digital skills component will contribute to the Regional Team Europe Initiative on Jobs through Trade and Investment in the Southern Neighbourhood
4. Beneficiar(y)/(ies) of the action	The action shall be carried out in the Southern Neighbourhood countries: Algeria, Egypt, Israel ([1]), Jordan, Lebanon, Libya, Morocco, Palestine*, Syria ([2]) and Tunisia.

[1] See Guidelines on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards on https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013XC0719(03)&from=en.

* This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue. Implementation of the present action will integrate the recommendations of

5. Programming document	Multi-annual indicative programme for the Southern Neighbourhood (2021-2027)[3]
6. Link with relevant MIP(s) objectives/expected results	MIP Priority Area 2 "Strengthen resilience, build prosperity and seize the digital transition" SO1: Strengthen economic governance and enhance entrepreneurship through research, innovation, and digitalisation.
PRIORITY AREAS AND SECTOR INFORMATION	
7. Priority Area(s), sectors	151 Government and civil society – general 160 Other social Infrastructure & services 220 – Communications 250 – Business and Other Services 430 – Other multisector
8. Sustainable Development Goals (SDGs)	Main SDG: SDG 9: "Industry, Innovation and Infrastructure" Other significant SDGs: SDG 5: Gender Equality SDG 8: Decent Work and Economic Growth SDG 10: Reduced inequality SDG 16: Peace Justice and Strong Institutions SDG 17: Partnerships for the Goals
9. DAC code(s)	22040 - Information and communication technology (ICT): 16020 – Employment creation: 25010 - Business Policy and Administration: 25030 – Business development services: 32130 – Small and medium-sized enterprises (SME) development:
10. Main Delivery Channel	11000 Other public entities in donor country 40000 Multilateral organisations

the Communication to the Commission on the review of ongoing financial assistance for Palestine C (2023) 8300, 21.11.2023.

[2] Co-operation with the Government of Syria suspended since 2011.

[3] Commission Implementing Decision C(2021)9399 of 16.12.2021 on a Multi-Annual Indicative Programme for the Southern Neighbourhood.

11. Targets	☐ Migration ☐ Climate ☒ Social inclusion and Human Development ☒ Gender ☐ Biodiversity ☒ Human Rights, Democracy and Governance			
12. Markers (from DAC form)	**General policy objective**	**Not targeted**	**Significant objective**	**Principal objective**
	Participation development/good governance	☐	☐	☒
	Aid to environment	☒	☐	☐
	Gender equality and women's and girl's empowerment	☐	☒	☐
	Reproductive, maternal, new-born and child health	☒	☐	☐
	Disaster Risk Reduction	☒	☐	☐
	Inclusion of persons with Disabilities	☒	☐	☐
	Nutrition	☒	☐	☐
	RIO Convention markers	**Not targeted**	**Significant objective**	**Principal objective**
	Biological diversity	☒	☐	☐
	Combat desertification	☒	☐	☐
	Climate change mitigation	☒	☐	☐
	Climate change adaptation	☒	☐	☐
13. Internal markers and Tags	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	EIP	☐	☒	☐
	EIP Flagship	YES ☒		NO ☐
	Tags	YES		NO
	transport	☐		☒
	energy	☐		☒
	environment, climate resilience	☐		☒
	digital	☒		☐
	economic development (incl.	☒		☐

	private sector, trade and macroeconomic support)		
	human development (incl. human capital and youth)	☒	☐
	health resilience	☐	☒
	migration and mobility	☐	☒
	agriculture, food security and rural development	☐	☒
	rule of law, governance and public administration reform	☒	☐
	other	☐	☐
	Digitalisation	☐ ☐	☒
	Tags	YES	NO
	digital connectivity	☒	☐
	digital governance	☒	☐
	digital entrepreneurship	☒	☐
	digital skills/literacy	☒	☐
	digital services	☒	☐
	Connectivity	☐ ☐	☒
	Tags	YES	NO
	digital connectivity	☒	☐
	energy	☐	☒
	transport	☐	☒
	health	☐	☒
	education and research	☐	☒
	Migration	☒ ☐	☐
	Reduction of Inequalities	☐ ☒	☐
	COVID-19	☒ ☐	☐

BUDGET INFORMATION	
14. Amounts concerned	Budget line(s) (article, item): 14.020110 Southern Neighbourhood Total estimated cost: EUR 14 000 000 Total amount of EU budget contribution: EUR 14 000 000
MANAGEMENT AND IMPLEMENTATION	
15. Implementation modalities (management mode	**Indirect management** with the entities to be selected in accordance with the criteria set out in section 4.3.1**.**

and delivery methods)	

1.2. Summary of the Action

The action contributes to eliminating existing obstacles and barriers for online services for citizens, both women and men and people with disabilities, public administrations and businesses, through the harmonisation of the digital regulatory environments including strengthened cybersecurity as well as through improved level of digital skills, literacy and digital competencies.

The action englobes three complementary components;

Component 1 aims to extend the benefits of the European Union's Digital Single Market to the Southern Mediterranean countries, channelling EU support to **digital transformation via regulatory reforms**. Future EU support to harmonizing the digital environments between EU and Southern Mediterranean partners is expected to bring benefits in the form of stronger regulation conducive to more competition and investments, as well as consumer rights protection, and the prospect of new wireless broadband opportunities and 5G.

Component 2 aims to improve **cybersecurity** prevention, preparedness and response of relevant public stakeholders by providing capacity building support in compliance with human rights and the rule of law, in line with the aims of the 2020 EU Cybersecurity Strategy and the Cyber Solidarity Act.

Component 3 on **digital skills** aims to standardise and improve the level of digital skills, literacy and competencies for the private sector in the Southern Neighbourhood, creating an ecosystem to boost equal business opportunities for all people and foster decent job creation.

The present action reflects the EU priorities under the **Joint Communication on a Renewed Partnership with the Southern Neighbourhood**4 and its **Economic and Investment Plan (EIP)**5. This action implements the **Multi-Annual Indicative Programme for the Southern Neighbourhood (2021-2027)** 6 under its **Priority Area** 2 "Strengthen resilience, build prosperity and seize the digital transition". The action contributes to the implementation of the **Economic and Investment Plan (EIP)** and in particular the regional activities linked to Flagships #1 (Support to social sectors, education, skills and health), #3 (Resilient economies), #4 (Sustainable economies), #5 (Connected economies), #7 (Digital transformation, research and innovation). The objectives of the action are also aligned with the Union for the Mediterranean (UfM) policy priorities.

The action is in line with the **EU Digital Decade Agenda** which was launched in March 2021 with concrete targets and vision for 2030 setting ambitious goals across four pillars: skills, government, infrastructure and business. Moreover, the action refers to the **EU Digital Competence Framework** (ECF, DigComp), the **EU Digital Education Action Plan (2021-2027)**[7] and the **EU Digital Economy and Society Index** (DESI).

[4] JOIN (2021) 2 final of 09.02.2021
[5] SWD(2021) 23 final
[6] C(2021) 9399 final
[7] European Commission: Directorate-General for Education, Youth, Sport and Culture, Digital education action plan 2021-2027 – Improving the provision of digital skills in education and training, Publications Office of the European Union, 2023

The action also promotes the **June 2023 Communication on the implementation of the EU Toolbox on 5G cybersecurity**[8] which is an essential component of the Security Union Strategy underpinning the broader European policy framework of strategic autonomy and enhanced resilience, and the specific framework for the protection of electronic communications networks and other critical infrastructures, in particular the implementation of Article 40 of the European Electronic Communications Code.

This action also contributes to the **regional Team Europe Initiative (TEI): "Jobs through Trade and Investment in the Southern Neighbourhood",** which involves France, Germany, Italy, Spain, Sweden, the European Training Foundation (ETF), the European Investment Bank (EIB) and the European Bank for Reconstruction and Development (EBRD).
The action also reflects the policy priorities in the region through **the Union for the Mediterranean (UfM)** where digital development represents shared interests by the 43 UfM Member countries. Component 3 takes into consideration the recommendations of the **UfM Progress Report on Regional Integration** (launched in 2021)[9] and of the **UfM Conference on Digital Transformation and Digital Skills for the Future**[10]. Moreover, it is in line with the **UfM Ministerial Declaration on Labour and Employment**, approved on 18 May 2022, which focuses on the need to tackle the digital skills gap, the digital gender divide, the digital accessibility gap for persons with disabilities and the digital infrastructure within and between the two shores of the Mediterranean, as well as the need to explore pathways for accelerating digital transformation as a vehicle for the creation of more decent jobs, inclusive economic growth, and an important vector of innovation and creativity.

The value added of the present regional action consists in promoting a harmonised approach in the Southern Mediterranean region towards digital policy reforms in line with EU best practice, as well as promoting a common digital skills' competency framework complementary to initiatives at national level.

The above components will be designed and implemented in full complementarity with bilateral and regional programmes in the digital sector (in particular in Annual Action Programmes 2023 and 2024), including Twinning and TAIEX actions and initiatives from other donors in the Southern Mediterranean region.

1.3 Beneficiar(y)/(ies) of the action

The action shall be carried out in Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria and Tunisia, out of which only Israel is not included in the list of ODA (Official Development Assistance) recipients.

[8] C(2023) 4049 final
[9] Regional-Integration-in-the-UfM_EN.pdf (ufmsecretariat.org)
[10] UfM Conference on Digital Transformation and Digital Skills for the Future - Union for the Mediterranean - UfM (ufmsecretariat.org)

2. RATIONALE

2.1. Context

Digital technologies are transforming almost every sector of the economy including products and services, as well societies and cultures. The technology creates new opportunities, demands, skills and improves transparency and accountability. Improper use of the technology can create new threats, risks, cybercrimes, community division and manipulation. Regulations are needed to be put in place to foster the safe use and development of digital technologies.

The E-government development index (EGDI), a composite index based on the weighted average of three normalized indices; Online Service Index, Telecommunications Infrastructure Index, and Human Capital Index, shows that except for Lebanon and Libya, Southern Neighbourhood (SN) countries are in the upper middle EGDI category ranked around position 100 out of 193. This is significantly lower than the EU average EGDI level[11].

As revealed by the EuroMeSCo Euromed Survey[12], enhancing digitalisation in the public sector and promoting regulatory framework, e-governance including cybersecurity (23%) and adapting education and vocational training to the requirements of digitalisation (46%), are seen as the most effective ways to support a digitalisation agenda in the SN countries.

The NRI ranking[13] confirms that the ICT regulatory environment in SN is still underdeveloped and governments in the region are not fast enough in adapting legislation for emerging technologies. Jordan, which scored highest on this measure among all the countries in the region, ranked 46th (out of 127 countries ranked), while the worst performer was Morocco – 90th.[14]

The considerable digital regulatory disparities and the lack of a framework for digital skills have a detrimental impact on socio-economic development of the Southern Neighbourhood.

2.2 Problem Analysis

In 2022, the Commission has ordered a study to identify partner countries' needs and interests and provide a gap analysis in the area of digital transformation in line with the countries' national strategies/priorities. The findings of the study have outlined that support should be programmed in priority areas to enhance regulatory approximation, harmonisation of digital skills and enhance cyber resilience.

Digital regulations

According to the Euro-Mediterranean Regulators' Group (EMERG) Benchmark Report 2021, the Southern Neighbourhood National Regulatory Authorities (NRAs) have developed expertise in the Telecom Regulations sector but there are other digital areas such as eTrust, emerging technologies, 5G security, network neutrality, and consumer protection for which further support is necessary.

[11] UN E-government Knowledgebase, https://publicadministration.un.org/egovkb/en-us/Data-Center2

[12] Launched in 12.2020, the survey was organised into five thematic blocks including 23 questions with a sample size of 800 respondents comprised of experts, civil society representatives and policy-makers in the SN and the EU

[13] Network Readiness Index (Benchmarking the Future of the Network Economy) https://networkreadinessindex.org/

[14] Digital Transformation in the Southern Neighbourhood, EuroMeSCo Euromed Survey

According to the International Telecommunication Union (ITU), the digital regulatory framework can be mainly categorized into the following main areas: Telecommunication and Connectivity, Digital Trust (eTrust), Data protection and Privacy, Cybersecurity & Cybercrime, ePayments, Consumer Protection and Emerging Technologies.

There is an increasing demand for professionals with a range of skills required by the digitalization of the public sector. To keep pace with fast evolving technologies, policy makers are compelled to design and implement appropriate strategies and policies for their countries' digital transformation on specialised topics. For this purpose, policy makers require a necessary set of skills and knowledge.
Some countries are already progressing in developing a digital regulatory framework, others are still in nascent stages (e.g. Libya and Lebanon). The main development in the regulatory framework of the region is focusing on the connectivity part while the rest of the areas are still in the early stage of development, with some differences between the countries.

Southern Neighbourhood countries have huge variances in terms of eTrust and eIDs regulations and implementation, with Morocco, Jordan, Tunisia, Egypt having laws and regulations related to Digital Transactions and Cybercrimes while Libya, Algeria, Lebanon and Palestine are still in the early stage. SN countries are still lacking the applications implementation of eTrust and eIDs and the regulations enforcement. Some countries have progressed in this regard like Egypt, Jordan and Morocco but with limited progress towards harmonisation with the EU counterparts and cross-border recognition.

Some countries have already made some steps in digital payments regulations. Jordan through the central bank has developed mobile payment switch and regulations for eWallets15. Also Palestine Monetary Authority licensed five ePayment companies[16]. Similarly, Egypt[17], Morocco and Tunisia have regulations enabling ePayments. These eWallets are mainly regulated for local payments/transfers, yet cross-border payments need to be further developed.

In this context, digital strategies need to be developed in the region for some countries as a start while others need support in developing and updating the set of specific strategies. As a second step, strengthening the implementation of digital regulations will improve the mainstreaming of digital in public services and adoption among citizens.

Most countries in the region have both, ministries focusing on digital transformation and independent telecom regulators (with the exception of Palestine). Some countries have specific entities that regulate and manage eTrust applications and eIDs such as ITIDA in Egypt and Tuntrus in Tunisia. Detailed assessment of stakeholders of eTrust and eIDs are needed specially that this kind of regulations are not centralized in the countries (nor follow one single framework).

Cybersecurity

While digitalisation has been increasing, many of the risks and threats associated with it have however been overlooked and inadequately addressed. Cyber threats can harm critical infrastructures (e.g. power grids, hospitals); but even at a lower scale, insecure systems can lead to data breaches that could significantly harm individuals, businesses or state authorities. Addressing the threats posed by malicious cyber activities and promoting secure digital services and infrastructure should therefore be a clear priority, especially in a context characterised with an increasingly volatile geopolitical landscape and continued instability at regional level.

[15] https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/24ab593c-e6da-4247-9a6c-7644b996d2f2.pdf
[16] According to the PMA annual report 2020 Page ix. List of companies' page 56
[17] https://www.tra.gov.eg/en/regulations/regulatory-framework/mobile-wallets-regulatory-rules/

While most South Partner Countries have contemplated the necessity to develop national cybersecurity strategies[18] and establish computer emergency response teams (CERTs), maturity, political engagement and awareness about cybersecurity remain relatively uneven in the region[19] and among various groups of the population. Considering such challenges, the EU could very much position itself as a strategic partner. On an issue more related to connectivity, for instance, Tunisia recently expressed interest in the EU's methodology, and notably the EU's toolbox on 5G Cybersecurity.[20]

The Commission already presented to Tunisian counterparts a three-step methodology based on the EU's trajectory comprising a threat landscape/assessment, the development of strategic and technical measures and an assessment of the advance of measures put in place. This entry point creates a momentum to take action at regional level on issues related to digital connectivity and its related cyber topics. In addition, the European Union Agency for Cybersecurity (ENISA) is also an important actor in the European cyber landscape, which could be associated in certain parts of a regional action and with which the collaboration could increase.

As cyber threats have a stronger societal impact, the understanding of resilience has to shift from a purely technical account (i.e. the capacity of networks to recover) to one that concerns also strategic and operational dimensions across the whole range of policy areas, including home affairs, security and defence, foreign policy, industrial and economic policy, research and technology development, and education. The multi-dimensional nature of threats in the cyberspace requires also flexible and adaptable governance models that engage the many levels and different actors (multi-stakeholder approach). In this perspective, a core issue to be tackled in the Southern Neighbourhood region is that of training and capacity building targeting individuals working in public agencies and institutions dealing with information & communication technology (ICT), to ensure an optimal level or preparedness and the sustainability of the action beyond EU funding in the years to come.

Finally, given the sensitivity of the issue, while implementing the action, attention should be paid in relation to human rights, data protection and good governance, in line with the 2020 EU Cybersecurity Strategy, the EU Strategic Framework and Action Plan on Human Rights and Democracy, and the EU Human Rights Guidelines on Freedom of Expression Online and Offline. Monitoring and controlling of social media content has become a key aspect of MENA cybersecurity policy, sometimes to the detriment of freedom of expression online.[21]

Digital skills

The Southern Neighbourhood region is constrained by poor regional economic integration, low level of digital transformation, high unemployment and volatile economic growth, which has been insufficient to deal with the rapidly expanding work force in the past decades.

Non-homogenous digital ecosystems and limited digital skills across the region result in a deep digital divide. In 2019 the share of population using internet across the region ranged from 57% in Egypt and 60% in Algeria, through 67% in Jordan and Tunisia, up to 71% in West Bank and Gaza, 74% in Morocco, and 78% in Lebanon – compared to 82% in the EU (2018) and 47% in middle income

[18] Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia No existing cybersecurity strategies in Libya nor Palestine.
[19] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
[20] Secure 5G deployment in the EU: Implementing the EU toolbox - Communication from the Commission | Shaping Europe's digital future (europa.eu)
[21] Euromesco Policy Study, Great Expectations: defining a trans-Mediterranean cybersecurity agenda: https://www.euromesco.net/wp-content/uploads/2021/08/GYI35BP-1.pdf

countries on average22. At the same time, there are noticeable disparities in usage rates along socioeconomic, demographic and geographical lines.

On an individual level, there are noticeable disparities in usage rates along socioeconomic, demographic and geographical lines. Regarding gender equality, hurdles to access, affordability, (lack of) education and skills and technological literacy, and inherent gender biases and discriminatory socio-cultural norms, are at the root of gender-based digital exclusion. For instance, while on average 58.5% of men in the Arab states use internet (in line with the global average of 58%), the same is true for just 44.2% of women (below the global average of 48%). In a worrying trend, the gender internet penetration gap widened between 2013 and 2019 by 5.2 percentage points (by way of comparison, in Europe it decreased by 4.1 percentage points over the same period). Even more noticeable is the digital divide between youth and older adults. The internet usage gap between those aged 18-29 and 60+ stood at 47% in Lebanon, 62% in Palestine, and a whopping 81% in Egypt. Less severe but nevertheless pronounced divergences also exist along educational and urban/rural lines; for instance, the gap between urban and rural internet usage varies from as little as 3% in Lebanon up to 21% in Morocco[23]. Moreover, as in other regions of the world, people with disabilities face even more challenges related to new skill requirements, technological barriers or challenges associated with working conditions such as low and irregular pay, long working hours or isolation[24].

According to ITU, basic digital skills, such as writing and receiving e-mails, are held by fewer than one in four persons in Algeria and Tunisia, and 50-75% in Morocco, Egypt and Lebanon. Between 15-35% of the population in Algeria, Lebanon and Tunisia, and 35-55% in Morocco and Egypt are in possession of standard digital skills, e.g. using basic formulas in spreadsheet, while just 5-10% of society in Morocco, Algeria, Egypt and Lebanon, and 10-15% in Tunisia, have advanced ICT skills. This lack of competences and skills seriously hampers the competitiveness of the private sector.

There is a need in the region to focus on the harmonisation, benchmarking, standardisation, and quality measurement of digital skills by introducing and adapting the EU's valuable tools and frameworks to the region. This will improve the understanding of digital skills' development ecosystem, analyse digital inclusion and equity, and offer equal opportunities in terms of jobs and lifelong learning.

One of the main challenges is skills measurement. Most of the indicators are based on self-reporting of individuals' digital skills that may be subjective. Most of the measures in the region are based on the number of trainings delivered to individuals, certifications or at the best case the number of individuals placed in jobs as a result of the programmes. The European Training Foundation (ETF) also identified that a main gap is the lack of a common way to measure (basic and advanced) digital skills in the region.

Moreover, the education system does not always equip young job seekers with the skills and knowledge needed by the private sector, which transcripts into a lack of working experiences and opportunities among youth. Besides that, there is no concrete adopted mechanism allowing the evaluation of individual digital skills showing their employability readiness. This creates challenges for the development of skills and competencies suitable to the job market on the local level, and also hampers ways of collaboration among companies on both sides of the Mediterranean.

[22] Individuals using the Internet (% of population) | Data (worldbank.org)
[23] https://www.euromesco.net/wp-content/uploads/2021/06/ES11_Qualitative-3-Sidlo-102-110.pdf
[24] https://www.ilo.org/wcmsp5/groups/public/---dgreports/---gender/documents/publication/wcms_769852.pdf

The adoption of digital solutions is still lagging behind due to an overall lack of professional service providers, along with a proper standardized assessment and benchmarking of the impact on SMEs. Service providers should be equipped with the right tools and competencies to in turn provide inclusive digital services to SMEs. Against this background, the action supports the development of a regional framework of assessment and professional training curricula to be adopted by the service providers.

Finally, it is also relevant to underline for all three components of the present Action that the digital transition must be done in line with the respect of specific environmental and climate change issues such as GHG emissions, air pollution, high energy and electricity usage as well as waste production (e.g. packaging). Therefore, the relevant environmental and climate change issues will be addressed and awareness raised when supporting the beneficiary countries.

Identification of main stakeholders and corresponding institutional and/or organisational issues (mandates, potential roles, and capacities) to be covered by the action.

Digital regulations

The Euro-Mediterranean Regulators Group (EMERG) and its constituting National Regulatory Authorities from 20 countries[25] will feature among the main stakeholders for this action, besides representatives from the relevant Ministries (i.e. Ministries of Telecommunication, Communication and Information Technologies, Economy and Sustainable Development etc.), government agencies in charge of the digital economy and society (especially those related to e-trust and privacy, as well as national standardization bodies). Other key government stakeholders may include representatives from line Ministries (e.g. Health, Transport, Justice, Education and Research, Employment, Infrastructures etc.). They will contribute to the policy making processes and participate in activities carried out under this project in their area of expertise.

Cybersecurity

Key stakeholders will be South Partner Countries' governments, including cybersecurity public agencies and competent ministries (ICT, Security, Justice, etc), the private sector, civil society, and end-users. Capacity building shall be approached at three levels, namely individual, organisational and that of the enabling environment, in a whole-of-government and whole-of-society participatory approach. In each South Partner Countries, key duty bearers, policy makers and implementers will be identified and engaged. Given the dynamism and complexity of the cybersecurity/critical information infrastructure field, a thorough stakeholder analysis shall be undertaken during the inception phase.

Digital skills

The main stakeholders will be institutional authorities and administrations in charge of digitalisation; policy makers from the ministries responsible for digital transformation, education and skills, industry and other line ministries involved in digital reform; as well as relevant national agencies for digital promotion, skills promotion agencies, national and regional chambers of commerce. Moreover, the private sector, digital service providers and business associations are important stakeholders, as their participation increases the programme's legitimacy and ensures that promoted frameworks and reforms are well-targeted on the private sector's needs and demands.

[25] Bosnia and Herzegovina, Croatia, Cyprus, Egypt, France, Germany, Greece, Israel, Italy, Jordan, Lebanon, Malta, Morocco, Palestine, Portugal, Spain, Switzerland, Tunisia, Turkey, Montenegro

Furthermore, civil society organisations, including women's rights organisations as well as those representing youth, people with disabilities and other people in vulnerable situations will be duly consulted and engaged to ensure that the programme contributes to an inclusive and gender-responsive digital environment.

2.3. Lessons Learned

Digital regulations

The level of maturity of the digital environments and ecosystems vary greatly across the Southern Neighbourhood. This area requires further harmonisation at regional level while maintaining a flexible approach in the design and implementation of the action. There is an increasing need for policy makers to possess the appropriate level of skills and knowledge accompanying the digital transformation.

The EU has supported the set up and functioning of EMERG through a successive round of technical assistance projects. Cooperation between the National Regulatory Authorities part of EMERG remains politically important (as confirmed by the Commission in 2023). Future EU support to EMERG is expected to bring further benefits to citizens and businesses in the Southern Neighbourhood region, in the form of stronger regulation that should in principle lead to competition and investments, as well as consumer rights protection, and the prospect of new wireless broadband opportunities and 5G. EMERG will have to develop a financial and technical sustainability model based on the agreement of the members on: Membership fees, Members budget contribution, Service fees. This action will build on the experience and lessons learned acquired during the EU support provided previously. It will also draw on the experience of supporting its peer organisation, EaPeReG, in the Eastern Partnership. A proper assessment of the sustainability requirements for EMERG will have to be carried out during the inception phase of the action.

Cybersecurity

Component 2 is the first attempt to tackle cybersecurity at regional level in the Southern Neighbourhood. It will build on the best practices from cybersecurity cooperation experience from other regions, such as "CybersecurityEast", the IPA-funded comprehensive regional programme EU Support to Cybersecurity Capacity Building in the Western Balkans or the action "Capacity Building and Cooperation to enhance Cyber Resilience" (CB4CyberResilience) under the former Instrument contributing to Stability and Peace (IcSP). It will also rely on the know-how developed through the EU's previous action at country level, whereby the Commission (DG CNECT) assisted the EU delegation in Nigeria in organising a training module and supported a session of information for Tunisian counterparts on the EU's 5G toolbox. Although cooperation on cybersecurity has a dominant bilateral logic in this region, a regional approach to the matter is a necessary complementary step to take to ensure a level-playing field across the region.

Cybersecurity and the protection of critical information infrastructure involve a wide range of stakeholders. Capabilities should be built collectively to better address the challenges in cyber space. Lessons from other projects show that it is important to establish a multi-stakeholder approach to ensure greater security of networks and critical infrastructure. The private sector needs to be involved in the implementation of a national cybersecurity strategy to ensure its sustainability. Different communities, officials/diplomats, security experts and development agencies need also to be closely associated.

A whole-of-society approach to cybersecurity should be promoted. Particular focus should be placed in the incorporation of safeguards in this action in relation to human rights, gender equality and cyber

violence against women and girls, accessibility and protection of people with disabilities, data protection and good governance, in line with the EU Cybersecurity Strategy and the EU Strategic Framework and Action Plan on Human Rights and Democracy, the EU Gender Action Plan III[26] and the 2021-2030 EU Disability Strategy. This is mainly important given that monitoring and controlling of social media content has become a key aspect of MENA cybersecurity policy, sometimes to the detriment of freedom of expression online.[27]

Digital skills

While there are important bilateral projects to support the digital transition (as indicated below), there is currently no digital skills' programme aiming at a harmonised digital competence and skills framework covering the whole region. In contrast, in the Eastern Neighbourhood there has been a positive impact with the EU4Digital Facility and its different pilot programmes, including one on digital skills. The facility started a second phase incorporating lessons which are also relevant for this action. Particularly, 1) for implementing pilots in the region, it has proven successful to start small, and scale up later to first prove the concept and then to adopt the piloted solution gradually (also through bilateral envelopes); 2) Plan enough time for activities implementation as they are complex due to the need to mobilise multiple stakeholders, decision making on the regional level, consultations, and dependencies with ongoing activities; 3) Government and local stakeholders' involvement and commitment are key as coordination and ownership will need to continue at national level; 4) Expert Networks should be established as part of an established governance structure.

The three components of the present action build on bilateral programmes and their independent evaluations, including: "EU support to Digital Transformation in Egypt (El Rakamia)" worth EUR 10 million (EU funded); "e-Tamkeen" programme enhances digital skills of civil servants for improved public services and it is implemented by Enabel in Morocco; "Green Innov'i" and its complementary "Innov'i project" which connects SMEs and startups to the EU market and builds digital skills and it is implemented by Expertise France in Tunisia; "Orange Digital Centres, Digital Skills for Employment" funded by Orange and implemented by GIZ" which focus on digital skills implemented in Egypt, Jordan, Morocco and Tunisia, "Industry 4.0, e-commerce and AI", implemented by GIZ in Tunisia; "EU digital action" which focuses on youth development, digital skills, and e-governance with Enabel and Expertise France in Palestine, and "Supporting digital skills for the next generation: GenerationDigital!" implemented in Algeria, Egypt, Morocco, Tunisia among other African countries funded by BMZ and implemented by GIZ. Lastly, this component will find synergies and complementarity with "Digital4people/Programme d'appui à la digitalisation en Tunisie", a large digitalisation programme of up to EUR 40 million (EU funded and foreseen for 2024).

Finally, the action makes reference to national TEIs in the region that include digitalisation as one of their relevant elements. Also, the action builds on the OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem[28] and the findings of the UNCTAD eTrade

[26] JOINT (2020) 17 final of 25.11.2020. The Gender Action Plan III is a Joint communication by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy which was welcomed through EU Presidency Conclusions of 16 December 2020. Drafting was led by European Commission in close consultation with EU Member States, EEAS, civil society organisations, partner governments, and international organisations (UN entities, International Finance Institutions among others). The different parties contributed to the drafting of the document through meetings and through responses to a survey conducted during the process.

[27] Euromesco Policy Study, Great Expectations: defining a trans-Mediterranean cybersecurity agenda: https://www.euromesco.net/wp-content/uploads/2021/08/GYI35BP-1.pdf

[28] OECD Digital Education Outlook 2023 : Towards an Effective Digital Education Ecosystem | OECD Digital Education Outlook | OECD iLibrary (oecd-ilibrary.org)

Readiness Assessments[29] which provide a snapshot of the e-commerce ecosystem in developing countries and regions for each of the seven pillars of the "e-Trade for all" initiative, which are key to embracing their digital transformation (and one of its main pillars being digital skills). The eTrade readiness assessment has been conducted for Jordan Tunisia, Egypt and Algeria in 2023. Moreover, the action builds on a regional mapping on digital trade recently concluded, and it will be built in line with the upcoming Digital Trade and e-Commerce regional programme (part of the Regional Annual Action Plan 2023 on Sustainable Trade) which has a dedicated part devoted to the private sector.

3. DESCRIPTION OF THE ACTION

3.1. Objectives and Expected Outputs

The **Overall objective** (Impact) of this action is to contribute to South Neighbourhood partner countries' inclusive and sustainable socio-economic development by eliminating existing obstacles and barriers to digital services for citizens (both women and men, and people with disabilities), public administrations and businesses through supporting the harmonisation of digital markets' regulatory framework, enhancing cybersecurity and improving the level of digital skills.

This objective will be pursued through 3 different but complementary components.

The **Specific objective** (Outcome) of **component 1 "Harmonising digital markets in the Southern Neighbourhood"** is the following:

1. Support the harmonisation of digital markets by improving telecom and digital regulations and regional convergence for affordable, accessible, secure, reliable and high-speed connectivity infrastructure and digital services.

The **Outputs** to be delivered for component 1 are:

- O1: The development of regulatory approximation of digital environments and electronic communications norms at regional level is supported in line with the EU best practice.

- O2: Improved capacities of national regulatory authorities for developing and implementing conducive regulatory frameworks on telecommunications.

- O3: The institutionalisation of sustainable EMERG network with defined services and consolidated structure is supported

- O4: Enhanced capacities of government officials who are engaged in digital transformation efforts in the Southern Neighbourhood countries.

The **indicative activities** for component 1 are the following:

- Conduct digital regulatory framework analysis and impact assessment, analyse gaps, cost benefit analysis and readiness for harmonisation.
- Conduct targeted studies to evaluate the level of digital market infrastructures, regulation and services development.
- Capacity building and technical support to improve the regulatory framework.

[29] eTrade Readiness Assessments | UNCTAD

- Promote peer to peer learning among the countries through dialogue; Support to networking and knowledge sharing between the telecom regulators and the standardisation organisations in the EU (ETSI - European Telecommunications Standards Institute, CEN – European Committee for Standardisation and CENELEC- The European Committee for Electrotechnical Standards) and Southern Neighbourhood Countries to improve the harmonisation of the regulations.
- Provide needs-based e-learning and training courses for government officials. Content-wise these courses will address the gender/age/digital gaps as well as issues related to accessibility and inclusiveness of digital markets. Furthermore, a gender-balance attendance and participation (i.e panels) and the accessibility criteria (venues, materials, etc…) will be taken into account.

The **Specific objective** (Outcome) of **component 2 "Enhancing cyber resilience and the security of the cyber space in the Southern Neighbourhood"** is the following:

1. Improve the prevention, preparedness and response of relevant stakeholders in the Southern Neighbourhood with regards to cyber threats, in compliance with human rights, gender equality and the rule of law.

The **Outputs** to be delivered for component 2 are:

- O1: The national legal framework and cybersecurity governance are strengthened in line with the framework for responsible state behaviour in cyberspace.

- O2: Increased operational capacities for cyber incidents management and improved inter-agency cooperation at national level.

- O3: A community of stakeholders sharing best practices and incident information is fostered at regional, trans-regional and international level.

The **indicative activities** for component 2 are the following**:**

- Implementation of training and workshops to exchange on/promote EU best practices on cybersecurity and ensure compliance with human rights.
- Provision of advice for the elaboration of draft legislation and policy documents in the field of cybersecurity.
- Cyber hygiene trainings to decision-makers and staff of public institutions (at all levels and working in different sectors) are held across the region[30].
- Provision of technical assistance to support the empowerment of Computer Security Incident Response Teams (CSIRTs) and Computer emergency response teams (CERTs)to handle major cybersecurity incidents affecting Critical Information Infrastructure (CIP).
- Implementation of community building activities around the organisation of joint cyber incident management meetings, table-top exercise(s) and mock operations.

[30] As the cyber space may be used by groups and individuals for malicious disinformation purposes which hamper human rights and stability, such trainings may include components related to the fight against disinformation online in line with UNESCO's 'Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach' (https://unesdoc.unesco.org/ark:/48223/pf0000387339).

- Organisation of a mentorship programme and study visits to EU Member States for exchange of knowledge and best practices among mid-career professionals with demonstrable leadership potential in the field of cybersecurity in the region.
- Assistance to the participation of target groups in multilateral fora, including the UN, international conferences and networks events. A gender-balance attendance and participation (i.e panels) and accessibility criteria (venues, materials, etc…) will be taken into account.

The **Specific Objective** (Outcome) of **component 3 "Enhancing Digital Skills for the private sector in the Southern Mediterranean"** is the following:

1. Support the harmonisation of digital competencies and skills for the private sector in the Southern Neighbourhood Countries and the establishment of a regional digital skills' platform.

The **indicative outputs** to be delivered for component 3 are:

- O1: Digital competencies and skills for the private sector are harmonised and aligned with the European Digital Competence Framework (ECF).

- O2: The quality of digital services is standardised in cooperation with service multipliers for the benefit of private sector support organisations and SMEs.

- O3: A regional digital skills' platform/network/group of practitioners is developed to exchange experiences and develop strategies linked to digital skills gaps, to foster decent job creation, in particular for youth, women and people with disabilities, and reinforces coordination among public and private stakeholders.

- O4: Private sector service providers are trained on digital skills and training networks for SMEs are established.

The **indicative activities** for component 3 are the following:

- Policy dialogue, best practice exchanges and knowledge sharing.
- In-depth assessment and analysis of digital skills, competencies and literacy gaps and development of dedicated action plans.
- Mapping and harmonisation of existing digital skills framework.
- Capacity building and technical assistance on digital skills tools and schemes.
- Regional and national Public-Private Dialogues (PPD) with relevant stakeholders.
- 'Train the trainers' and awareness raising initiatives. Assessments or studies on the impact of digital skills initiatives on environment and job creation.
- Partnership with corporates.

3.2. Mainstreaming

Environmental Protection, Climate Change and Biodiversity

Outcomes of the Environmental Impact Assessment (EIA) screening (relevant for projects and/or specific interventions within a project).

The EIA screening classified the action as Category C (no need for further assessment). However, the specific environmental issues linked to digitalization, such as GHG emissions, air pollution, energy consumption and waste production will be taken into consideration during the implementation of the action.

Technical assistance and peer exchanges foreseen by the action will also aim to strengthen the partner government's capacity on integrating environment and climate change into digital policy making.

Outcome of the Climate Risk Assessment (CRA) screening (relevant for projects and/or specific interventions within a project).

The CRA screening concluded that this action is no or low risk (no need for further assessment). As mentioned here above, any climate-related risk will however be assessed and considered during the implementation of the action.

Gender equality and empowerment of women and girls

As per OECD Gender DAC codes identified in section 1.1, this action is labelled as G1. This implies that equal opportunities and gender mainstreaming are embedded throughout the action. This is in line with the EU Gender Action Plan III, and the thematic area of engagement: "Addressing the challenges and harnessing the opportunities offered by the green transition and the digital Transformation".

The three components will ensure the equal participation of women, integrate a gender perspective into their activities as a cross-cutting priority, and will strive to promote gender equality and equal opportunities. Gender equality incentives will be incorporated particularly in capacity building activities. The three components will work with partners to ensure a balanced representation of women and men among action beneficiaries to the greatest extent possible (e.g. the action will not propose or accept single-gender workshops, panels, etc.). Activities focusing on support to NRAs, EMERG, CSIRTs/CERTs… will also include specific capacity building activities on gender inclusion for telecom and cybersecurity regulations. The digital skills component will pay particular attention to business support organisations representing female entrepreneurs, and will also put emphasis on women entrepreneurship through the use of role models, peer learning and mentoring, fair participation of women to trainings and activities of the programme.

Human Rights

The action will be implemented in respect of a Rights-Based approach, notably a human rights approach, at all levels and stages of its design and implementation, e.g. avoid any unintentional human rights harm, imbalance or negative impact.

Human rights, democracy and the rule of law, and a gender responsive approach will remain at the heart of the EU's response.[31] The action will be taking into account the principles of non-discrimination, meaningful participation, transparency, accountability and respect to all human rights. Human Rights mainstreaming will equate with implementing the programme in accordance with defined EU values that are relevant to protection and promotion of fundamental rights in the digital economy.

[31] EU Action Plan on Human Rights and Democracy 2020-2024

Disability

As per OECD Disability DAC codes identified in section 1.1, this action is labelled as D0. This implies that this action and its component are not considered relevant for the inclusion of persons with disabilities. Whenever possible, in alignment with the 2021-2030 EU Disability Strategy, the Action will contribute to making visible the situation of persons living with disabilities by using indicators disaggregated by disability status, and by promoting the collection and use of disaggregated data for policy making. The Action will ensure that rights of persons with disabilities will be respected, and the planned activities are disability inclusive. The Action will encourage partners and programme participants to take the initiatives to protect and support the empowerment of persons with disabilities, for instance by associating organisations representing people with disabilities.

Democracy

Promotion of democratic values will be integrated in the design of individual actions, whenever relevant, and will be included in the set of indicators accompanying these actions. A particular focus should be placed in the incorporation of safeguards in this action in relation to human rights, data protection and good governance, in line with the EU Strategic Framework and Action Plan on Human Rights and Democracy.

Conflict sensitivity, peace and resilience

Component 2 of this action on Cybersecurity aims to contribute to the achievement of SDG 16 (Peace, Security and Strong Institutions), in particular the following targets: 16.A "Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime".

3.3. Risks and Assumptions

Category	Risks	Likelihood (High/ Medium/ Low)	Impact (High/ Medium/ Low)	Mitigating measures
Category 1 – To the external environment	Political instability within some of the partner countries	**High**	**Low**	Possibility to tailor activities based on situation on the ground. For example, non-inclusion of countries in crisis will not hamper the Action's implementation.
Category 1 – To the external environment	Limited ability to carry out activities on the ground	**Medium**	**Medium**	Possibility to carry out some activities online and ensure virtual follow up with relevant stakeholders.
Category 2 – To planning, processes and systems	Speed of policy implementation	**Medium**	**Medium/ High**	The speed of policy implementation could be maintained ensuring close relationship between implementing partners and relevant political counterparts through the EU

				Delegations.
Category 2 – To planning, processes and systems	Change in priorities	**Low**	**Low**	Any potentially relevant changes in the political environment will be closely monitored and the necessary adjustments taken during the implementation of the actions proposed.
Category 2 – To planning, processes and systems	Overlapping with other on-going initiatives at the national level	**Medium**	**Low**	The projects financed by this Action will be implemented in close contact with EU Delegations in the region and other development partners, in order to avoid any duplication. Should risk however appear, this shall result in adapting the proposed approach.
Category 3 – To people and the organisation	Lack of trust and limited cooperation among countries	**High**	**Medium**	The cooperation between participating countries could be promoted in a gradual manner and around consensual matters through a phased approach with clear deliverables and milestones, to ensure results and sustainability.
Category 3 – Risks related to people and the organisation	High turnover of staff in the partner countries	**High**	**Medium**	The sustainability of projects under this Action will be developed throughout the inception period. When possible, each action should include a "train the trainer" approach at national level in order to ensure this key point.
Category 3 – To people and the organisation	Engagement of stakeholders	**Medium**	**Medium**	The engagement of the different stakeholders can be supported by the organisation of regional and public-private dialogues.

External Assumptions

- No major governance disruption takes place in the target countries.
- Partner countries are willing to reach a higher degree of cooperation within the region and with the EU.
- Partner countries commit to optimize the sustainability of the respective projects by making available the necessary human, financial and material resources.
- Policy makers, local actors and social partners are willing to cooperate and share their experience within the region.

3.4. Intervention Logic

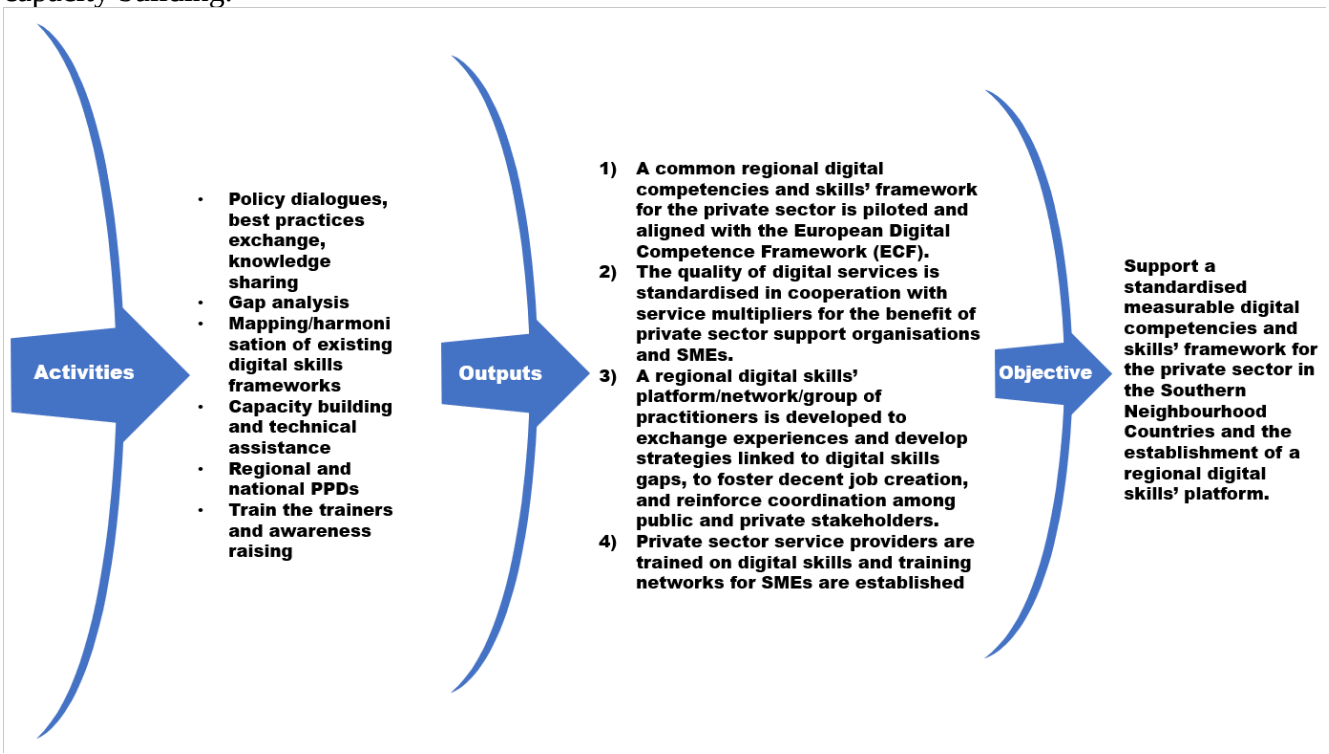
The theory of change behind the proposed intervention takes into account the assessment of the situation and the top priorities of the Southern Neighbourhood partner countries, and it tries to address the need to enhance and support the region's digital transformation.

For **component 1**, solid regulations governing ICT are implemented and enforced by regulatory authorities and other relevant bodies mandated to ensure compliance with governmental policies and regulations, to promote efficient investment, fair competition and protect the interests of end-users.
The complexity and constant evolution of technologies requires policy makers to gain a timely understanding of technical aspects that can affect the deployment of digital infrastructure and the delivery of digital services.
To achieve the above, the following intervention logic applies. If a digital regulatory framework gap analysis is conducted and capacity building/ technical support to improve the regulatory framework is provided, then the digital markets in the region are likely to become more harmonized. The capacities of public officials who are engaged in digital transformation in the Southern Neighbourhood countries may be enhanced if quality needs-based e-learning and training courses are provided to them. Proper regulatory framework, training and infrastructure may constitute an incentive to provide more digital public services. The activities of the Euro-Mediterranean Regulators Group have a sustainable impact on regulatory reforms in the region if the network consolidates its structure, and the members from the National Regulatory Authorities are actively involved in the implementation of policy recommendations. Targeted needs-driven support to NRAs will be given on ICT regulatory issues that are relevant at national and regional level. The Action will make extensive use of the peer-to-peer cooperation modality to enhance partnerships between EU and Southern Neighbourhood regulators.

For **component 2**: if decision-makers in South Partner Countries (SPCs) are sensitised to cyber threats, UN cyber norms and the application of international frameworks and laws on cyber, they will be able to facilitate the implementation of the UN framework for responsible state behaviour into their national policies and strategies. If CSIRTs/CERTs in SPCS are supported through technical, organisational assistance and empowered to cooperate with other relevant agencies to handle major cyber incidents targeting Critical Information Infrastructure, then the capacities of SPCs to adequately prevent, respond to and address cyber incidents and/or accidental failures will be enhanced and the cooperation in the national ecosystem will be improved. If activities are organised around joint cyber incident management meetings, table-top exercise(s) and mock operations, a community of practitioners in the field of cyber could be built in the Southern Neighbourhood. If this community of practitioners is established and if the participation of SPC representatives in international and/or regional cooperation mechanisms is promoted, regional cooperation on cybersecurity issues could be enhanced. Finally, if the three projects' outputs are successfully delivered, the cybersecurity prevention, preparedness and response of relevant public stakeholders in the Southern Neighbourhood will be improved, in compliance with human rights and the rule of law.

For **component 3**, this action aims to develop a standardized digital skills framework focusing on the harmonization, benchmarking and quality measurement of digital skills and competencies by introducing and adapting EU tools and the ECF framework to the region, as well as to set up a regional digital skills platform. This will improve the understanding of digital skills development, better promote digital inclusion and equity as well as generate opportunities in terms of decent jobs creation, higher employment opportunities and lifelong learning. As illustrated below, the underlying logic is that key challenges in the digitalization process can be addressed more effectively through a common understanding. The private sector and its service providers and multipliers will benefit as this component aims to strengthen digital skills and competencies favoring the creation of an ecosystem in the region, building a network of trainers, providing a platform for regional exchange and dialogue, increasing private sector capacities, and raising awareness. Complementarity to possible bilateral

initiatives should be accounted for, especially on exchange of best practices and possible synergies for capacity building.



3.5. Indicative Logical Framework Matrix

Component 1

Results	Results chain: Main expected results	Indicators	Baselines (2023)	Targets (2027)	Sources of data	Assumptions
Impact	To contribute to South Neighbourhood Partner Countries' inclusive and sustainable socio-economic development by eliminating existing obstacles and barriers to digital services for citizens, public administrations and businesses through supporting the harmonisation of digital markets' regulatory framework, enhancing cybersecurity and improving the level of digital skills.	Number of countries supported by the EU to (1) develop and/or revise, (2) implement digital-related policies/strategies/laws/regulations (GERF)	1 tbd* (2024) 2 tbd* (2024)	1 tbd*(2029) 2 tbd* (2029	National and regional statistics in the SN region; Action monitoring reports	*Not applicable*
Outcome 1	Support the harmonisation of digital markets by improving telecom and digital regulations, and regional convergence for affordable, secure, reliable and high-speed connectivity infrastructure and digital services, while supporting the greening of ICT sector.	Rate of implementation of the planned activities	1 tbd* (2024) 2 tbd* (2024)	1 tbd*(2029) 2 tbd* (2029	Reports Minutes of meetings Benchmark Report Regulatory recommendation	The action is not disrupted by adverse events, such as a fragile security situation, natural hazards, public health crises. Political stability in the target countries The application of new cybersecurity strategies and associated activities does

						not have any adverse impact on human rights in the target countries.
Output 1	Developed regulatory approximation of digital environments and electronic communications norms at regional level in line with the EU best practice.	Number of countries supported by the EU to (a) develop and/or revise digital-related policies/ regulations (**GERF 2.10 (a) OPSYS core indicator) Number of countries supported by the EU to implement digital-related policies/regulations (**GERF 2.10 (b) OPSYS core indicator) Number of countries that have improved the regulatory environment for affordable, secure, reliable and/or high-speed connectivity infrastructure and services Number of countries with policy analyses and recommendations by the Action Number of representatives of countries made aware of policy/regulatory gaps and recommendations to address these gaps, disaggregated by national or regional event, sex, country and institution	To be determined by the implementing partner in the preparatory phase	To be determined by the implementing partner in the preparatory phase		No major governance disruption in the target countries. Partner countries are willing to reach a higher degree of cooperation within the region and with the EU.

Output 2	Improved capacities of national regulatory authorities for developing and implementing conducive regulatory frameworks on telecommunications.	Number of Experts working group workshops organised Regulatory recommendations drafted Number of qualitative exchange of data on digital markets Number of activities assisting member countries in the establishment of independent regulators Number of measures taken by partner country governments to improve the access of women, men, girls and boys, in all their diversity, to basic digital education and training, disaggregated at least by sex (GAP III)	To be determined by the implementing partner in the preparatory phase	To be determined by the implementing partner in the preparatory phase		Partner countries commit to optimise the sustainability of the respective projects by making available the necessary human, financial and material resources.
Output 3	Institutionalized sustainable EMERG network with defined services and consolidated structure	Number of activities assisting member countries in the implementation of national regulatory reforms	To be determined by the implementing partner in the preparatory phase	To be determined by the implementing partner in the preparatory phase		Policy makers, local actors and social partners are willing to cooperate and share their experience within the region.
Output 4	Enhanced capacities of government officials who are engaged in digital transformation efforts in the	Number of certificates issued certifying technical capacity and quality of knowledge.	To be determined by the implementing	To be determined by the implementin	Training material	Partner countries commit to optimise the sustainability of the respective projects by

	Southern Neighbourhood countries	Number of representatives of NRAs and concerned ministries participating in trainings Number of relevant stakeholders capable of developing, implementing and monitoring digital strategies	partner in the preparatory phase	g partner in the preparatory phase		making available the necessary human, financial and material resources.

Component 2:

Results	Results chain: Main expected results	Indicators	Baselines (2023)	Targets (2027)	Sources of data	Assumptions
Outcome	Cybersecurity prevention, preparedness and response of relevant public stakeholders in the Southern Neighbourhood is improved, in compliance with human rights and the rule of law	1.1. Improvement of country position at ITU's Global Cybersecurity and Cyber-wellness Index 1.2. Number of South Partner countries adopting national cyber strategies, action plans and/or policy documents in compliance with human rights and the rule of law 1.3. Level of involvement of key private sector entities (especially from critical infrastructure/services) and civil society (including women, youth and people	2020 Ranking: Algeria on 104th, Egypt on 23nd, Israel on 36th, Jordan on 70th , Libya on 113th, Lebanon on 109th, Morocco on 49th,Palestine on 122nd , Tunisia on 45th	Improvement of country position at ITU's Global Cybersecurity and Cyber-wellness Index by at least 3 places (2029)	Global Cybersecurity Index	The action is not disrupted by adverse events, such as a fragile security situation, natural hazards, public health crises. Political stability in the target countries The application of new cybersecurity strategies and associated activities does not have any adverse impact on human rights in the target countries.

		with disabilities representatives) in cybersecurity decision-making and implementation.				
Output 1	The national legal framework and cybersecurity governance are strengthened in line with the framework for responsible state behaviour in cyberspace.	1.1. Increased awareness of Decision-makers on cybersecurity, cyber norms and internal low (from 1 to 10) 1.2. Number of draft national cyber strategies, action plans and/or policy documents in line with the EU best practice and standards Number of incident response organisations and CSIRTs/CERTs established and/or functional in the South Partner countries.	To be determined by the implementing partner in the preparatory phase	To be determined by the implementing partner in the preparatory phase	Project reports National reports from cyber-coordinating Ministries Press releases	Willingness of relevant Ministries to engage with the EU and in international conferences
Output 2	Increased operational capacities for cyber incidents management and improved inter-agency cooperation at national level.	1.1. Number of incident response organisations and national Computer Emergency Response Teams (CERTs) created and/or further developed in the target countries that are recognized by the private sector and key government agencies as national and international focal points for cyber incidents	To be determined by the implementing partner in the preparatory phase	To be determined by the implementing partner in the preparatory phase	Project update reports National legislation on the setting up of national CERTs National CERTs reports/ websites	National legislative process for the establishment of CERTs is not blocked Allocation of funding from the national budget for the minimum CERT set up and staff recruitment is approved Good and efficient cooperation amongst

		1.2. Number of incident management/response cases monitored and effectively handled by national computer emergency response teams (CERTs) 1.3. Increased level of cyber-hygiene awareness of decision-makers and public institutions staff (from 1 to 10)				Ministries and Agencies Required software and hardware is available Trained staff remain within their institutions beyond the capacity building exercise Ability of the implementing partner to mobilise timely the right expertise for the roll out of activities Translation and interpretation services for the roll out of activities do not create delays
Output 3	A community of stakeholders sharing best practices and incident information is fostered at regional, trans-regional and international level.	3.1. Number of formal or informal cyber information sharing networks created and/or enhanced that facilitate incident report sharing/early warning/mitigation of serious cyber incidents. 3.2. Number of table-top exercises and mock operations undertaken within the project framework. 3.3. Number of countries gaining membership to	To be determined by the implementing partner in the preparatory phase	To be determined by the implementing partner in the preparatory phase	Project update reports National CERTs reports/websites Regional organisations' reports Press releases	Minimum existing trust for good and efficient cooperation amongst countries

		international professional cyber associations.				

Component 3:

Results	Results chain: Main expected results	Indicators	Baselines (values and years)	Targets (values and years)	Sources of data	Assumptions

Outcome 1	Support a standardised measurable digital competencies and skills' framework for the private sector in the Southern Neighbourhood Countries and the establishment of a regional digital skills' platform.	1.1 Functioning framework established. 1.2 Functioning platform established and its usage ensured.	1.1 tbd* (2024) 1.2 tbd* (2024)	1.1 tbd* (2029) 1.2 tbd* (2029)	Studies; after event reports/feedback forms; Project progress reports; Final report National statistics; Ad hoc surveys	1. The political and security situation allows for the implementation of project activities and does not deteriorate to an unmanageable level. 2. National government partners remain committed and support project implementation. 3. Trust is built among stakeholders.
Output 1	A common regional digital competencies and skills' framework for the private sector is piloted and aligned with the European Digital Competence Framework (ECF).	1.1.1 Number of countries adopting and using the framework. 1.1.2 Number of public-private dialogues to develop and agree on this framework.	1.1.1 tbd* 1.1.2 tbd*	1.1.1 tbd* 1.1.2 tbd*		

Output 2	The quality of digital services is standardised in cooperation with service multipliers for the benefit of private sector support organisations and SMEs.	2.1.1 Satisfaction level of stakeholders on quality of actions/recommendations proposed in regional framework. 2.1.2 Number of companies benefiting from the newly created framework.	2.1.1 tbd* 2.1.2 tbd*	2.1.1 tbd* 2.1.2 tbd*		
Output 3	A regional digital skills' platform/network/group of practitioners is developed to exchange experiences and develop strategies linked to digital skills gaps, to foster decent job creation, in particular for youth and women, and reinforces coordination among public and private stakeholders.	3.1.1 Number of jobs created, disaggregated by sex. 3.1.2 Number of companies benefiting from newly created online platforms, including women-led. 3.1.3 Number of workshops and knowledge-sharing events organised for private sector networks, including women networks.	3.1.1 tbd* 3.1.2 tbd*	3.1.1 tbd* 3.1.2 tbd*		
Output 4	Private sector service providers are trained on digital skills and training networks for SMEs are established.	4.1.1 Number of digital skills development trainings conducted, including to women. 4.1.2 Number of trainers trained, including women.	4.1.1 tbd* 4.1.2 tbd*	4.1.1 tbd* 4.1.2 tbd*		

*tbd = to be determined during the inception phase.

4. IMPLEMENTATION ARRANGEMENTS

4.1. Financing Agreement

In order to implement this action, it is not envisaged to conclude a financing agreement with the partner countries.

4.2. Indicative Implementation Period

The indicative operational implementation period of this action, during which the activities described in section 3 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of adoption by the Commission of this financing Decision.

Extensions of the implementation period may be agreed by the Commission's responsible authorising officer by amending this financing Decision and the relevant contracts and agreements.

4.3. Implementation Modalities

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures[32].

4.3.1. Indirect Management with pillar-assessed entities

Each of the three components of this action may be implemented in indirect management with a pillar-assessed entity or potentially a consortium of pillar-assessed entities.

For component 1, the entity will be selected using the following criteria: its ability to provide specialised knowledge on ICT regulatory topics; in house expertise as well as access to a large pool of outside experts which can be mobilise for short term assignments; any previous experience of cooperating with regional regulatory organisations will be a plus; capacity and flexibility to identify logistical arrangements (e.g. via subcontracting) in order to facilitate meetings on behalf of EMERG.

For component 2, the entity will be selected using the following criteria: specific cybersecurity technical expertise; expression of support from cyber-competent authority/ies in the EU; management capacity demonstrated through implementation of previous actions in the security sector; track record of engagement with the Southern Neighbourhood region.

For component 3, the entity will be selected using the following criteria: suitability in terms of the nature of the action; own operational capacity and relations with the key stakeholders of this action; value added in terms of digital skills development in the Southern Neighbourhood; transparency and absence of conflict of interests in performing its tasks.

In case of a consortium, each entity would need to fulfil the above-mentioned criteria.

The implementation by these entities entails carrying out the activities identified in section 3, related specifically to each component and the overall objective of the action.

[32] EU Sanctions Map. Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails.

4.3.2. Changes from indirect to direct management mode due to exceptional circumstances

If the implementation modality under indirect management as defined in section 4.3.1. cannot be implemented due to circumstances beyond the control of the Commission, the modality of implementation by grants under direct management would be used according to the criteria mentioned for each component under section 4.3.1.

4.4. Scope of geographical eligibility for procurement and grants

The geographical eligibility in terms of place of establishment for participating in procurement and grant award procedures and in terms of origin of supplies purchased as established in the basic act and set out in the relevant contractual documents shall apply, subject to the following provisions.

The Commission's authorising officer responsible may extend the geographical eligibility on the basis of urgency or of unavailability of services in the markets of the countries or territories concerned, or in other duly substantiated cases where application of the eligibility rules would make the realisation of this action impossible or exceedingly difficult (Article 28(10) NDICI-Global Europe Regulation).

4.5. Indicative Budget

Indicative Budget components	**EU contribution (amount in EUR)**	**Third-party contribution (amount in EUR)**
Implementation modalities – cf. section 4.3		
Component 1		
Indirect management with a pillar-assessed entity– cf. section 4.3.1	4 000 000	N.A.
Component 2		
Indirect management with a pillar-assessed entity– cf. section 4.3.1	4 000 000	N.A.
Component 3		
Indirect management with a pillar-assessed entity– cf. section 4.3.1	6 000 000	N.A.
Evaluation – cf. section 5.2 **Audit** – cf. section 5.3	may be covered by another Decision	N.A.
Strategic communication and Public diplomacy – cf. section 6	will be covered by another Decision	N.A.
Contingencies	N.A.	N.A.
Totals	**14 000 000**	

4.6. Organisational Set-up and Responsibilities

A steering committee will be established for each component with the participation of the relevant Commission services.

5. PERFORMANCE MEASUREMENT

5.1. Monitoring and Reporting

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process, and part of the implementing partners' responsibilities. To this aim, each implementing partner shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its Outputs and contribution to the achievement of its Outcomes, and if possible at the time of reporting, contribution to the achievement of its Impacts, as measured by corresponding indicators, using as reference the logframe matrix.

Monitoring will assess gender equality results and the implementation of the rights-based approach working principles (applying all human rights for all; meaningful and inclusive participation and access to decision-making; non-discrimination and equality; accountability and rule of law for all; and transparency and access to information supported by disaggregated data). Monitoring will be based on indicators that are disaggregated by sex, age, and disability when applicable.

The Commission may undertake additional project monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).
Arrangements for monitoring and reporting, including roles and responsibilities for data collection, analysis and monitoring:

The monitoring level will be for each component of the action. Every component will have its own logical framework, which will be completed during the inception period and updated during implementation. SDGs indicators and EU Result Framework Indicators should be taken into account. To ensure a closer follow-up, every implementing partner may provide a monthly Flash Report indicating the past activities, activities in the pipelines, difficulties encountered and measures taken to mitigate.

5.2. Evaluation

Having regard to the nature of the action, a mid-term evaluation will be carried out for this action or its components via independent consultants contracted by the Commission.

It will be carried out for accountability and learning purposes at various levels (including for policy revision), taking into account in particular the complexity and the various topics covered by the action.

Evaluation shall also assess to what extent the action is taking into account the human rights-based approach as well as how it contributes to gender equality and women's empowerment and disability inclusion. Expertise on human rights, disability and gender equality will be ensured in the evaluation teams.

The Commission shall form a Reference Group (RG) composed by representatives from the main stakeholders at both EU and national (representatives from the government, from civil society organisations (private sector, NGOs, etc.), etc.) levels. If deemed necessary, other donors will be invited to join.

The Commission shall inform the implementing partners at least 2 months in advance of the dates envisaged for the evaluation exercise and missions. The implementing partners shall collaborate efficiently and

effectively with the evaluation experts, and inter alia provide them with all necessary information and documentation, as well as access to the project premises and activities.

The evaluation reports shall be shared with the partner countries and other key stakeholders following the best practice of evaluation dissemination[33]. The implementing partners and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the partner countries, jointly decide on the follow-up actions to be taken and any adjustments necessary, including, if indicated, the reorientation of the project.

The financing of the evaluation shall be covered by another measure constituting a financing Decision.

5.2. Audit and Verifications

Without prejudice to the obligations applicable to contracts concluded for the implementation of this action, the Commission may, on the basis of a risk assessment, contract independent audit or verification assignments for one or several contracts or agreements.

6. STRATEGIC COMMUNICATION AND PUBLIC DIPLOMACY

All entities implementing EU-funded external actions have the contractual obligation to inform the relevant audiences of the Union's support for their work by displaying the EU emblem and a short funding statement as appropriate on all communication materials related to the actions concerned. To that end they must comply with the instructions given in the 2022 guidance document *Communicating and raising EU visibility: Guidance for external actions* (or any successor document).

This obligation will apply equally, regardless of whether the actions concerned are implemented by the Commission, the partner country, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU Member States. In each case, a reference to the relevant contractual obligations must be included in the respective financing agreement, procurement and grant contracts, and contribution agreements.

For the purpose of enhancing the visibility of the EU and its contribution to this action, the Commission may sign or enter into joint declarations or statements, as part of its prerogative of budget implementation and to safeguard the financial interests of the Union. Visibility and communication measures should also promote transparency and accountability on the use of funds. Effectiveness of communication activities on awareness about the action and its objectives as well as on EU funding of the action should be measured.

Implementing partners shall keep the Commission and the EU Delegation/Office fully informed of the planning and implementation of specific visibility and communication activities before the implementation. Implementing partners will ensure adequate visibility of EU financing and will report on visibility and communication actions as well as the results of the overall action to the relevant monitoring committees.

[33] See best practice of evaluation dissemination