EN

THIS ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX 21

to the Commission Implementing Decision on the financing of the multiannual action plan in favour of Sub-Saharan Africa for 2024-2025

Action Document for Safe Digital Boost for Africa (SDBA)

MULTIANNUAL PLAN
This document constitutes the multiannual work programme within the meaning of Article 110(2) of the Financial Regulation, and an action plan within the meaning of Article 23 of the NDICI-Global Europe Regulation.

1 SYNOPSIS

1.1 Action Summary Table

1. Title **CRIS/OPSYS business reference** **Basic Act**	Safe Digital Boost for Africa (SDBA) OPSYS number: ACT-62401 Financed under the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe)
2. Team Europe Initiative	Yes Team Europe Initiative in support to African economic integration towards the African Continental Free Trade Area (AfCFTA) Team Europe Initiative Digital Economy and Society in Sub-Saharan Africa.
3. Zone benefiting from the action	The action shall be carried out in Sub-Saharan Africa
4. Programming document	Multi-Annual Indicative Programme for Sub-Saharan Africa 2021-2027
5. Link with relevant MIP(s) objectives / expected results	Priority area 4: Digital and Science, Technology and Innovation Result 1.1: Secure, human-centric and harmonised digital standards, legal and regulatory frameworks are promoted at regional/continental levels. Priority Area 5: Sustainable Growth and Decent Jobs Specific Objective 1: Increase sustainable intra-African trade and mobility, making them safer, cheaper, faster and greener; and strengthening Africa-EU trade. Result 1.6: Liberalisation of trade in services progresses and digital trade is facilitated. Specific Objective 3: An investment climate in Sub-Saharan Africa conducive to private sector development and investments, and improved business capacities and access to finance for MSMEs. Result 3.1: Improved investment climate, regional market intelligence and identification of barriers to investments.

PRIORITY AREAS AND SECTOR INFORMATION				
6. Priority Area(s), sectors	Sub-Saharan Africa Regional MIP: Priority Area 4: Digital and Science, Technology and Innovation Priority Area 5: Sustainable Growth and Decent Jobs DAC Sector: 220 – communications 331 - Trade policy and regulations			
7. Sustainable Development Goals (SDGs)	Main SDG: SDG 8 – Decent work and economic growth Other significant SDGs: SDG 1 – No Poverty SDG 5 – Gender Equality SDG 9 – Industry, Innovation and Infrastructure SDG 10 – Reduced Inequalities SDG 16 – Peace, Justice and Strong Institutions SDG 17 – Partnerships for the Goals			
8 a) DAC code(s)	22010 – Communications policy and administrative management - 15% 15110 - Public sector policy and administrative management – 15% 22040 – Information and communication technology - 30% 33110 - Trade policy and administrative management - 10% 33120 - Trade facilitation - 20% 33130 - Regional trade agreements (RTAs) - 10%			
8 b) Main Delivery Channel	40000 - Multilateral Organisations			
9. Targets	☐ Migration ☐ Climate ☒ Social inclusion and Human Development ☒ Gender ☐ Biodiversity ☐ Education ☒ Human Rights, Democracy and Governance			
10. 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 @	☒	☐	☐
11. Internal markers and Tags:	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	Digitalisation @	☐	☐	☒
	digital connectivity digital governance digital entrepreneurship digital skills/literacy digital services	YES ☐ ☒ ☒ ☒ ☒	NO ☒ ☐ ☐ ☐ ☐	
	Connectivity @	☒	☐	☐
	digital connectivity energy transport health education and research	YES ☐ ☐ ☐ ☐	NO ☒ ☒ ☒ ☒	
	Migration @	☒	☐	☐
	Reduction of Inequalities1 @	☐	☒	☐
	Covid-19	☒	☐	☐
BUDGET INFORMATION				
12. Amounts concerned	Budget lines (article, item)[1]: 14.020120 : 25 150 000 14.020121 : 42 150 000 14.020122 : 32 700 000 Total estimated cost: EUR 100 000 000			

[1] Calculated as follows: the Continental component (EUR 9 000 0000) was split along the 3 budget lines as such: 35% on West Africa line (EUR 3 150 000), 35% on East and Central Africa line (EUR 3 150 000), 30% on Southern and Indian Ocean line (EUR 2 700 000).

	Total amount of EU budget contribution EUR 100 000 000 Team Europe Initiative in support to African economic integration towards the African Continental Free Trade Area (AfCFTA) to which: Denmark, France, Germany, Finland, Ireland, the Netherlands, Portugal, Sweden are contributing. For the time being, there are no indicative TEI MS contributions available Team Europe Initiative Digital Economy and Society in Sub-Saharan Africa (Code: 001) to which Belgium, Estonia, Finland, France, Germany, Lithuania, Luxembourg, Netherlands, Portugal, Spain and Sweden are contributing. For the time being, there are no indicative TEI MS contributions available.
MANAGEMENT AND IMPLEMENTATION	
13. Type of financing	**Direct management** through**:** **-** Grant - Procurement **Indirect management** with the entity(ies) to be selected in accordance with the criteria set out in section 4.4.3

1.2 Summary of the Action

The Action has the objective to provide comprehensive support for trade and digitalisation towards a sustainable setup of an African single digital market within a robust cybersecurity environment. The objectives of the Action span across three macro-areas: eCommerce and ePayments; eGovernance; and cybersecurity to complement the support provided under other EU Actions including the Policy and Regulation Initiative for Digital Africa (PRIDA), the Data Governance in Africa initiative, Africa Europe Regulators Partnership and overall digital infrastructure investments.
The Action will be segmented into five distinct components: regional clusters of countries in Western, Eastern, Central and Southern Africa, as well as a continental component that may support coordination and implementation of said clusters.

Within the area of **eCommerce and ePayments**, the Action will support the different steps of digitally-enabled Business-to-Business (B2B) and Business-to-Consumer (B2C) trade transactions. From ordering to delivering goods and services, it will focus on expanding and rendering more inclusive, secure and trusted existing eCommerce platforms in collaboration with national postal services. At the same time, the Action will support the payment systems enabling such transactions through the interconnectivity of existing payment systems, offering tailor-made solutions for low transactions traders, and facilitating fintech integration, all in line with EU standards in view of their future interoperability with EU systems.

Through its **eGovernance** work stream**,** the Action aims to address related legal and technical gaps at national, regional and continental level by supporting an enabling environment, the development and implementation of identified reusable eGovernance building blocks and services that will accelerate the development of an African single digital market.

To complement this, the Action will focus on tackling the essential aspects of **cybersecurity**, by enhancing cyber resilience of target regions and countries. It will support the development of strategies, laws and regulations, promoting cyber hygiene, as well as enhancing capacity for the protection of critical infrastructure. Such an approach will not only ensure a unified political strategy against cross-border cyber threats, but also facilitate cooperation at technical level in preventing, deterring and responding to cyber-attacks.

The **Overall Objective** (Impact) of this Action is to accelerate digital trade and e-governance at continental, regional and bilateral levels within a robust cybersecurity environment in the framework of an African single digital market.

The **Specific Objectives** (Outcomes) of this action are to:

1. Enable and increase the inclusive and secure use of eCommerce platforms for cross-border trade.
2. Enable and harmonise national payment systems and improve cross-border ePayments and their interoperability.
3. Improve the legal, organisational and technical enabling environment for eGovernance and enhance related cross-border interoperable service delivery.
4. Enhance the development of regionally harmonised cybersecurity frameworks and protection of critical information infrastructure.

1.3 Zone benefitting from the Action

The Action shall be carried out in sub-Saharan Africa countries, out of which all are included in the list of ODA recipients.

2 RATIONALE

2.1 Context

The Action is aligned with the priorities set under the Global Gateway strategy and the Joint Communication Towards a Comprehensive Strategy with Africa launched in 2020.[2] It fully contributes to the Global Gateway Africa-Europe Investment Package announced at the EU-AU Summit in February 2022, and it is considered a crucial intervention to promote alignment with EU policies and values in the current geopolitical situation.[3] In parallel, the specific work streams related to the areas of eCommerce and ePayments will contribute to the objectives of the EU Trade Policy Review of increased cooperation with African countries in economic integration and the use of common standards.[4]

The Global Gateway defines digital transformation, and in particular investments on digital infrastructure, as one of the key geopolitical priorities of the EU. The EU is increasingly committed to connecting countries and regions with hardware investments that will make digital technologies and services accessible to all within and across continents, with a focus on Sub-Saharan Africa. The gender gap in ICTs in Africa is 23%. Key factors include availability, affordability, norms, capacity and skills, relevant content, participation in decision-making roles pertaining to the Internet and/or in the technology sector, relevant policies, and/or other systemic barriers.[5] Investments in infrastructure alone are not sufficient to achieve and sustain digital transformation: they need to be complemented by interventions that ensure the financial and operational viability of digital connectivity. By addressing the regional and continental layers of eCommerce and ePayments, eGovernance and cybersecurity, as part of efforts within the Africa-Europe Investment Package, the Action has the goal to provide a comprehensive contribution at the intersection of trade and digitalisation towards a sustainable setup of a single digital market in Africa.

eCommerce and ePayments

This Action builds on the momentum for African integration under the African Continental Free Trade Agreement (AfCFTA) and the African Union (AU) Action Plan for Boosting Intra-African Trade (BIAT).[6] The AfCFTA is one of the AU flagship projects under the ten-year implementation plan of its Agenda 2063, where the main objective is

[2] The Global Gateway, JOIN(2021) 30 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021JC0030. Towards a comprehensive Strategy with Africa, JOIN(2020) 4 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0004.

[3] EU-Africa: Global Gateway Investment Package.

[4] Trade Policy Review - An Open, Sustainable and Assertive Trade Policy, COM(2021) 66 final, https://eur-lex.europa.eu/resource.html?uri=cellar:5bf4e9d0-71d2-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[5] AU Strategy for Gender Equality & Women's Empowerment 2018-2028, https://au.int/sites/default/files/documents/36195-doc-52569_au_strategy_eng_high.pdf.

[6] Action Plan for boosting intra-African trade, https://au.int/web/sites/default/files/newsevents/pressreleases/26498-pr-action_plan_for_boosting_intra-african_trade_f-english.pdf.

to 'create a single market for goods and services with free movement of people and investments', thus expanding intra-African trade across the continent, enhancing competitiveness, and supporting economic transformation in Africa.[7] Following the AU Strategy, endorsed by the Sharm El Sheik Declaration, the AU Assembly mandated an approach for incorporating eCommerce into the AfCFTA in February 2020.[8] In addition, the African Digital Transformation Strategy (AU DTS) 2020–2030 set the objective to create a Digital Single Market in Africa by 2030.[9] As a result, a "Protocol on Digital Trade" was incorporated under Phase III of the AfCFTA agreement negotiations in an aim to reduce digital trade barriers between countries. Finally, the AU Data Policy Framework also recognises that the strategies to enhance e-commerce cannot be formulated in isolation since e-commerce intersects with other issues, including Digital ID, data governance, customs duties, cross-border data flows, cybersecurity, payments system interoperability, among others.[10] These strategies must be designed with an in-depth understanding of the gendered nature of socio-economic challenges. They must consider the factors that hinder women and girls from adopting technology and digitalization and explore use cases and potential measures to mitigate such challenges.

Trade and regional integration constitute an important component of the Africa-EU partnership. The 6th Africa- EU Summit in February 2022 reiterated the commitment of the two partners to support the continental economic integration process, in particular the AfCFTA.
The European Union, as first trade partner for African products, primary Aid for Trade provider and key partner for sustainable and green investment in Africa, is the strategic partner to support the African economic integration agenda. It stands ready to share good practices and its own experience to accompany African efforts in the digitalisation of trade towards a single digital market. And both the EU and Africa have an interest in partnering for further alignment on Digital Trade to contribute to creating a level-playing field for African and EU based businesses selling products both in Africa and in the EU. Partnering will also result in increased and easier market access for EU and African businesses especially in countries where bilateral trade agreements with the EU (Economic Partnership Agreements, EPAs) are signed, and security for their consumers in line with EU standards.

eGovernance
Effective digital public services can provide a wide variety of benefits across social and economic aspects, ensuring the advancement of good governance, democratic participation, rule of law and transparency. Functional eGovernance benefits governments, citizens and businesses alike, by increasing transparency and enabling greater participation, as well as ease of doing business. In the EU, the eGovernment Action Plan set goals to modernise digital public services and make the EU a better place to work, live and invest.[11] The eIDAS Regulation created one single framework for electronic identification (eID) and trust services, making it more straightforward to deliver services across the European Union and ensuring that electronic interactions between businesses are safer, faster and more efficient across 27 EU MS.[12]

The AU DTS 2020-2030 refers to eGovernance and Digital ID as critical 'sectors' to drive digital transformation. Supporting the setup of a regionally harmonised eGovernance ecosystem at legal and technical level in Africa ultimately provides for economies of scale and scope, allowing sustainable business ecosystems to thrive. According to the AUC, in 2021 nearly 85% of African countries had national ID systems underpinned by an electronic database and more than 70% of African countries collect biometric data to ensure uniqueness of identities. There are more than 35 African countries in the process of developing and improving their foundational

[7] Agreement establishing the African Continental Free Trade Area (AfCFTA), https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf.
[8] Sharm El Sheik Declaration, October 2019, https://au.int/sites/default/files/decisions/37590-2019_sharm_el_sheikh_declaration_-_stc-cict-3_oct_2019_ver2410-10pm-1rev-2.pdf.
[9] The Digital Transformation Strategy for Africa (2020-2030), https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.pdf.
[10] AU Data Policy Framework, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf.
[11] EU eGovernment Action Plan 2016-2020, COM(2016) 179 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179.
[12] REGULATION (EU) 910/2014 (eIDAS Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910.

legal identification and national ID systems to address the identification gap. Main eGovernance building blocks, in particular eID, e-signature, interoperability, and digital registries, form an essential foundational layer and provide legal certainty for participants in the digital society as they progress toward a digital single market by creating services, fostering further innovation and investments.

Cybersecurity

When developing legal and technical elements for eCommerce and ePayments transactions, as well as eGovernance building blocks and services, safeguarding infrastructure and data from unathorized access is fundamental. Given the increasing reliance on digital platforms and the Internet, the potential for cyber threats poses a significant risk to both continents' socio-economic growth. The EU and AU have acknowledged the growing threats posed by cyberattacks, cybercrime, and other malicious cyber activities, which jeopardize the safety and prosperity of their respective regions. The shared goal is to create a resilient and secure cyber ecosystem that safeguards critical infrastructures, businesses, and the personal data of citizens, thus promoting trust in digital technologies and fostering economic growth.

Recent key policy developments in Europe include the 2023 EU NIS Directive 2.0, which reinforces cybersecurity requirements foreseen by the original NIS Directive across sectors[13]; the EU Cybersecurity Act (2019), which strengthened the mandate of the European Union Agency for Cybersecurity (ENISA) and introduced a framework for the certification of ICT products, services, and processes; the Joint Communication on Resilience, Deterrence, and Defence, which addresses cyber threats and cyber-attacks, emphasizing the importance of international norms and principles in cyberspace.[14] The EU's Cyber Diplomacy Toolbox complements policy work by guiding the EU's external action on the framework of its common foreign and security policy in response to malicious cyber activities.

In parallel, the AU Convention on Cybersecurity and Personal Data Protection (also known as Malabo Convention) addresses the need for harmonized legislation concerning cybersecurity and data protection across the continent.[15] The AU DTS further sets the vision for a secure and resilient digital space in Africa, emphasizing the importance of capacity building, cross-border cooperation, and Public-Private Partnerships (PPPs). The 2022 AU Data Policy Framework - the implementation of which is supported by the EU and its MS through the *Data Governance in Africa* Global Gateway flagship initiative - includes specific recommendations to AU MS, highlighting how "security of data (including confidentiality, integrity and availability) does [not only] depend on the physical location of the servers hosting such data.[16] Rather, it is a function of the normative rules - including norms, policies, regulations, laws and protocols (such as data standards and technical interfaces), and the implementation of technologies and security measures (such as encryption, firewalls and access controls) - that are put in place by public or private service providers in the way that they store, access, share and use the data".

The Action will be in line with the EU Gender Action Plan 2021-2025 (GAP III) and its thematic areas of engagement "Advancing equal participation and leadership" and "Addressing the challenges and harnessing the opportunities offered by the green transition and the digital transformation".[17] Specifically, it aims to strengthen economic and social rights and the empowerment of girls and women and to advance equal participation and leadership, acknowledging the need to ensure that all genders are protected from specific cyber threats and this diversity is considered when designing government and trade digital services. Additionally, the Action will be aligned to the EU-AU Innovation Agenda, ensuring gender equality and empower women, youth, persons with

[13] DIRECTIVE (EU) 2022/2555 (NIS 2 Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1702656774498.

[14] REGULATION (EU) 2019/881 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881.
Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450.

[15] African Union Convention on Cybersecurity and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

[16] AU Data Policy Framework, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf.

[17] EU Gender Action Plan (GAP) III, JOIN(2020) 17 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0017.

disabilities and other groups in vulnerable situation, as well as the AU Strategy on Gender Equality and AU Women's Empowerment (GEWE) 2018-2028, which endorse technological and E- solutions and platforms which advance gender equality and women's empowerment.[18]

2.2 Problem Analysis

eCommerce and ePayments

Digitalisation increases the scale, scope and speed of trade. It allows companies to bring new products and services to a larger number of digitally connected customers across the globe.

Digital trade covers digitally ordered but physically delivered products (e.g. buying a physical book from an eCommerce platform) and products which are digitally ordered and digitally delivered (e.g. purchasing market research). Despite playing an increasingly important role at global level, African digital trade is still in a nascent stage and faces several challenges ranging from weak technological infrastructure and innovation, legal and regulatory frameworks to lack of trust and consumer protection in the online space.

The majority of online Business-to-Business (B2B) activity within Africa appears to be carried through independent websites owned by individual firms[19]. SMEs operating their own specialised B2B websites prefer not to be on a marketplace because they see no value-added in using such marketplaces. Sector-specific B2B marketplaces (machine tools, car parts, etc.) exist, but most of these appear to focus on national markets. B2B marketplaces with transactional capability are usually foreign-owned and designed to sell into Africa, rather than from one African country to another. And African businesses, particularly MSMEs enter the markets as suppliers rather than consumers of third-party digital products. High-value specialised products, such as medical equipment, are presently the most traded online B2B goods in Africa and are easier to trade cross-border.[20] Higher profit margins can absorb currency fluctuations and make it easier to justify dedicated freight solutions or courier services. Lower-priced goods struggle to justify the significant intra-African freight costs and delays. It is often simpler and quicker to import goods in bulk from outside of Africa: businesses reselling smaller items, such as spare parts, often sourced directly from international suppliers, rather than within Africa. In addition, evidence shows that women-owned e-commerce business face greater barriers than those owned by men in entering the market and scaling up their business—including a lack of access to funding, patriarchal attitudes and less specific digital training.[21]

Whilst COVID-19 gave a boost to African eCommerce, the region lags others in the 2020 UNCTAD business-to-consumer (B2C) eCommerce Index[22]. For B2C online marketplaces for physical goods, 10 African countries concentrate 94% of all online business on the continent[23]. The majority of marketplaces in Africa use a domestic, country-focused model; that is, national platforms that only sell in one country. Just 1% of Africa's eCommerce marketplaces are responsible for 60% of the marketplace traffic on the whole continent.

In terms of ePayments, only 11% of the marketplace websites enable financial transactions (the rest are classified sites with sales made offline) which limits the possibilities of selling internationally. In certain regions, the development of digital trade is dependent on the establishment of the Payments and Settlement systems. In addition to the recently being developped continental Pan-African Payment and Settlement System (PAPSS), Regional

[18] The AU-EU Innovation Agenda, July 2023, https://research-and-innovation.ec.europa.eu/system/files/2023-07/ec_rtd_au-eu-innovation-agenda-final-version.pdf.
AU Strategy for Gender Equality & Women's Empowerment 2018-2028, https://au.int/sites/default/files/documents/36195-doc-52569_au_strategy_eng_high.pdf.

[19] International Trade Centre (ITC) and eCommerce Forum Africa, https://intracen.org/file/internationaleCommerceinafricalowrespdf.

[20] EU's digital task force, June 2019, https://digital-strategy.ec.europa.eu/en/library/new-africa-europe-digital-economy-partnership-report-eu-au-digital-economy-task-force.

[21] Gender Equality in Digitalization. Key Issues for Programming, UNDP, 2021, https://www.undp.org/sites/g/files/zskgke326/files/migration/eurasia/UNDP-RBEC-Gender-Equality-Digitalization-guidance.pdf.

[22] https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf.

[23] Africa Marketplace Explorer, International Trade Center - https://ecomconnect.org/.

Payments and Settlement System are currently being implemented in all 5 RECs. However, none include other payment service providers in settlements to broaden access and positively contribute to financial inclusion and competition in the payments industry. Further technical and financial support would be needed to accelerate their implementation and harmonisation in view of the AfCFTA and the PAPSS.

Several regional electronic payments systems still face the issue to organise electronic payments between countries that do not have single currencies, and system integration and adoption is weak. And several regions would benefit from increased capacity in technology profiling, identification, demonstration, selection and recommendations for the implementation of Payments Settlement System.

Finally, mirroring the same issue eCommerce faces, there are currently ePayment solutions for high-value tansactions but there is a lack of ePayments methods for low transactions mostly coming from MSMEs or small-scale cross border traders.

eGovernance

As stated in the AU DTS, "despite advancement over the past years, according to the UN e-government development index, Africa is lagging compared to other regions [and] disparity of eGovernment development level is high among Member States of the African Union. […] The political will, lack of coordinating structures among the AU member states and a single pan African digital ID system has been the main reasons for the low levels of digital governance."

Benefits of successful digital government initiatives include more efficiency of government operations, increased transparency and easier citizen access to government services, as well as ease of doing business; increased trust and cooperation between government agencies, both internally and across borders. Regional harmonisation and complementarity of legal, organisational and technical environments must be ensured to enable cross-border interoperability to avoid that nationally developed solutions become redundant or obstructive once countries wish to communicate or offer services across borders. If harmonisation is not ensured, the continent can end up in a situation where digital government services are developed and working within borders but not across-borders for digital single market enablement. Substantial investments and time costs can be prevented if solutions are developed following the same standards and frameworks from the beginning making it easier as a next step to connect them to one another.

Technical environment requirements include building blocks, such as trusted authentication, registries, secure data exchange and interoperability, which is the ability of organisations to interact and exchange information, knowledge and services within and across borders. Regional harmonisation of both legal and technical environments should be ensured to enable cross-border interoperability to avoid that nationally developed solutions become redundant or obstructive once countries wish to communicate or offer services across borders.

Legal, regulatory and technical capacity are fundamental to ensure successful adoption of technologies in public administration, but these efforts may be ineffective if organizational change is not considered. Here, challenges are frequently underestimated. Governments often view eGovernance and digital transformation as a purely technical matter, while the capability to plan and allocate sufficient resources to digital transformation is often neglected. Organizational choices show eGovernment implementation is effective and sustainable when administrations strive to ensure a user-centred approach to digital government service delivery.

Averages for Internet use are 35% for men and 24% form women for Africa. In addition to being less connected, women are underrepresented online and in data. Few countries collect gender-disaggregated user data. Also, fewer women than men use social media or other online platforms. This has first-order implications for online representation, access, perspectives and knowledge creation, but there are also second-order implications in terms of the data sets created, the algorithms developed, andthe machine learning that takes place in the digital transformation of the public sector, such as the unintentional exclusion of certain groups in vulnerable situation (minorities, persons with disabilities, and those living in rural or remote areas) in service delivery. There are also intersectionality and multipliers effect in settings characterized by inequitable powerrelations and discrimination that can interfere with the ability of women, those living in poverty,and other vulnerable groups to access public services. There is still insufficient understanding of how the design and implementation of e-government affects people of different ages, capabilities and income levels and what needs to be done to address discrimination and

ensure equity for all.[24]

Cybersecurity

African countries consistently rank lower in various global cybersecurity indexes, pointing to significant vulnerabilities both at legal and technical level that could be exploited by threat actors. Given that cyber threats do not respect borders, regional and international collaboration becomes imperative.

When it comes to policy enablers, African countries already have a common framework in the abovementioned AU Convention on Cyber Security and Personal Data Protection. However, as of November 2023, only 19 countries out of 55 had signed and 15 countries had ratified the convention, which allowed for the Convention to entry into force in June 2023.[25]Although the AUC and regional bodies including the Economic Community of West African States (ECOWAS), the Southern African Development Community (SADC) and the East African Community (EAC) have shown interest in establishing continental and regional cybersecurity frameworks, regional implementation also remains challenging. The absence of cohesive cybersecurity regulations and their inconsistent enforcement leaves gaping vulnerabilities. Without robust regulations, governments are unable to counter sophisticated cyber threats, industries fail to protect their assets, and citizens are left vulnerable to cybercrime. The multilayered nature of cybersecurity requires a strategic perspective that harmonises various policy objectives – from safeguarding critical infrastructure to ensuring individual privacy. Most African countries struggle with adopting international cybersecurity standards, with challenges ranging from legislative shortfalls, fragmented enforcement mechanisms, and limited capacity to manage cyber threats.

Educating and building capacity is vital in creating a cybersecurity-aware society. Yet, in many African countries, there's an evident shortage of qualified professionals and awareness programmes. The general population often lacks basic cybersecurity awareness, making them easy prey for cyber-attacks. While larger enterprises might have some cyber defences in place, SMEs, due to the high associated costs and lack of expertise, remain highly vulnerable. Even where there is awareness, businesses might lack the resources to transform this knowledge into actionable defences due to financial constraints or lack of expert guidance.

Despite these challenges, the private sector has shown a growing interest in strengthening Africa's cyber landscape, supported by regulatory support from some governments and international investments. A holistic approach involving governmental bodies, non-profits, academia, and the private sector is essential for creating a cyber-resilient ecosystem. Currently, there is a lack of platforms that promote multi-stakeholder engagement, resulting in fragmented efforts. Effective partnerships can facilitate the exchange of best practices, resources, and intelligence to counter common threats. But complexities arising from differing institutional mandates, objectives, and capacities often hinder these collaborations.

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

- The African Union Commission (AUC), African Union, in particular the Digital Division within the Infrastructure and Energy Department (IED), and the Department of Economic Development, Trade, Industry and Mining (ETTIM) will mobilise required continental actors and coordinate the implementation of continental activities;
- The Secretariats of selected Regional Economic Communities (RECs) may play a key role to help structure and coordinate the overall activities and support the identification of potential participants at the regional and national level.
- National governments, especially Ministries of Trade and ICT and associated entities, regulators and agencies mandated to oversee and manage eCommerce, eGovernance, and cybersecurity at national level and engaging in cross-border cooperation. National Contact Points could be designated in each REC to link with relevant national administrations. Their intervention should promote the public-private dialogue at the national level.
- Private sector organisations, especially those in the tech and critical infrastructure sectors may ensure the

[24] 2022 UN E-Government Survey
[25] African Union (2020). African Union Convention On Cyber Security And Personal Data Protection – Status List.

participation and representation of African and European businesses.

- Civil Society Organisations (CSOs) will ensure the participation and representation of women, children, persons with disabilities and minorities entrepreneurs and consumers.
- Academia specialising in eCommerce, ePayments, eGovernance and cybersecurity may engage for research support and consultation.
- International organisations and European partners working on digitalisation, cybersecurity and economic integration may engage for implementation and support.

3 DESCRIPTION OF THE ACTION

3.1 Objectives and Expected Outputs

The Overall Objective of this action is to accelerate digital trade and e-governance at continental, regional and bilateral levels within a robust cybersecurity environment in the framework of an African single digital market.

The Specific Objectives of this action are to:

1. Enable and increase the inclusive and secure use of eCommerce platforms for cross-border trade.
2. Enable and harmonise national payment systems and improve cross-border ePayments and their interoperability.
3. Improve the legal, organisational and technical enabling environment for eGovernance and enhance related cross-border interoperable service delivery.
4. Enhance the development of regionally harmonised cybersecurity frameworks and protection of critical information infrastructure.

The Outputs to be delivered by this action contributing to the corresponding Specific Objectives (Outcomes) are:

Contributing to Specific Objective 1:

1.1 Continental, Regional and National legal frameworks in cross-border digital trade are developed and/or harmonised in line with EU standards while enhancing the capacity of regulatory actors.

1.2 African B2B and B2C eCommerce platforms are supported in their cross-border development and in ensuring trust and inclusivity.

1.3 Fintech integration and SME development within eCommerce platforms is fostered, with special consideration for women and young entrepreneurs.

1.4 Businesses and citizens awareness to utilise the opportunities offered by eCommerce platforms is increased.

Contributing to Specific Objective 2 :

2.1 Continental, Regional and National legal frameworks in cross-border digital payments are developed and/or harmonised in line with EU standards while enhancing the capacity of regulatory actors.

2.2 Regional payments and settlement systems to facilitate cross-border B2B and B2C payments are improved and/or extended, with special consideration for small-scale traders.

2.3 Regional payment systems interconnection and interoperability with the Pan-African Payment and Settlement System (PAPSS) and future proofing for interoperability with EU system(s) is facilitated.

2.4 Businesses and citizens awareness to utilise the opportunities offered by ePayments is increased.

Contributing to Specific Objective 3:

3.1 Capacities of continental, regional and national actors to improve and harmonise their legal, organisational and technical frameworks for interoperable and cross-border digital government services are increased.

3.2 Technical solutions and building blocks to deploy national and regional level digital government services are developed and customised.

Contributing to Specific Objective 4:

4.1 Capacities of competent authorities to design and implement cybersecurity norms, strategies and regulations are increased at continental, regional and national level.

4.2 Mechanisms and operational capacities for the identification and protection of critical infrastructure and incident response are enhanced.
4.3 Cyber hygiene and awareness of cybersecurity threats are improved through regional and international cooperation.

3.2 Indicative Activities

Activities relating to Output 1.1:

- Analysis of existing continental legal frameworks, including the analysis of regulations for eCommerce of the African Continental Free Trade Area Agreement's Digital Trade protocol.
- Gap Analysis of existing REC and/or national regulations for digital trade, equivalent EU regulations and the proposed AfCFTA digital trade protocol.
- Gap Analysis on the possible alignment of existing regulations with EU standards and on their implementation/enforcement.
- Evaluation of the potential to mainstream social and environmental safeguards in the specific context of vulnerabilities of African countries, citizens and ecosystems.
- Development and/or review of existing model laws in the key aspects related to cross-border digital trade (electronic transactions, electronic signatures, data protection, consumer protection, etc.) that can be transposed at regional and national level in line with EU standards including among others those on security, social rights and environment protection in view of future interoperability.
- Organisation of multi-stakholder workshops (public/private/regulators/civil society) to collaborate on enabling regulation frameworks.
- Transposition of model laws at the regional and national level in the key aspects related to cross-border digital trade based on the continental legal framework.
- Assessment of and/or development of a Monitroning and Evaluation framework on the status of the regional legal frameworks related to digital trade at the regional level taking into account the existing frameworks and best practices in Member States.
- Update and/or develop regional legislation related to digital trade in line with EU standards including among others those on security, social rights and environment protection in view of future interoperability. Domestication of regional legal frameworks into national legislation for regional cross-border digital trade.

Activities relating to Output 1.2:

- Development and introduction of an African Trustmark.
- Development and/or improvement of effective track and trace systems.
- Identification and introduction of eCommerce friendly geolocation systems that can complement the ongoing efforts of introducing national postal addressing systems for last mile delivery.
- Facilitate the integration of tools for customer feedback and/ or redress for greater trust/accountability.
- Identify the Tariff Barriers (TBs) and Non-Tariff Barreirs (NTBs) faced by eCommerce platform operators in selected countries.
- Draft action plans to address the identified TBs and NTBs, engaging the innovation ecosystem to resolve challenges.
- Map the door-to-door delivery of low value items amongst selected countries, including cross – border eCommerce and ePayments platforms, logistics providers, public transport and customs officials, taking into consideration environmental aspects.
- Implement pilot door to door delivery programmes for selected value chains amongst selected countries in partnership with eCommerce and ePayment platforms, national postal services and customs offices promoting de minimis valuations for small items.

Activities relating to Output 1.3:

- Identify the TBs and NTBs faced by eCommerce platform to integrate Fintech operators in selected countries.
- Identify the TBs and NTBs faced by eCommerce platform to develop affordable real time cross-border interoperable payment systems for eCommerce industry.
- Identify FinTech products which could be scaled at a regional level through policy innovations (e.g. sandboxes).

Activities relating to Output 1.4:

- Awareness event and/or campaigns for eCommerce targeting specific groups such as traders, public officers, customs officers, postal services employees, logistics firms, informal sector and local traders and general public.
- Development of toolkits for MSMEs, SMEs and citizens.

Activities relating to Output 2.1:

- Analysis of existing continental legal frameworks, including the analysis of regulations for ePayments of the African Continental Free Trade Area Agreement's Digital Trade protocol.
- Gap Analysis of existing REC and/or national regulations for digital payments, equivalent EU regulations and the proposed AfCFTA digital trade protocol.
- Gap Analysis on the possible alignment of existing regulations with with EU standards and on their implementation/enforcement.
- Evaluation of the potential to mainstream social and environmental safeguards in the specific context of vulnerabilities of African countries, citizens and ecosystems.
- Development and/or review of existing model laws in the key aspects related to cross-border digital payments (electronic transactions, electronic signatures, data protection, consumer protection, etc.) that can be transposed at regional and national level in line with EU standards including among others those on security, social rights and environment protection in view of future interoperability.
- Organisation of multi-stakholder workshops (public/private/regulators/civil society) to collaborate on enabling regulation frameworks.
- Transposition of model laws at the regional and national level in the key aspects related to cross-border digital payments based on the continental legal framework.
- Assess of and/or development of a Monitoring and Evaluation framework on the status of the regional legal frameworks related to digital payments at the regional level taking into account the existing frameworks and best practices in Member States.
- Update and/or develop regional legislation related to digital payments in line with EU standards including among others those on security, social rights and environment protection in view of future interoperability.
- Support domestication of regional legal frameworks into national legislation for regional cross-border digital payments.

Activities relating to Output 2.2:

- Introduce an appropriate national payment method for real time payments based on the ISO/IEC 18004 standard across selected countries (i.e. a QR Code).
- Operationalise a regional Public Key Infrastructure (PKI).
- Connect the appropriate payment method (i.e. QR code) for real time payments with national ePayments, m-Payments operators, MNOs, as well as banks that have adopted the ISO 20022 Universal financial industry message scheme across selected countries.
- Develop the appropriate payment method (i.e. QR code) regulatory framework for interoperability through bilateral agreements in line with EU standards for future interoperability.
- Engage with fintech startups to develop innovative payment solutions tailored to the regional needs

Activities relating to Output 2.3:

- Assess the technical, legal and operational readiness of the current national and regional systems to connect to the PAPSS.
- Define the necessary steps to create a regional payment system based on ISO20022 to connect to the PAPPS for all payment providers, including Mobile Money Providers (MMPs), agent networks by enhancing Bank-to-mobile transactions.es with the PAPPS and EU counterparts including the European Central Bank, focusing on lessons learned, and how to best prepare for interoperability.
- Assess the interoperability capacity of national payment systems to process and settle payments with other regions such as the EU.
- Draft Action plans to define the necessary steps that will enable regional payment systems compatible with the EU counterparts.
- Facilitate dialogues with the EU payment systems focusing on interoperability issues and how to resolve

them (i.e between African and European fintech companies, between African and EU payment system operators).

Activities relating to Output 2.4:

- Organize awareness events and/or campaigns for ePayments for specific sub - groups such as traders, public officers, customs officers, informal sector and local traders.
- Develop toolkits for MSMEs, SMEs and citizens.

Activities relating to Output 3.1:

- Support the establishment of eGovernance regional clusters (focus areas of work may include electronic identity (eID), digital signature, interoperability, registries, payment systems) and facilitate exchanges, trust building, cooperation and coordination within and across clusters.
- Support development or adjustment of continental, regional legal/regulatory and organisational and/or technical frameworks for eGovernance and secure cross-border information exchange and eServices, inspired by European best practices.
- Support implementation and domestication of regional legal/regulatory frameworks for eGovernance.
- Support the development of joint eGovernance curriculums and expand eGovernance training portfolio, including fellowship programs, with a specific target on women and marginalised groups.

Activities relating to Output 3.2:

- Support assessment of technical and organisational environment gaps at national and cluster level for provision of identified digital government services.
- Provide technical assistance to develop terms of reference for eGovernance systems and applications (eg. electronic identity (eID), digital signature, interoperability, registries, payment systems) that are preferably open-source supporting building blocks based architecture.
- Provide support at the national and regional levels to customise identified solutions and building blocks to develop digital government services.
- Support national and regional-level deployment of the identified digital government services (e.g., data validation, background checks, information verification).
- Capacity building for technical and non-technical staff involved in designing, managing, building, commissioning and maintaining the digital government services and building blocks.

Activities relating to Output 4.1:

- Undertake a comprehensive Cybersecurity Maturity Assessment, monitoring progress with global standards including continental frameworks and EU NIS Directive as references; conduct assessments to identify and categorise critical infrastructure entities and cyber threat landscape whilst engaging duty-bearers.
- Provide technical assistance for the review, amendment, ratification of the continental Malabo Convention.
- Support Regional Economic Communities (RECs) and governments in reviewing, drafting and implementing harmonised cybersecurity strategies, legislation and regulation; support national transposition and development of strategies, in line with regional frameworks the Malabo Convention, as well as seek convergence with the Budapest Convention.
- Support establishment or further development of Cybersecurity Centres of Excellence at the national level or within Regional Economic Communities (RECs), where relevant.
- Development and/or review of existing regional model laws for cybersecurity and their action plans; support related domestication.

Activities relating to Output 4.2:

- Provide technical support for the establishment, strengthening, and day-to-day operations of regional, national CSIRTs, and, where possible, supporting the development of CSIRTs within Regional Economic Communities (RECs) and/or at continental level.
- Develop specialized incident response toolkits customized for critical information infrastructure sectors to ensure swift and effective responses to cyber incidents, inclusive of relevant hands-on training on using the Incident Response Toolkit.
- Foster strong collaboration between CSIRTs and critical information infrastructure entities by facilitating

knowledge and experience sharing on incident handling on critical information protection and other relevant issues, conducting joint exercises, and establishing shared platforms for knowledge sharing.
- Promote the setup of Public and Private Partnerships (PPP) for critical information infrastructure.
- Provide technical assistance towards membership to Cybersecurity Collaboration Frameworks (e.g. Forum of Incident Response and Security Teams (FIRST).

Activities related to Output 4.3:
- Organize cyber hygiene campaigns and training sessions that are tailored to the unique needs and context of African countries. Design comprehensive cyber hygiene training program curricula tailored for various sectors across Sub-Saharan Africa, possibly through Centres of Excellence (CoE).
- Develop and run media campaigns that promote best practices in cyber hygiene by engaging with local communities, educational institutions, and organizations to encourage a culture of cyber hygiene and collective responsibility, with a special emphasis on capacitating women, youth and persons with disabilities.
- Support mechanisms for continuous knowledge sharing on cybersecurity issues, including threat intelligence, emerging trends, and evolving cyber threats for regional, continental and international cooperation.
- Support the organisation of innovative competitions on cybersecurity including but not limited to policy hackathons or table-top exercise; as well as capacity-building activities on technical skills and joint exercises.
- Support one, or a network of, academic institutions to host training programmes and identify skillset gaps; as well as identify duty-bearers and rights-holders to participate in an expert network.
- Support scalability of national solutions or innovations at the cluster-level.

The commitment of the EU's contribution to the Team Europe Initiative to which this action refers, may be complemented by other contributions from EU MS in a Team Europe approach. It is subject to the formal confirmation of each respective member's meaningful contribution as early as possible. In the event that the TEIs and/or these contributions do not materialise, the EU action may continue outside a TEI framework.

3.3 Mainstreaming

Environmental Protection & Climate Change

Outcomes of the SEA screening
The Strategic Environmental Assessment (SEA) screening concluded that no further action was required.

Outcomes of the EIA (Environmental Impact Assessment) screening
The EIA (Environment Impact Assessment) screening classified the action as Category C (no need for further assessment).

Outcome of the CRA (Climate Risk Assessment) screening
The Climate Risk Assessment (CRA) screening concluded that this action is no or low risk (no need for further assessment).

Gender equality and empowerment of women and girls
As per the OECD Gender DAC codes identified in section 1.1, this action is labelled as G1. This implies that this action promotes women's meaningful involvement and contributes to their economic and social empowerment.
The gender digital divide affects Sub-Saharan Africa. Women are, for example, less likely to have a mobile phone than men and the use of Internet by women is lower than by men. In addition, women tend to have less market entry opportunities, less access to this job market and less decision-making spaces for policy formulation.[26]

[26] Unrealized Potential: Female Entrepreneurship and the Digital Gender Gap in Sub-Saharan Africa, United Nations Development Programme, 2023, https://www.undp.org/publications/dfs-unrealized-potential-female-entrepreneurship-and-digital-gender-gap-sub-saharan-africa?gad_source=1&gclid=EAIaIQobChMI3pTO5-eggwMVApGDBx2J3QBaEAAYASAAEgKhMPD_BwE.

This Action can contribute to reducing the barriers to success and entry into markets for women and youth owned businesses by fostering regulatory reforms, digital trade expansion and digital payments access for women and young entrepreneurs. This is particularly relevant in services sectors since services firms in Africa have a higher percentage of female top managers than manufacturing firms. And it is also particularly relevant in the case of small-scale cross border traders which tend to be women in their majority. Special focus shall be directed towards the support of female founders in the development of eCommerce platforms and digital support services, as well as the encouragement of them to network and raise investments. Equally, the Action will consider that a gender perspective in the design and implementation of digital government services is key to ensure public policy and services are accessible by all.
According to ISC2, a world leading organisation for cybersecurity professionals, women make up for a mere quarter or the global workforce in the field, while Sans Institute estimates only 9% of cybersecurity professionals in Africa are female. Hence specific target will be considered in related capacity building activities.

The action will mainstream gender at all stages, including by supporting specific activities with gender analysis and integrating sex-disaggregated data and gender-sensitive indicators to better assess the impact on gender equality.

Human Rights

The action will integrate a rights-based approach and will contribute to ensuring that rights holders, including vulnerable groups, are taken into account.
It will contribute to the development of better human digital rights regulation through improving access for citizens to government services as well as ensuring better infrastructure security and increased cyber hygiene to protect individuals and communities from related threats, in line with EU standards. The Action will strive to create platforms of continuous dialogue with civil society to address concerns related to the indirect impacts that the use of technologies might have in the development and implementation of eID frameworks and digital government services at broad.
For the cybersecurity workstream, the Action will have dedicated activities on cyber hygiene that are relevant to human rights protection.
The action will also encourage active participation of a wide range of stakeholders in economic groupings and industry clusters aimed at generating benefits at community level.
At all stages gender-responsive human rights-based approach 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) will guide the planning and implementation of the Action.

Disability

As per OECD Disability DAC codes identified in section 1.1, this action is labelled as D0. This implies that no activity is foreseen to target specific people with disabilities, but the Action will indirectly contribute to improving the inclusion of people with disabilities through improvements in their access to digital trade and employment opportunities, digital services and technologies. Digital trade and digital governance can play a major role to empower people with disabilities to get involved in remote access to services and work in Africa and international markets.

Reduction of inequalities

This action can ultimately contribute to the reduction of inequalities through strengthening the business and governance environment and consumer security to contribute to economic development and decent job creation.
Increasing innovation, business opportunities, trust and security in governance services and digital markets can ease the entry of new businesses which can give rise to reducing inequalities through more economic opportunities for other sectors of population.
A special focus will target the stimulation and engagement of disadvantaged groups or small-scale cross border traders to get prepared for the digital trade. These activities will focus on reaching out through proper channels (e.g. communication in refugee camps, through local communities, local civic organisations, etc.).

Democracy

Accelerating Gender Equality: Let's Make Digital Technology Work for All, World Bank Blogs, 2023, https://blogs.worldbank.org/africacan/accelerating-gender-equality-lets-make-digital-technology-work-all.

The development of clear and secure regulatory frameworks will be promoted with a strong emphasis on ensuring good governance and transparency in the policy and regulatory adoption. The engagement of civil society and private sector organisations in advocacy will be promoted to ensure more inclusive and transparent governance structures that reply to the needs of the private sector and consumers.

Conflict sensitivity, peace and resilience

The action will not have a core focus on peace and resilience, however in line with the development-security nexus, it is important to flag the relevance of economic sustainable growth for stabilisation and sustainable development

Disaster Risk Reduction

This action will not target or impact disaster risk reduction, however it will ensure climate impact mitigation through the strengthening of harmonised regulations (regional/ national) on Digital trade, Digital Governance and Cybersecurity complying with EU standards.
Moreover, the development of digital capacity in the public and private sector can be considered to be steps towards a better and more comprehensive use of tools to assess disaster risk reduction.

Other considerations if relevant

N.A.

3.4 Risks and Lessons Learnt

Category	**Risks**	**Likelihood (High/ Medium/ Low)**	**Impact (High/ Medium/ Low)**	**Mitigating measures**
People and Organisation	Duplication of efforts with other national and regional initiatives.	Medium	Medium	Close collaboration with the region's EU Delegations as well as the RECs, particularly in terms of countries belonging to several RECs to ensure that the action does not clash with nor duplicates ongoing efforts.
External Environment	Lack or little political will by the national governments to implement the activities encompassed in the action.	Low	High	The commitment of selected national governments will be sought ahead of the implementation of the action.
Planning	Coordination with wide range of stakeholders at both national and regional level could hinder the successful implementation of the action.	Medium	Medium	Engagement with key stakeholders will be ensured from the outset. Close collaboration between the implementation partners and the beneficiaries will be prioritised.
Planning	Complex implementation modalities involving multiple	Low	Medium	Clear roles and responsibilities will be defined and a role to coordinate the work of Team Europe members will be assigned.

	Team Europe members could result in delayed implementation and/or reduced impact on the ground.			
People and Organisation	Inadequate needs assessment results in frameworks not matching requirements.	Medium	Medium	Perform comprehensive needs assessment through surveys, interviews, focus groups, and analysis. Validate results through peer review.
Planning	Inadequate needs assessment results in frameworks not matching requirements.	Medium	Medium	Perform comprehensive needs assessment through surveys, interviews, focus groups, and analysis. Validate results through peer review.
People and Organisation	Information systems maturity prevent integration and interoperability of regional and national systems.	High	Medium	Follow once only principle when designing and adapting systems in question. Contribute to establishing regional and continental standards. Perform gap analysis and plan upgrades. Use open architectures and shared platforms.
Planning	Cybersecurity investments not seen as a priority by some member states.	Medium	High	Showcase the financial and social implications of cyber threats and the ROI of proactive cybersecurity investment.
External environment	Rapid evolution of cyber threats outpacing defense measures	High	High	Facilitate platforms of exchange on cyber threat intelligence for real-time sharing of threat information. Foster research in cyber defense mechanisms.
People and Organisation/External environment	Varied cultural perceptions on privacy and security	Medium	Medium	Organize awareness campaigns that are culturally sensitive and tailor messages to each region's unique cultural backdrop.

Lessons Learnt:

The complexity of regional programmes has shown that implementation of pilot programmes amongst pilot countries with similar levels of economic development, legal, regulatory, and technical readiness could provide the proof-of -concept for a full-scale regional implementation.

As digital development has become a mainstream domain in the development cooperation field, the EU has been implementing various regional and bilateral projects. Yet, this is the first time a comprehensive regional project in SSA including such a broad spectrum of interrelated components is designed. Ongoing projects in Africa include PRIDA, AU-EU D4D Hub, EGEE-ICT, Africa Connect, Initiative for Digital Government and Cybersecurity in the Horn of Africa, Data Governance in Africa (as of 2023), Digital Regulators Partnership (as of 2023-2024) and some other bilateral projects and technical assistance activities. As digital finance programmes in SSA are concerned, the ongoing project 'Leveraging digital finance to increase resilience of ACP countries' (2020-2024) is the only example of project also including activities in African partner countries.

Systems sustainability requires local proponents and partners, not just EU-led efforts, by building local ownership and leadership to continue functioning after external support pulls out. Capacity development aims to equip partners to manage programs independently long-term. In this context the importance of political will and regional leadership cannot be underestimated. Local governance structures and permissions are essential to initiate activities since cooperation with local authorities is key for local buy-in and sustainability of EU funded actions. Public-private and regional partnerships should be empowered via incentives and technical assistance to spur business-driven digital development aligned with public goals. These partnerships with private sector bring innovation and resources that can sustain solutions for a long term.

It is crucial to make technical competencies a core requirement in the education and training programs for government staff. This will ensure that they are well-prepared to handle the digital demands of their roles and contribute effectively to building communities for the digital future. Regional centers of expertise play a significant role in this process by sharing best practices locally and adapting global knowledge to meet the specific cultural and contextual needs of government staff,enabling them to perform their duties efficiently and effectively while being up-to-date with the latest technological advancements. It is also valuable to have South-South exchanges within regions, as they facilitate peer-to-peer learning and enable relevant staff to participate in trainee and mentorship programs in more advanced environments to learn by doing from the best.

Comprehensive consultations and discussions are crucial before initiating transformative actions, notably in the landscape of cybersecurity where mutual trust is paramount to establishing cooperation. Ongoing capacity-building initiatives and robust public-private partnerships are paramount to bridge the existing knowledge gap and offer the required technological and strategic expertise to tackle emerging cyber threats. By embracing a harmonised, region-wide approach, African countries can strengthen their collective cybersecurity posture. Continuous reflections and recalibrations based on lessons from previous and ongoing actions will ensure the project's agility and responsiveness to the dynamic cybersecurity challenges of the region.

3.5 Intervention Logic

The Action has the goal to provide comprehensive support for trade and digitalisation towards a sustainable setup of an African Single Digital Market within a robust cybersecurity environment.

In parallel, the Action will enhance cyber resilience of target regions and countries, by supporting the development of strategies, laws and regulations addressing cybersecurity, while enhancing capacity for the protection of critical infrastructure.

With regards to **eCommerce and ePayments**, it will support the different steps of digitally enabled trade Business-to-Business (B2B) and Business-to-Consumer (B2C) transactions. From ordering to delivering good and services, it will focus on expanding and rendering more inclusive, secure and trusted existing eCommerce platforms in collaboration wih national postal services. At the same time, it will support the payment of such transactions through the interconnectivity of existing payment systems, offering tailor-made solutions for low transactions traders, and facilitating fintech integration, all in line with EU standards in view of their future interoperability with EU systems.

An approach targeting certain pilot countries having eCommerce platforms with export potential, focusing on the different steps of the value chain across the whole commercial transaction (from ordering, to payment, to delivery) for a/a few specific product (s) or service (s) may be considered.

With regards to **eGovernance,** the Action will support the enabling environment for the digital transformation of public administration through the uptake of digital government services, by targeting the required legal, regulatory, organisational and technical aspects. The Action will work towards the establishment of eGovernance building blocks, including eID, e-signature, interoperability, and digital registries.

The above will be accompanied with measures to contribute to increase cybersecurity with the ultimate goal to streghthen the **Cybersecurity** ecosystem in Sub-Saharan Africa through regional cooperation in the regional clusters.

In addition, the Action will address the fragmented cross-border ECommerce, E-Payment, and EGovernance ecosystems, within identified regional clusters, coupled with regulatory and policy support at public authorities level (AUC, RECs, Member States).

Instead of developing a top-down approach, the action will consider the national and regional strategic priorities alongside the Specific Objectives to put together a bottom-up approach that will seek to address every day challenges faced by citizens in Sub-Saharan Africa.

At the inception phase, a situational analysis of the readiness of the regional cluster countries, including identifying bottlenecks for the development of cross border eCommerce, ePayments, digital government services and cyber resilience may be conducted. Then, focusing on countries that comply with defined criteria such as *i.a.* technical and infrastructure readiness, legislation, regulatory similarities, export potential within African and towards the EU, as well as political commitment to lead digital regional integration may be selected to participate in the activities of this action.

It is expected that:

IF appropriate technical assistance is deployed at national, regional and continental level all along the activities mentioned in the Action at the AUC, REC and country level and expanding frameworksa and services in the areas of eCommerce, ePayments, eGovernance and cybersecurity in possible selected countries, with similar technical and legislative levels of readiness;

IF strong political commitment is demonstrated towards deepening digital integration within a robust cybersecurity environment to address the current differences or lack of regulatory frameworks and promote harmonisation amongst countries of the same region in the areas of eCommerce, ePayments and eGovernance

THEN important stepts towards to set up of an African Digital Single Market will be made.

3.6 Logical Framework Matrix

This indicative logframe constitutes the basis for the monitoring, reporting and evaluation of the intervention.
On the basis of this logframe matrix, a more detailed logframe (or several) may be developed at contracting stage. In case baselines and targets are not available for the action, they should be informed for each indicator at signature of the contract(s) linked to this AD, or in the first progress report at the latest. New columns may be added to set intermediary targets (milestones) for the Output and Outcome indicators whenever it is relevant.

- At inception, the first progress report should include the complete logframe (e.g. including baselines/targets).
- Progress reports should provide an updated logframe with current values for each indicator.
- The final report should enclose the logframe with baseline and final values for each indicator.

The indicative logical framework matrix may evolve during the lifetime of the action depending on the different implementation modalities of this action.
The activities, the expected Outputs and related indicators, targets and baselines included in the logframe matrix may be updated during the implementation of the action, no amendment being required to the Financing Decision.

PROJECT MODALITY (3 levels of results / indicators / Source of Data / Assumptions - no activities)

Results	**Results chain (@): Main expected results (maximum 10)**	**Indicators (@): (at least one indicator per expected result)**	**Baselines (values and years)**	**Targets (values and years)**	**Sources of data**	**Assumptions**
Impact	To accelerate digital trade and e-governance at continental, regional and bilateral levels within a robust cybersecurity environment in the framework of an African single digital market.	1. Intra-African trade from its current total trade 2. Exports to countries in same continent, as a % of total exports, 2020 3. The contribution of the internet to the African economy as % of GDP 4. Exports of digital services as a % of total exports 5. Ranking of African countries according to e-government performance 6. Ranking of African countries on global cybersecurity indexes	1. 18% (2018) 2. 14,8 % (2020) 3. 5,3% (2016) 4. 26,8% (2019) 5. TBD/various 6. TBD/various	1. 40% 2. 20% 3. 7% 4. 30% 5. TBD/various 6. TBD/various	1 AfCFTA 2 OECD (Africa's Development Dynamics 2022) 3 CEA 4. OECD (idem) 5. UN E-Government Development Index (EGDI) 6. Global Cybersecurity Index	*Not applicable*

Outcome 1	Enable and increase the inclusive and secure use of eCommerce platforms for cross-border trade.	1.1 Share of SSA Africa economies with relevant digital trade legislation 1.2 Enterprises with B2B eCommerce sales to other African countries 1.3 Enterprises with B2C eCommerce sales to other African countries 1.4 % of enterprises of all sizes using eCommerce platforms for cross-border, regional, continental sales	1.1 Electronic transactions 61% (2022), Consumer protection 52% (2022), Privacy and data protection 61% (2022), Cybercrime 72% (2022) 1.2 To be defined (TBD) in a baseline study during inception 1.3 To be defined (TBD) in a baseline study during inception 1.4 To be defined (TBD) in a baseline study during inception	1.1 Increased by 15% 1.2 Increased by 15% 1.3 Increased by 15% 1.4 Increased by 15%	1.1 The UNCTAD Global Cyberlaw Tracker 1.2 AUC, AfCFTA Secretariat reports 1.3 AUC, AfCFTA Secretariat reports 1.4 AUC, AfCFTA Secretariat reports	Harmonisation of legislation progressing as planned and foreseen Stable regional economic situation and no conflict affecting trade
Outcome 2	Enable and harmonise national payment systems and improve cross-border ePayments and their interoperability.	2.1. % of enterprises conducted cross-border B2B electronic payments 2.2. % of enterprises conducted cross-border B2C electronic payments 2.3. % of small traders conducted cross-border B2B and B2C electronic payments	2.1. To be defined (TBD) in a baseline study during inception 2.2. TBD in a baseline study during inception 2.3 TBD in a baseline study during inception	2.1. Increased by 10% 2.2 Increased by 10% 2.3 Increased by 10%	2.1. Final evaluation reports, Regional studies by RECs 2.2 Final evaluation reports, Regional studies by RECs 2.3 Final evaluation reports, Regional studies by RECs	African banks and financial services providers implement e-payment services that are affordable and secure for enterprises ePayment B2B and B2C benefits are largely promoted within the AfCFTA implementation

Outcome 3	Improve the legal, organisational and technical enabling environment for eGovernance and enhance related cross-border interoperable service delivery.	3.1 Number of countries that have adopted harmonised eGovernance frameworks. 3.2 Number of developed digital government services under the EU-funded intervention (Aligned with GERF 2.12 a,b) 3.3 Number of cross-border services initiated under the EU-funded intervention	3.1 TBD in a baseline study during inception 3.2 TBD in a baseline study during inception 3.3 TBD in a baseline study during inception	3.1 TBD in a baseline study during inception 3.2 TBD in a baseline study during inception 3.3 TBD in a baseline study during inception	3.1 GERF 1.10 UN e-Government Development Index 3.2 Progress and final report for the EU-funded intervention 3.3 Progress and final report for the EU-funded intervention	Political will for regional cooperation and national-level supports harmonised frameworks and digital government services implementation
Outcome 4	Enhance the development of regionally harmonised cybersecurity frameworks and protection of critical information infrastructure.	4.1 Number of cyber incidents reported annually in countries and regionas supported under the EU-funded intervention	4.1 TBD in a baseline study during inception phase	4.1 TBD during inception phase	4.1 Project update reports, National reports from cyber coordinating Ministries, Civil society scrutiny reports, Press releases	
Output 1 **relating to Outcome 1**	1.1 Continental, Regional and National legal frameworks in cross-border digital trade are developed and/or harmonised in line with EU standards while enhancing the capacity of regulatory actors.	1.1.1 Number of improved continental legal acts in digital trade 1.1.2 Number of harmonised legal frameworks drafted	1.1.1 0 in 2024 1.1.2 To be defined (TBD) in a baseline study during inception	1.1.1 4 for 4 key areas 1.1.2 One per region	1.1.1 AUC, AfCFTA Secretariat reports 1.2.1 Progress reports, Final evaluation reports	Political commitment at the AU, AfCFTA. RECs and country levels to implement the necessary legal amendments

Output 2 **relating to Outcome 1**	1.2 African B2B and B2C eCommerce platforms are supported in their cross-border development and in ensuring trust and inclusivity.	1.2.1 Number of supported eCommerce platforms to extend cross-border 1.2.2 Cross-border eCommerce sales by enterprises as % of all enterprises undertaken sales via eCommerce 1.2.3 Number of capacity building and Technical assistance workshops for a continental mechanism of trust mark for African digital platforms 1.2.4 Number of capacity building events implemented for African competition and consumer protection authorities 1.2.5 Percentage of population using eCommerce	1.2.1 0 in 2024 1.2.2 TBD in a baseline study 1.2.3 0 in 2024 1.2.4 TBD in a baseline study during inception 1.2.5 TBD in a baseline study during inception	1.2.1 one platform per region 1.2.2 Increase by 25% 1.2.3 Two per region 1.2.4 Three annual events 1.2.5 Increased by 10%	1.2.1 RECs reports 1.2.2 RECs reports and other official statistics 1.2.3 Progress reports, Final evaluation reports 1.2.4 Progress reports, Final evaluation reports 1.2.5 Progress reports, Final evaluation reports	Political commitment at AU, AfCFTA and RECs level to implement the necessary reforms Sufficient number of existing eCommerce platforms are interested in EU support and expansion of their operation cross-border Required minimum technical capacity to develop an African digital trustmark (trust seal) mechanism
Output 3 **relating to Outcome 1**	1.3 Fintech integration and SME development within eCommerce platforms is fostered, with special consideration for women and young entrepreneurs.	1.3.1 Number of dialogue and networking events held to promote collaboration between eCommerce platforms and fintech start ups	1.3.1 0 in 2024	1.3.1 Two per region	1.3.1 Progress reports, Final evaluation reports	Continued dialogue and sharing of experiences among continental, regional, and national stakeholders

Output 4 **relating to Outcome 1**	1.4 Businesses and citizens awareness to utilise the opportunities offered by eCommerce platforms is increased.	1.4.1 Number of public and private sector workshops/meetings/events organised with support of the action by region 1.4.2 Number of awareness campaigns on opportunities of using ePayments held 1.4.3 Number of national/regional stakeholders reached out	1.4.1 zero in 2024 1.4.2 0 in 2024 1.4.3 0 in 2024	1.4.1 Two per region 1.4.2 Three per region 1.4.3 Ten per region	1.4.1 Progress reports, Reports of RECs, AUC, AfCFTA Secretariat 1.4.2 Progress reports, Final evaluation reports 1.4.3 Progress reports, Final evaluation reports	Continued dialogue and sharing of experiences among continental, regional, and national stakeholders
Output 1 **relating to Outcome 2**	2.1 Continental, Regional and National legal frameworks in cross-border digital payments are developed and/or harmonised in line with EU standards while enhancing the capacity of regulatory actors.	2.1.1. Number of improved continental legal acts in digital payments 2.1.2 Number of harmonised legal frameworks drafted	2.1.1. 0 in 2024 2.1.2 To be defined (TBD) in a baseline study during inception	2.1.1 4 for 4 key areas 2.1.2 One per region	2.1.1 AUC, AfCFTA Secretariat reports 2.1.2 Progress reports, Final evaluation reports	Political commitment at the AU, AfCFTA, RECs, country levels to implement the necessary legal amendments
Output 2 **relating to Outcome 2**	2.2 Regional payments and settlement systems to facilitate cross-border B2B and B2C payments are improved and/or extended, with special consideration for small-scale traders.	2.2.1 Number of countries supported 2.2.2 Number of cross-border B2B e-payment methods per REC	2.2.1 0 in 2024 2.2.2 TBD in a baseline study	2.2.1 Two per region 2.2.2 One per REC operational in each Member State	2.2.1 Progress reports, Final evaluation reports 2.2.2 RECs reports, UNCTAD eTrade Readiness reports	Political commitment at the RECs level Financial and technical capacities of regional payment and settlement authorities to finance and implement required actions

Output 3 **relating to Outcome 2**	2.3 Regional payment systems interconnection and interoperability with the Pan-African Payment and Settlement System (PAPSS) and future proofing for interoperability with EU system(s) is facilitated.	2.3.1 Number of countries supported 2.3.2 Number of regional payment systems interconnected with the Pan-African Payment and Settlement System 2.3.3 Number of regional payment systems that have been future-proofed for interoperaiblity with EU systems 2.3.4 Number of dialogue events held between EU and African partners on interoperability	2.3.1 0 in 2024 2.3.2 0 in 2024 2.3.3 0 in 2024 2.3.4 0 in 2024	2.3.1 Two per region 2.3.2 One per region 2.3.2 One per region 2.3.4 Two per region	2.3.1 Progress reports, Final evaluation reports 2.3.2 Progress reports, Final evaluation reports, PAPSS reports 2.3.3 Progress reports, Final evaluation reports 2.3.4 Progress reports, Final evaluation reports, RECs reports	The RECs and countries are willing to connect with the PAPSS The RECs and countries are willing to interconnect their payment systems with the EU in a future
Output 4 **relating to Outcome 2**	2.4 Businesses and citizens awareness to utilise the opportunities offered by ePayments is increased.	2.4.1 Number of public and private sector workshops/meetings/events organised with support of the action by region 2.4.2 Number of awareness campaigns on opportunities of using ePayments held 2.4.3 Number of national/regional stakeholders reached out	2.4.1 zero in 2024 42.4.2 0 in 2024 2.4.3 0 in 2024	2.4.1 Two per region 2.4.2 Three per region2.4.3 Ten per region	2.4.1 Progress reports, Reports of RECs, AUC, AfCFTA Secretariat 2.4.2 Progress reports, Final evaluation reports 2.4.3 Progress reports, Final evaluation reports	Continued dialogue and sharing of experiences among continental, regional, and national stakeholders
Output 1 **relating to Outcome 3**	3.1 Capacities of continental, regional and national actors to improve and harmonise their legal, organisational and technical frameworks for interoperable and cross-border digital government services are increased.	3.1.1 Number of countries adopting harmonised frameworks (Aligned with GERF 2.10b)	3.1.1 0 in 2024	3.1.1 TBD in inception phase	3.1.1 Progress and final report for the EU-funded intervention	Political commitment at the AU, RECs and country levels to implement the necessary legal, organisational and technical amendments

Output 2 **relating to Outcome 3**	3.2 Technical solutions and building blocks to deploy national and regional level digital government services are developed and customised.	3.2.1 Number of national and regional digital government service requirements analyses conducted (Aligned with GERF 2.12 a) 3.2.2. Number of national and regional digital government service requirements analyses conducted (Aligned with GERF 2.12 a) 3.2.3. Number of national and regional digital government services deployed (Aligned with GERF 2.12 b)	3.2.1 0 in 2024 3.2.2 0 in 2024 3.2.3 0 in 2024	3.2.1 TBD in inception phase 3.2.2 TBD in inception phase 3.2.3 TBD in inception phase	3.2.1 Progress and final report for the EU-funded intervention 3.2.2 Progress and final report for the EU-funded intervention 3.2.3 Progress and final report for the EU-funded intervention	Political will for regional cooperation and national-level support for digital government services deployment and implementation Solutions are identified for development and customisation are feasible for the challanges faced

Output 1 **relating to Outcome 4**	4.1 Capacities of competent authorities to design and implement cybersecurity norms, strategies and regulations are increased at continental, regional and national level.	4.1.1 Number of countries supported under the EU-funded intervention with updated and internationally aligned cybersecurity policies 4.1.2 % of countries supported under the EU-funded intervention adopting EU NIS Directive standards 4.1.3 Number of countries supported under the EU-funded intervention with revised legal frameworks aligning with international standards 4.1.4 Number of strategies developed and implemented at national, regional, and continental levels thanks to the EU intervention	4.1.1 0 in 2024 4.1.2 0 in 2024 4.1.3 0 in 2024 4.1.4 0 in 2024	4.1.1 TBD in inception phase 4.1.2 TBD in inception phase 4.1.3 TBD in inception phase 4.1.4 TBD in inception phase	4.1.1 Project update reports, National reports from cyber coordinating Ministries, Civil society scrutiny reports, Press releases 4.1.2 Regional Cybersecurity Audit Reports, Press releases 4.1.3 Project reports, Reports from ENISA, EUROPOL, FIRST, Trusted Introducer, Cybercrime Convention Committee (T CY) assessments 4.1.4 Project update reports, National reports from cyber coordinating Ministries, Civil society scrutiny reports, Press releases	Political willingness for policy and regulatory cooperation Cooperation across different levels of governance

Output 2 **relating to Outcome 4**	4.2 Mechanisms and operational capacities for the identification and protection of critical infrastructure and incident response are enhanced.	4.2.1 % of critical infrastructure assets identified and classified 4.2.2 Number of CSIRTs established or supported under the EU-funded intervention that are operationg effectively	4.2.1 0 in 2024 4.2.2 0 in 2024	4.2.1 TBD in inception phase 4.2.2 TBD in inception phase	4.2.1 National CERTs reports, Security Incident Management Maturity Model 3 (SIM3) Assessment Results, FIRST, Trusted Introducer 4.2.2 National CERTs reports, Security Incident Management Maturity Model 3 (SIM3) Assessment Results, FIRST, Trusted Introducer	Infrastructure development keeps pace with policy Availability of necessary technology and expertise
Output 3 **relating to Outcome 4**	4.3 Cyber hygiene and awareness of cybersecurity threats are improved through regional and international cooperation.	4.3.1 Number of public and private sector workshops/meetings/events organised under the EU-funded intervention 4.3.2 Number of cyber hygiene campaigns held under the EU-funded intervention 4.3.3 Number of national/regional stakeholders reached out	4.3.1 0 in 2024 4.3.2 0 in 2024 4.3.3 0 in 2024	4.3.1 TBD in inception phase 4.3.2 TBD in inception phase 4.3.3 TBD in inception phase	4.3.1 Project reports, Civil society scrutiny reports, Press releases 4.3.2 Project reports, Civil society scrutiny reports, Press releases 4.3.3 Project reports, Civil society scrutiny reports, Press releases	Receptive international environment for collaboration Active public participation to cyber hygiene initiatives

4 IMPLEMENTATION ARRANGEMENTS

4.1 Financing Agreement

In order to implement this action, it is envisaged to conclude a financing agreement with: ECOWAS, COMESA and SADC. It is not envisaged to conclude a financing agreement for the rest of the action, namely for the Continental, Eastern Africa and Central Africa components.

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 84 months from the date of entry into force of the financing agreements mentioned in 4.1 and from the date of adoption by the Commission of this Financing Decision for the rest of the action.

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 of the Budget Support Component

N.A.

4.4 Implementation Modalities

The Commission will ensure that the EU 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[27].

4.4.1 Direct Management (Grant)

a) Purpose of the grant(s)

The Grant will contribute to achieving part of the specific objectives foreseen in section 3 under the Continental component, in particular activities related to the coordination of the action.

b) Type of targeted applicants

Non-profit organisations

4.4.2 Direct Management (Procurement)

Procurement is envisaged for coordinating and monitoring the implementation of the Action and its geographical components, contributing to the entire action.

4.4.3 Indirect Management with an entrusted entity

A part of this action may be implemented in indirect management with entity (ies), which will be selected by the Commission's services using the following criteria: i) past experience in managing EU actions; ii) technical capacities and available expertise or operational capacity to mobilise a targeted technical expertise in the area targeted; iii) Experience in working with the private sector, academia, business organisations, CSOs; iv) previous experience in the region and level of engagement with relevant African stakeholders; and v) ability to operate at widespread country level in Africa.

The implementation by this (these) entity (ies) entails part of the objectives and outcomes foreseen in section 3

[27] www.sanctionsmap.eu. 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.

under the Continental (in particular, related to the content of the of activities), Western Africa, Central Africa, Eastern Africa, Southern Africa.

4.4.4 Changes from indirect to direct management mode (and vice versa) due to exceptional circumstances (one alternative second option)

Should the implementation through indirect management with an entrusted entity as described in section 4.4.3 reveal not possible due to circumstances outside of the Commission's control, the Commission will revert to direct management through procurement contributing in achieving all the specific objectives of the action.

Similarly, should direct management – grants as described in section 4.4.1 and direct management – procurement as described in section 4.4.2 reveal not be possible due to circumstances outside of the Commission's control, the Commission will revert to indirect management with an entity, which will be selected by the Commission's services using the following criteria: i) past experience in managing EU actions; ii) technical capacities and available expertise or operational capacity to mobilise a targeted technical expertise in the area targeted; iii) Experience in working with the private sector, academia, business organisations, CSOs; iv) previous experience in the region and level of engagement with relevant African stakeholders; and v) ability to operate at widespread country level in Africa. The implementation entails the four specific objectives of the action under continental and geographical components.

4.5. 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.

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).

4.6. Indicative Budget

Indicative Budget components	**EU contribution (amount in EUR)**
Implementation modalities – cf. section 4.4	
Continental component	**9 000 000**
Direct Management (Grant) – cf section 4.4.1	2 000 000
Direct Management (Procurement) – cf section 4.4.2	2 000 000
Indirect Management with entrusted entity (ies) – cf section 4.4.3	5 000 000
Western Africa component[28]	**22 000 000**
Indirect Management with entrusted entity (ies) – cf section 4.4.3	22 000 000
Central Africa component	**15 000 000**
Indirect Management with entrusted entity (ies) – cf section	15 000 000

[28] The Western Africa component is covered by a Financing agreement with ECOWAS for an amount of EUR 22 000 000.

4.4.3	
Eastern Africa component	**24 000 000**
Indirect Management with entrusted entity (ies) – cf section 4.4.3	24 000 000
Southern Africa component[29]	**30 000 000**
Indirect Management with entrusted entity (ies) – cf section 4.4.3	30 000 000
Evaluation – cf. section 5.2 **Audit** – cf. section 5.3	May be covered by another Decision
Contingencies	NA
Totals	**100 000 000**

4.7 Organisational Set-up and Responsibilities

Each geographical component will have a Steering Committee piloted by either the AUC, or the corresponding REC, or a country on a rotating basis, and the European Union. This Committee will be tasked with overseeing and validating the overall direction and policy of the programme's components. Depending on its configuration, the Committee may include the AfCFTA Secretariat, the Regional Business Councils, Member States relevant authorities such as Ministries of Trade, and of Information, Communication and Technology, and the corresponding REC(s). The selected contractors or implementing partners as per section 4.4 above will ensure the secretariat of the Steering Committee.

The European Commission will ensure the overall monitoring and coordination of the Action. Under the continental component, one of the implementing partners will be tasked to support such coordination and monitoring, creating synergies between the implementation of the different geographic components.

The European Commission will regularly report to the relevant Technical Consultative Groups established in the frame of the Sub-Saharan Africa Multi-Annual Indicative Programme, which involve institutional and non-institutional African stakeholders (i.e. AUC, RECs, AUDA, AfCFTA Secretariat, Business Associations, etc.).

As part of its prerogative of budget implementation and to safeguard the financial interests of the Union, the Commission may participate in the above governance structures set up for governing the implementation of the action and may sign or enter into joint declarations or statements, for the purpose of enhancing the visibility of the EU and its contribution to this action and ensuring effective coordination.

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 partner's responsibilities. To this aim, the 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 results (Outputs and direct Outcomes) as measured by corresponding indicators, using as reference the logframe matrix (for project modality) and the partner's strategy, policy or reform action plan list (for budget support).

The Commission may undertake additional project monitoring visits both through its own staff and through

[29] The Southern Africa component (EUR 30 000 000) is covered by both SADC (EUR 20 000 000) and COMESA (EUR 10 000 000) Financing agreements.

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).

Roles and responsibilities for data collection, analysis and monitoring:

Roles and responsibilities for data collection, analysis and monitoring: the implementing partner(s) will be responsible for monitoring and reporting on indicators of the logframe matrix, including the collection of baselines and data collection in the inception phase of the action.
Indicator values will be measured at regional or on a country-by-country basis depending on the nature of the activities and encompassing sex-disaggregated data where relevant.
In addition, considering the complexity of the action that covers different implementation levels it will be critical that implementing partners are able to communicate and report on the specific activities in each country (at a country-by- country level) to have a clear overview on the impact of the action at country level. While the indicator values at the logframe matrix may remain aggregated for the sake of simplification, implementing partners will need to be able to provide the disaggregation details in their regular reporting agreed mechanisms and in line with the country plans to be developed through the reporting phase.

With regard to the nature of the Action, data collection, performance monitoring and reporting will be carried out for each geographic component individually. Specific modalities for each of them (indicators, targets and assumptions) will be defined in the respective contracts/agreements and during the inception phases, in a way that will provide inputs for the performance monitoring of the Action globally.

5.2 Evaluation

Having regard to the importance and nature of the action, a mid-term and a final evaluation may be carried out for this action or its components via independent consultants contracted by the Commission.
It will be carried out for problem solving and learning purposes in particular with respect to the effectiveness of activities implemented at regional level,
approaches and implementation modalities. The final evaluation will be carried out for accountability and learning in particular with respect to the effectiveness of activities implemented at regional level, approaches and implementation modalities.
In case a final evaluation is envisaged: it will be carried out for accountability and learning purposes at various levels (including for policy revision), taking into account in particular the fact that all regions may not advance at the same rhythm and that a key factor of success is the involvement of the different stakeholders.
The Commission shall inform the implementing partner at least 1 month in advance of the dates envisaged for the evaluation missions. The implementing partner 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 may be shared with the partners and other key stakeholders following the best practice of evaluation dissemination. The implementing partner and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, apply the necessary adjustments.

The evaluation will be gender and human rights sensitive, assess gender equality and human rights results and implementation of rights-based approach working principles (participation, non-discrimination, accountability and transparency).

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

5.3 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

The 2021-2027 programming cycle will adopt a new approach to pooling, programming and deploying

strategic communication and public diplomacy resources.

In line with the 2022 "Communicating and Raising EU Visibility: Guidance for External Actions", it will remain a contractual obligation for all entities implementing EU-funded external actions 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. This obligation will continue to apply equally, regardless of whether the actions concerned are implemented by the Commission, partner countries, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU member states.

However, action documents for specific sector programmes are in principle no longer required to include a provision for communication and visibility actions promoting the programmes concerned. These resources will instead be consolidated in Cooperation Facilities established by support measure action documents, allowing Delegations to plan and execute multiannual strategic communication and public diplomacy actions with sufficient critical mass to be effective on a national scale.

Appendix 1 REPORTING IN OPSYS

A Primary Intervention (project/programme) is a coherent set of activities and results structured in a logical framework aiming at delivering development change or progress. Identifying the level of the primary intervention will allow for:

Articulating Actions or Contracts according to an expected chain of results and therefore allowing them to ensure efficient monitoring and reporting of performance;

Differentiating these Actions or Contracts from those that do not produce direct reportable development results, defined as support entities (i.e. audits, evaluations);

Having a complete and exhaustive mapping of all results-bearing Actions and Contracts.

Primary Interventions are identified during the design of each action by the responsible service (Delegation or Headquarters operational Unit).

The level of the Primary Intervention chosen can be modified (directly in OPSYS) and the modification does not constitute an amendment of the action document.

The intervention level for the present Action identifies as (tick one of the 4 following options);

Action level (i.e. Budget Support, blending)		
☒	Single action	Present action: all contracts in the present action
Group of actions level (i.e. top-up cases, different phases of a single programme)		
☐	Group of actions	Actions reference (CRIS#/OPSYS#):
Contract level		
☐	Single Contract 1	
☐	Single Contract 2	
	(…)	
Group of contracts level (i.e. series of programme estimates, cases in which an Action includes for example four contracts and two of them, a technical assistance contract and a contribution agreement, aim at the same objectives and complement each other)		
☐	Group of contracts 1	