Draft Annex I to the Multi Partner Contribution Agreement

CRIS No. FED/2021/425-948

Description of the Action

D4D Collaboration for the Horn of Africa Initiative on Digital Government and Cybersecurity

Project Details

Project Title:	**D4D Collaboration for the Horn of Africa Initiative on Digital Government and Cybersecurity**
CRIS No.:	
Country:	A selected number of countries of the Horn of Africa Region (Republic of Djibouti, Federal Democratic Republic of Ethiopia, Republic of Kenya, State of Eritrea, Republic of Somalia, Republic of Sudan); To be selected in the inception phase.
Total budget:	11.037.351 EUR
European Commission financial contribution:	10 Mio. EUR
BMZ financial contribution:	1.037.351 EUR
Name of the Organisation:	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Name of Partner:	Expertise France (EF)
Name of Partner:	International and Ibero-American Foundation for Administration and Public Policies (FIIAPP)
Implementing partner(s):	International Telecommunication Unit (ITU) Digital Impact Alliance (DIAL) Estonian Centre for International Development (EstDev)
Starting date:	01.01.2022 The implementation of the activities under this Action may only start after the commissioning by BMZ.
End date:	29.02.2025
Project Duration:	38 months

Table of Contents

List of Abbreviations

AfDB	African Development Bank
API	Application Programming Interface
ATU	African Telecommunications Union
BMZ	German Federal Ministry for Economic Cooperation and Development
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection.
CSIRT	Computer Security Incidents Response Teams
CSO	Civil Society Organisations
D4D	Digital4Development
DIAL	Digital Impact Alliance
DSM	Digital Single Market
DTC	Digital Transformation Centre
EAC	East African Community
EC	European Commission
EF	Expertise France
eGA	Estonia's e-Governance Academy
EU	European Union
EUD	European Union Delegation
EUD	Local EU Delegations
FIIAPP	International and Ibero-American Foundation for Administration and Public Policies
GDP	Gross Domestic Product
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
HoA	Horn of Africa
HoAI	Horn of Africa Initiative

ICT	Information and Communication Technology
IGAD	Intergovernmental Authority on Development
INTPA	International Partnerships (DG INTPA of the European Commission)
IoT	Internet of Things
ITU	International Telecommunication Union
M&E	Monitoring and Evaluation
MFA	Ministry of Foreign Affairs
MOOC	Massive Open Online Course
MPCA	Multi-Partner Contribution Agreement
MSO	Member States Organisations
OSC	Operational Steering Committee
PCP	Project Contact Point
PMU	Project Management Unit
PPP	Public Private Partnership
RTF	Regional Technical Forum
SDG	Sustainable Development Goal
ToR	Terms of Reference
UN	United Nations
WB	World Bank

1 Executive Summary

This Multi Donor Action aims to support the member states of the Horn of Africa (HoA) region to enhance their public sector service delivery through improved and secure digital delivery channels.

The Horn of Africa Initiative (HoAI) launched in October 2019 by the governments of Djibouti, Somalia, Kenya, Ethiopia, and Eritrea to identify and harmonise regional approaches that address common challenges in the region. The present six member states of the Initiative (including Sudan as newest member since May 2021) have set ambitious goals for a coordinated regional approach on issues ranging from regional connectivity and infrastructure, economic integration and employment promotion, to resilience building and human capacity development.

The adoption of digital technologies, especially those that enable digital public service delivery, have been identified as bearing strong development potential and is a strategic priority for the HoAI. The Action therefore aims to support the HoAI member states in undertaking the first necessary strategic, institutional, regulatory, and human capacities needed to establish digital government services with a potential for regional harmonization. To be able to support secure digital services, the Action also focusses on strengthening an efficient, effective and sustainable cybersecurity in the region. It complements national related programmes and regional intitaives, notably those supported by other development partners supporting HoAI.

The Action contributes primarily to the progressive achievement of the following SDGs:

- SDG 8: Promote inclusive and sustainable economic growth, employment, and decent work for all;
- SDG 9: Build resilient infrastructure, in particular through investments in information and communication technology;
- SDG 16: Promote peaceful and inclusive societies for sustainable development, especially to develop effective, accountable, and transparent institutions at all levels.

The **overall objective** of the Action is to support member states of the Horn of Africa region to effectively apply digital technologies towards an efficient, people-centred and harmonised digital public service delivery. The **specific objectives** of the Action are to support selected Horn of Africa countries to enhance their digital service delivery through implementing digital government services and to develop and improve national and regional cybersecurity in the HoA region.

This Multi Donor Action is jointly co-financed by the European Union and the Federal Ministry for Economic Cooperation and Development (BMZ) and implemented by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Expertise France (EF) and International and Ibero-American Foundation for Administration and Public Policies (FIIAPP).

2 Context

2.1 Background

The HoA region in East Africa— including Djibouti, Eritrea, Ethiopia, Kenya, Somalia, and Sudan—is a region of contrasts when it comes to social and economic development. In terms of economic development, the combined Gross Domestic Product (GDP) of the region is around USD 244.5 billion and is dominated by the two larger countries, Ethiopia, and Kenya, which make up around 72.5% of the region's population and 84% of its GDP. For social development, there are also numerous internal and external challenges that undermine progress towards national targets and the SDGs including armed conflict, migration, refugee movements, border skirmishes, organised crime, and high unemployment.

Considering these challenges and differences, the countries that make up the region see an opportunity to focus on regional collaboration to improve their economic development, internal security, stability, and trade, as well as geo-strategic position in Africa. To this end, the six countries in the region formed the Horn of Africa Initiative in 2019 to coordinate their collective investments. HoAI governance structure is light, composed of a rotating Chair (a Minister of Finance) who is supported by a temporary Secretariat. These arrangements are not subject to legal agreements but based on understanding reached between the six countries and three multilateral partners (AfDB, EU and World Bank).

The HoAI aims specifically to promote economic growth in the HoA region by furthering regional economic cooperation in important areas like trade, economic integration, connectivity, and regional infrastructure, as well as providing a framework for dialogue and collaboration. In particular, the HoAI Secretariat brings together the combined resources of these six countries and multilateral partners to invest in four pillars that will enhance regional cooperation. The emphasis of the pillars lies on increasing the efficiency of investments throughout the actions and is in line with the UN 2030 Agenda, the Addis Ababa Action Agenda on Financing for Development, and other global and regional conventions.

The four pillars of the HoAI agenda are as follows:

1. Regional connectivity, to form an interconnected HoA infrastructure that promotes transport, energy and digital connectivity;
2. trade and economic integration, to boost growth and jobs;
3. resilience, to improve the region's capacity to withstand climatic and other shocks and to promote peace and security;
4. human capital development, notably to boost skills for future employment.

This action supports Pillar 1 of the HoAI – regional connectivity to support digital trade, e-government, and cybersecurity – by contributing to the dialogue and coordination among countries. This action is aligned with the BMZ digital strategy[1] to achieve the global sustainability targets for Agenda 2030 – specifically Pillar 4 “Good Governance and Human Rights”.

2.2 Problem Analysis

The priorities in Pillar 1 *Regional Infrastructure Networks* focus specifically on the Single Digital Market and its core components of Digital Infrastructure, Data Market, and Data Services Market: E-Government and Cybersecurity.[2] In this regard, six countries have reaffirmed their commitment to leveraging frontier technologies, establishing robust digital infrastructure, and addressing the existent digital divide, even as progress towards these goals remains unequally distributed throughout the region.

The momentum for change in the HoA is consistent with demand for national digital transformation and regional integration across Africa. For example, ten countries profiled in the DIAL Listening Study[3] (including Kenya as an HoA country) have shown considerable progress on many measured indicators of digital government over the last 20 years. As a result of the focus on regional connectivity infrastructure, national priorities for e-government and cybersecurity in the HoA countries are expected to converge to some extent because of this action, while also contributing to regional development and integration between neighbours.

The HoAI promises to help governments remove barriers at the regional level and connect global investments in infrastructure and technology to national and regional priorities. This will enable those governments to expand connectivity, capacity, and service delivery for their citizens while also creating a single data market that grows the digital economy across the region.

With improvements in connectivity, the digital environment also becomes more vulnerable to cyber-attacks, thus cybersecurity will also be a main focus of this effort in order to help secure these digital services as well as ensure access and equity for citizens and private business alike.

2.2.1 E-Government

E-government services support digital transactions and have the potential to transform the way governments, people, businesses, and civil society interact in all aspects of life. As the UN Data Revolution[4] report puts it, “too many countries still have poor data, data arrives too late

[1] https://toolkit-digitalisierung.de/en/digital-strategy/
[2] https://hoainitiative.org/wp-content/uploads/2021/03/HoAI-Project-Profiles.pdf
[3] https://digitalimpactalliance.org/unlocking-the-digital-economy-in-africa-announcing-dials-new-listening-study-with-smart-africa/
[4] https://www.undatarevolution.org/report/

and too many issues are still barely covered by existing data." To overcome this challenge and gain a contextual understanding of issues, governments need to make access to data more pervasive and granular by implementing a coordinated approach across sectors involving regular data collection, publishing and encouraging the use of open public data, and delivering services using open APIs (Application Programming Interface).

The launch of digital services goes farther than reducing unnecessary paperwork and increasing administrative efficiency. Secure, standardized e-identities – used by citizens to access public services, and by businesses to electronically process proposals contracts and tenders – will encourage inclusive economic growth and collaborative business ecosystems and will foster regional and cross-regional innovation. While more than half of Africa's citizens have some form of digital ID, the continent is still lagging in adopting e-governance policies which enable its adoption (DIAL, 2020)[5]. Another cross-cutting problem is the lack of access to the internet; the World Bank estimates that only 29% of the population in Sub-Saharan Africa has access to the internet.[6] When looking at the Horn of Africa, that number decreases to an average of 25.4% between the six countries in the HoA region.[7] Citizen-oriented e-services by the governments are also being affected by the technological constraints imposed on civil servants, sometimes making them inefficient, inadequate, user-unfriendly, and overpriced.

Despite these challenges there are several positive trends. These include an increase in affordable mobile phones across the continent, a decrease in the cost of mobile subscriptions, increased cellular coverage, and the growth of e-commerce platforms. In the HoA region specifically, all countries have made different levels of progress in terms of e-government, with Kenya ranking quite high but others, like Djibouti and Sudan, continuing to rank quite low. In January 2019, the EU published the report, *Guidelines and Roadmap for full deployment of e-governance systems in Africa*[8]*,* a study by the Estonia e-Governance Academy. The report provides a classification system that groups countries according to specific cooperation needs relevant for the specific country context and in line with the state of digital readiness. The report groups the status of e-government according to three different "groups", which have been identified below.

Group	Description	HoA Country
1	The first group of countries have implemented various digital government services, have an organizational structure and at least basic regulation, and in most cases, some form of digital ID and interoperability. Online services are generally accessible and well presented. These countries have preconditions for continued development and can act as regional examples and leaders.	Kenya

[5] https://digitalimpactalliance.org/unlocking-the-digital-economy-in-africa-announcing-dials-new-listening-study-with-smart-africa/

[6] https://databank.worldbank.org/reports.aspx?source=2&series=IT.NET.USER.ZS&country=

[7] *Ibid.*

[8] *Guidelines and Roadmap for full deployment of e-governance systems in Africa*

2	The second group has limited progress, and it is likely that more upstream support may be needed for this group (like awareness-raising, regulatory adjustment, or technical support). Projects here should be regional or at least involve more than one country.	Ethiopia Sudan Djibouti
3	The third group has low levels of development, unrest or extreme poverty that are lagging in many respects. Even if e-governance can be useful for such countries and may allow them to leap-frog to faster development, there could be issues with finding adequate national capacity for knowledge transfer and sustainability of reforms.	Eritrea Somalia

2.2.2 Cybersecurity

Cybersecurity Context for Africa

According to the Africa Cybersecurity Report 2018, cybercrimes cost African economies USD 3.5 billion in 2017; in 2018, annual losses to cybercrimes were estimated for Kenya at USD 210 million. Sudan has faced a growing pace of cyberattacks, from 5,612 attacks in 2015 to 135,250 attacks in 2017. Addressing cybersecurity in the region not only will help to level the playing field for the region's digital economy but will improve its resilience and reduce vulnerability.

It is not easy to quantify the cybersecurity risks. Globally, from 2019–2023, approximately $5.2 trillion[9] in global value has been or will be at risk from cyberattacks. More than 10.5 million records are lost or stolen every month; 438,000 every hour, and a single large-scale attack can trigger $53 billion in economic losses. Amongst developing countries, Africa has been among the fastest-growing regions in terms of cybercrime activities, with the World Economic Forum declaring cybercrime as one of the greatest threats of 2019 in Africa.

These cyberattacks often have a disruptive impact on regional e-commerce and e-health services, as well as on critical infrastructure like power grids, financial and customs systems, and digital identity systems that rely on data and digital services. As more African countries increase access to broadband connectivity, their citizens and businesses are becoming more interconnected and at the same time more vulnerable to cyber-attacks. Only 20% of African states, however, currently have the basic legal frameworks in place for countering cybercrime, which will only rise as Africa's e-commerce industry expects to reach USD 75 billion by 2025. In terms of human resources, it is estimated that Africa already has a shortage of 100,000 proficient cybersecurity personnel.

Within the HoA region itself, there are huge contrasts in terms of infrastructure: Djibouti is served by eight major international submarine cables; Kenya is served by four; Somalia has just one cable connection, and Eritrea remains the last remaining coastal African country with

[9] https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview

no undersea cables (landlocked Ethiopia is reliant on connectivity through Djibouti and Sudan). Governments in the HoA region also face common challenges to improving cybersecurity, including: lack of technical expertise; lack of a designated national authority or legal framework; insufficient public and private partnerships; weak regional and international cooperation; lack of general awareness and strategy; and limited operational Computer Security Incidents Response Teams (CSIRT) capacity.

2.3 Relevance of the Action

The Action will be implemented by GIZ, EF and FIIAPP as partners to the European Commission, together with the implementing partners of the GovStack Initiative[10] (with the grantees Estonia, International Telecommunication Union (ITU) and the Digital Impact Alliance (DIAL)) all organisations will support the HoA Countries by working to implement and scale new efforts on digital government and cybersecurity, respectively, in support of Pillar One of the HoAI. The overarching goal of this support is to provide strategic advice and activities which enable any government agency or department, particularly those in low-resource settings, to build new government digital services without having to design, test, and operate the underlying systems and infrastructure. These goals have been brought together under the GovStack and Cybersecurity Approach, in support of the HoAI, enumerated below.

The relevance and the significant demand for strengthening digital government and cybersecurity in the HoA region has been validated in two "GovStack and Cybersecurity Initiative" virtual workshops held in March and July 2021. Over 100 participants – including representatives of HoA countries Djibouti, Eritrea, Ethiopia, Kenya, Somalia, and Sudan – alongside technical experts, partner organisations like Smart Africa, the World Bank, the EU and private sector representatives discussed the status of digital investments and initiatives in the different countries.

During these two workshops, the HoA country officials described their respective challenges and visions. The key elements raised included the following:

(i) Importance of a multi-stakeholder's governance/cooperation to build flexible, reliable, and inclusive e-services that bring together various stakeholders;
(ii) Strong need for capacity building in the area of e-government and cybersecurity in order to build reliable governmental services;
(iii) Interest in the development of interoperable platforms that link systems in the region;
(iv) Ambition of several countries to deploy electronic payment and digital national identity;
(v) Importance of legal frameworks as data protection remains challenging both from conceptual and operational point of views; and

[10] Founding partners of GovStack are Germany (BMZ and implementing partner GIZ), Estonia, ITU and DIAL.

(vi) Ensuring the secure exchange of data at governmental level, which is critical and will require sustainable cybersecurity strategies.

Regarding e-government, this workshop highlighted that countries varied in how far along they were in terms of e-government development. Some of the findings have been summarised below, in accordance with the eGA taxonomy summarized in section 2.2.

Levels	Characteristics	Countries	Possible Focus
1	- Have a strategy/roadmap - Several government services are already digitized - Existing governance mechanism - Strong local providers ecosystem	Kenya	✓ The GovStack: Technical requirements for interoperability, security, and information exchange ✓ Quick-wins services ✓ Sectoral digital services
2	- Have a strategy/roadmap - A lead-agency is identified - Limited government services digitized	Ethiopia Sudan Djibouti	✓ Projectised roadmap ✓ Citizen-centric design for high priority projects/services ✓ Capacity development ✓ Quick wins ✓ Partial GovStack implementation (focusing on high-priority Building Blocks)
3	- No strategy/roadmap - No clear lead-agency - No/very limited government services - Weak/limited local providers ecosystem	Somalia Eritrea	✓ Awareness raising ✓ Capacity development ✓ Strategy/Roadmap ✓ Governance support ✓ High-impact digital services / Quick wins ✓ Digital Literacy, adoption campaigns ✓ Partial GovStack implementation (focusing on high-priority Building Blocks)

To address these gaps, the Action will support governments seeking to deepen and implement their overall digital transformation strategies by facilitating the development and scaling up of digital services that are cashless, paperless, presence-less, frictionless, personalized and consent-based. This will accelerate delivery of digital government processes, as well as provide guidance and support to ensure that governments' transformation happens in a sustainable and climate-friendly manner towards a digital and green economy.

Regarding cybersecurity, the following table illustrates the situation across the region and details key areas of prioritized support, which were discussed with the Horn of Africa national representative during the workshop.

	CYBERSECURITY STRATEGY AND ACTION PLAN	C-SIRT AND RELATED SPECIALIZED AGENCY	PROTECTION OF CRITICAL INFRASTRUCTURES	PROTECTION OF PERSONAL DATA	DIGITAL FORENSICS LAB

	Definition of a national strategy and clear objectives	*Operational center and specific implementing agency*	*Element mentioned in the strategy / action plan*	*Element mentioned in the strategy / action plan*	*Existing capacity*
Djibouti	X.	X	X	X	X
Eritrea	X	X	X	X	X
Ethiopia	□	□	X	X	X
Kenya	□	□	□	□	□
Somalia	□	□	□	□	□
Sudan	X	□	X	□	□

To address these gaps and help operationalise and implement strategies, a comprehensive and consistent response to cybersecurity capacity is required across the HoA region. Pooling resources to support such efforts is not only cost-effective for governments, but also efficient, as an integrated data market is only as protected as its weakest link.

The proposed cybersecurity approach will be defined in the inception phase related to the prioritization of support and align the countries' cybersecurity strategy with EU's cybersecurity strategy by encouraging countries to comply with international standards.

2.3.1 Relevant Policy Frameworks

African Policy Framework

AU Digital Transformation Strategy: The actions to support digital infrastructure development and cybersecurity in this action are also in line with the African Union's Digital Transformation Strategy for Africa (2020-2030)[11]. This strategy builds on existing initiatives and frameworks to support the development of a Digital Single Market (DSM) for Africa, as part of the integration priorities of the continent. The vision underlying this strategy is the aspiration for an integrated and inclusive digital society and economy in Africa that improves the quality of life of Africa's citizens.

[11] https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

AU Malabo Convention: The African Union developed in 2014 a Convention on cybersecurity and data protection, known as the Malabo Convention[12]. Several articles of the Malabo Convention focus on the security of electronic transactions (article 7); the processing of personal data (article 13); the protection of critical infrastructures (article 25). The 32nd article of the Convention specifically mentions the necessity to take measures at the level of the African Union to promote cybersecurity and combat cybercrime. It specifically evokes the need to (i) Promote the adoption of measures strengthening cyber security; (ii) Work out methods to analyse cyber security needs; (iii) Advise African governments on how to promote cyber security; (iv) Formulate and promote the adoption of harmonized codes of conduct for the use of public officials in the area of cyber security.

Digital Economy Blueprint: This action is also aligned with the Digital Economy Blueprint[13] that was adopted in 2019 by the Government of Kenya. Pioneered by Kenya but for all of Africa, the Blueprint takes into account the increasing importance of the digital economy. It aims to improve not only Kenya's efforts towards national digital transformation, but all of Africa's ability to to harness the economic growth of digitalisation to promote larger efforts towards diversification and transformation. It identifies five pillars that are key to steering national digital transformation and building a digital economy: Digital Government, Digital Business, Infrastructure, Innovation-Driven Entrepreneurship, and Digital Skills and Values. This action addresses primarily the Digital Government and Infrastructure Pillars of the Digital Economy Blueprint, as well as the cross-cutting issue of data security.

Smart Africa Manifesto: Kenya adopted the Smart Africa Manifesto[14] document alongside six other African countries, the overall objective of which is to harmonise the policies of the signatories. Of relevance to this action, the 5th principle of the Smart Africa Manifesto is to highlight the need to leverage ICT in order to promote sustainable development, most notably by embracing suitable innovations in the fields of cybersecurity, cloud computing, mobility, and shared infrastructures and services.

EU Policy Framework

EU Cooperation: The EU is highly involved in discussions on how to use[15] digital technologies to build inclusive digital economies and societies. Through its external cooperation, the EU aims to be a “trend-setter” in the global debate on how to use digital technology for sustainable and inclusive development, especially in regard to its human-centred approach to digitalisation and a green digital transformation, as well its pioneering efforts in digital policy-making, technology development, and data governance.

---

[12] 29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)
[13] https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf
[14] https://smartafrica.org/who-we-are/
[15] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

EC D4D Approach: The European Commission (EC) articulated its Digital4Development (D4D) approach[16] in 2017, which – in line with the new European Consensus on Development[17] – celebrated the potential of digital technologies and services as powerful enablers for sustainable inclusive development and growth in Africa and beyond. This action is therefore in line with the D4D approach that seeks to maximise the uptake of digitalisation as driver for social and economic growth, as well as the achievement of the SDGs in partner countries.

EU Cybersecurity Strategy:[18] One lead to follow in helping HoA government is the 2020 EU Cybersecurity Strategy[19], which aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies. The strategy focuses on three areas of action:

(i) Resilience, technological sovereignty and leadership
(ii) Operational capacity to prevent, deter and respond
(iii) Cooperation to advance a global and open cyber space

German Digital Development Policy Framework

Digital Strategy of the Federal Ministry of Economic Cooperation and Development[20]: New digital technologies play a key role to achieve the global objectives for sustainable development. As a result, Germany believes that digitalisation in developing countries can offer particular potential and opportunities in relation to five key areas: 1) Work, 2) Local Innovation, 3) Equal opportunities, 4) Good governance and human rights and 5) Data for development. In the digital strategy "digitalisation for development", the BMZ laid out specific objectives for digitalisation in German development policy.

Spanish Digital Development Policy Framework

Spain has presented its Digital Strategy 2025, which includes nearly 50 measures over the next five years to drive the country's digital transformation process, in line with the European Union's digital strategy, through public-private collaboration and with the participation of all the country's economic and social agents.
FIIAPP is aligned with Digital Spain 2025 in terms of economic growth, reducing inequality, increasing productivity, and taking advantage of all the opportunities offered by new technologies, with respect for constitutional and European values, and the protection of individual and

[16] https://ec.europa.eu/digital-single-market/en/blogposts/digital4development-new-approach-eus-development-tool-kit
[17] https://ec.europa.eu/international-partnerships/european-consensus-development_en
[18] Joint Communication to the European Parliament and the council "The EU's cybersecurity strategy for the digital decade", Brussels, 16.12.2020 JOIN(2020) https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[19] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
[20] https://toolkit-digitalisierung.de/app/uploads/2021/07/BMZ-Strategy-Digital-Technologies-for-Development-1.pdf

collective rights. Digitalisation plays an important role in all sectors in which FIIAPP is active. This includes health, education, agriculture and food security, basic infrastructure, water and sanitation, governance, social protection, financial services, and others. Our vision can be summarised in two aspects: it is "digital for inclusive societies" and "digital for inclusive and sustainable economic growth".

3 Design of the Action

3.1 Objectives and Outputs

The **overall objective** of the Action is to support member states of the Horn of Africa region to effectively apply digital technologies towards an efficient, people-centred and harmonised digital public service delivery.

This overall objective will be pursued through two complementary components adhering to two specific objectives, to be fulfilled implemented by GIZ/FIIAPP (Specific Objective 1) and Expertise France (Specific Objective 2) respectively.

Specific Objective 1: Selected Horn of Africa countries enhanced their service delivery through implementing digital government services.

Specific Objective 2: HoA countries develop and improve national and regional cybersecurity.

Specific Objective 1 – Digital Public Service Delivery through e-Government Building Blocks (implemented by GIZ and FIIAPP)

To achieve the Specific Objective 1, the Action has the following outputs:

Output 1	The strategic, technical, and regulatory prerequisites to introduce government e-services in selected countries of the Horn of Africa Region are evaluated (Implemented by GIZ)
Short Description	Output 1 aims at evaluating the necessary strategic, technical, and regulatory framework conditions to enable the implementation of digital government services, based on common digital government building blocks in selected member states of the HoA Initiative. This Output focusses on identifying public services, with a potential for regional harmonisation, that can be digitalised with Ministries and other Public Sector authorities in selected member states of the HoA region. These could for example include services related to international trade, cross-border communication, or the exchange of data.

Output 2	E-government building blocks are technically adapted for the use in selected member states of the Horn of Africa Region (Implemented by GIZ)
Short Description	Output 2 focusses on the development of generically, but nationally localized software components or e-government building blocks (e.g. digital registries, identity and authentication, e-payments, etc.) that in combination provide key functionalities to facilitate generic workflows and the development of digital government services common across multiple sectors. These locally specified and adapted building blocks serve as basis for the development of concrete national digital government services, with a potential for regional harmonization. Selected government agencies will be supported to test the e-government building blocks on a freely accessible platform (GovStack), and to develop national high-priority digital government services.

Output 3	The technical and methodological competences of civil servants in the Horn of Africa Region to implement the e-government building blocks have been strengthened (Implemented by GIZ & FIIAPP)
Short Description	Output 3 aims at equipping civil servants from different public authorities in the HoA Region, participating in the piloting and introduction of new e-government services, with the adequate technical and methodological skills to introduce digital government services. To this extent, capacity building modules will be implemented, in fields such as change management processes (3 training programs implemented by FIIAPP), inter-institutional exchange or on technical issues with regards to the e-government building blocks (3 training programs implemented by GIZ). To foster the cross-national dialogue and exchanges between different public sector organizations, technical Communities of Practice will provide a framework for mutual learning and discussion (implemented by GIZ:).

Specific Objective 2 – Cybersecurity (implemented by EF)

To achieve the Specific Objective 2, the Action has the following outputs:

Output 1	Strategic and institutional cybersecurity frameworks are reinforced and converging towards shared regional standards
Short Description	This output will define a common strategic and institutional framework in regional cooperation. Readiness cybersecurity assessments will be conducted at national levels in order to carry a comprehensive review of the cybersecurity policies, procedures, and practices with the aim to identify critical cybersecurity gaps that will lead to the definition of emerging priorities and recommendations to address these gaps and priorities. These strategies should be harmonised in parallel, converging towards common regional cybersecurity guidelines which will be achieved through the setting up and supporting the workings of a Regional Technical Committee (RTC) involving the main stakeholders.

Output 2	Cybersecurity awareness and capacities of government officials and IT professionals as well as the general public are strengthened.
Short Description	In order to strengthen cybersecurity awareness and empowerment government officials and IT professionals as well as the general public to secure the internet, awareness raising activities will be conducted that will include high-level dialogues, workshops on digital hygiene and the development of awareness campaigns and communication materials. In addition, on-site and on-line trainings as well as e-learning materials and activities will be developed and tailored to IT professionals.

Output 3	Operational capacities to handle cybersecurity incidents are enhanced
Short Description	This output will support the establishment and equipment of CSIRTs as well as the strengthening of their procedures necessary to secure and maintain the services and infrastructures that are vital to national security and economic growth. In addition, the project component will facilitate information sharing and technology exchange between countries of the region. This will be done through the set-up of a platform which will provide the cybersecurity experts with advice and assistance in the daily management of CSIRTs. The possibility of introducing common operational tools will be explored at inception and – if deemed feasible – implemented in a pilot phase.

3.2 Intervention logic / Method of Implementation

Govstack approach

The digital government component (*Specific objective 1: Digital Public Service Delivery through e-Government Building Blocks*) will be implemented by GIZ and FIIAPP. It is based on the GovStack Initiative, initiated by GIZ, Estonia, ITU and DIAL, to accelerate national digital transformation and digitalization of government services for the achievement of Sustainable Development Goals (SDGs) by 2030. The Initiative aims to build a shared "Digital Government Services Infrastructure" or a "Government Technology Stack" comprising reusable common foundational digital capabilities and services, called Building Blocks.

GovStack building blocks are reusable, interoperable, reconfigurable, generically defined software components that, once combined, provide critical functionalities to facilitate common workflows across sectors. They include software components such as security, registration, authentication, digital payments, digital identity, shared data repositories, content management, and data collection. Governments can deploy GovStack elements across any government agency, department, and across different sectors to build new government or market-driven digital services without redesigning, testing, and operating the underlying systems and infrastructure themselves.

The goal of the first component of the present Action is therefore to use the GovStack approach to support selected HoA countries to enhance their digital service delivery through implementing digital government services.

The intervention logic for the component implemented by GIZ and FIIAPP is as follows:

- Selection of public services with a potential for digitalization and with relevance for a potential regional harmonization, identification of technical, organisational, and regulatory requirements (Output 1, implemented by GIZ)
- Specification and local adaptation of the e-government building blocks to the identified national requirements (Output 2, implemented by GIZ)
- Development of technical skills and change-management capacities within the participating public sector institutions (Output 3) (jointly implemented by GIZ and FIIAPP)

In close coordination with national authorities, the project will include a cross-country multi-stakeholder engagement process to evaluate the technical and regularity prerequisites for the introduction of government e-services in selected member states of the HoA Region. This collaborative process will ensure that the selected public sector authorities and respective public services have a relevance also for a regional harmonisation with other HoA member states, that do not participate in this first digital service delivery process.

Upon selecting five government services to be digitalised, implementation roadmaps will be elaborated with the national authorities involved in the service delivery process for the selected service. This process will commence with a definition of technical requirements by the participating public authorities, as well as a collaborative planning of the piloting phase. The implementation roadmaps will also entail a planning for the roll-out phase and potential regional harmonization, that will be steadily enriched with insights from the pilot to serve as a document containing next steps and recommendations at the end of the Action.

Based on the requirement analysis with the participating public authorities in the selected HoA member states, the existing GovStack e-government building blocks are adapted to the local

needs, bearing in mind the local regulatory environment, legacy infrastructure and organisational and contextual elements identified in the requirement analysis. Upon local adaptation, the e-government building blocks will be freely accessible on a regional or national service platform, to serve as basis for piloting concrete public digital services based on the e-government building blocks.

The Action will also provide the necessary change management support and conduct relevant capacity development activities for the respective public authorities involved in the GovStack deployment process.

The founding partners of the GovStack Initiative (ITU, Estonia and DIAL) will provide technical support to the component. Each partner represents a different part of the digital ecosystem and will support the action with special competency, specific activities will be defined in the inception phase.

ITU will support the technical leadership of the component. That includes the overall management of the technical parts, including engagement with experts, advisory to experts and guiding the technical work. Estonia will mainly support with strategic advocacy and events, for example with overall PR and awareness-raising in various forums relevant to the component. DIAL will support the overall strategy of the component. Together, these partners will ensure alignment with agreed-upon country and prospective regional objectives.

Cybersecurity approach

The cybersecurity component (*Specific objective 2: Horn of Africa countries develop and improve national and regional cybersecurity, promoting a single regional market in HoA countries*) will be implemented by EF. It has the following intervention logic:

The efficient, effective and sustainable strengthening of cybersecurity in the region relies on the adoption of the following regional outputs:

1. Robust cybersecurity frameworks (strategic and institutional) at a national level, is required to create the appropriate institutions that can shape national developments and enhance regional cooperation through shared standards.
2. Awareness and capacity building on cybersecurity, which is required to create and maintain trust in the regions digital infrastructure and ensure adequate integration and political backing for the action.
3. Technical tooling and support are required to sustain these efforts.

Activities in these three areas are interrelated in order to reinforce their relative impact. Thus, policy dialogues would be combined with targeted technical cooperation, capacity building measures, and public outreach in order to create/deepen and extend relations and networks.

Expertise France has developed a methodology that addresses the entire spectrum of cyberspace security through the following actions:

- Assessment of countries' level of cybersecurity preparedness and identification of their needs;
- Establishment of strategic, institutional, and legal frameworks, starting with the development of national policies and strategies in terms of cybersecurity and protection of critical infrastructure;

- Raising user-awareness on computer hygiene and decision-makers on their responsibilities in securing the cyberspace;
- Improvement of security incident management capabilities, by supporting the creation of computer security incident response teams (CSIRTs) and training of the teams in charge; (the decision on the implementation of the CSIRT (and incurring related costs) shall be submitted for approval of the Steering Committee either during the annual meeting or through ad hoc written consultation sent electronically to all members);
- Strengthening compliance with human rights and rule of law principles;
- Establishment of national, regional, and international cooperation.

Component 2 will adopt an incremental and flexible approach to planning and implementation in close coordination with the EU institutions, Member States' representatives and implementing partners.

Expertise France has identified the following success factors:

(i) focus on a sustainable capacity building approach,
(ii) prioritize the users' needs and priorities,
(iii) ensure the good coordination and cooperation.

This approach requires working closely with key stakeholders, including the creation of a working group in each beneficiary country.

The project approach, to be confirmed at inception phase, will thus focus in particular on the following:

(i) Existing regional and national actions.
Example: the World Bank is currently developing a cyber strategy and proposals of action and coordination calls have already started in order to exchange information and work on future synergies.
(ii) Existing country capacities and identified good practices.
(iii) South-South cooperation related to the creation of cybersecurity strategies, CERT and cyber labs. This can be achieved through "train the trainer" approaches.

Coordination between the Organisation and the Partners

In order to coordinate the implementation of activities, effectively explore and use synergies, as well as to ensure a transparent implementation and coordination, GIZ (organisation) and EF and FIIAPP (partners) will commit to a regular and structured exchange of information, knowledge and learnings. The modalities for cooperation and exchange will be agreed upon in a designated Partnership agreement and the organization and partners will ensure, that a coordinated approach to implementation will lead to a timely and adequate communication with regards to the partners and the EU and its institutions. Responsibilities with regards to implementation are clearly separated in this Description of the Action, as well as further specified in the partnership agreement to ensure accountability.

3.3 Indicative Activities

To achieve the envisaged outputs and the specific objective, the following key activities per output are foreseen. This list of key activities is indicative, will be reconfirmed during the inception phase and may change over the project cycle based on progress and feedback by stakeholders.

3.3.1 Indicative Activities Specific Objective 1 (GIZ & FIIAPP)

Key activities to **Specific objective 1** (implemented by GIZ and FIIAPP): Horn of Africa countries enhance their digital service delivery through implementing regional e-government building blocks.

Output 1 (GIZ)	**Key Activities**
The strategic, technical and regulatory prerequisites to introduce government e-services in selected countries of the Horn of Africa Region are evaluated.	***a.*** ***Stakeholder Interest Mapping and Needs Assessments:*** In order to prepare the selection process of five government services to be digitalised, a stakeholder interest and status-quo mapping will be conducted, to identify interests, regulatory and IT-related frameworks with the aim of obtaining an overview with regards to possible public sector institutions and respective service mandates, that could digitalized on the basis of the e-government building blocks.
	b. ***Multi-Stakeholder Consultation Process:*** Based on the needs assessment and stakeholder mapping, a cross-country multi-stakeholder consultation process, including the relevant public authorities in the HoA member states, for example, ICT Ministries and implementing agencies, as well as other public sector agencies, the private sector, academia and citizen representation, will be conducted. This process will ensure that the selected services to be digitalized have an adequate stakeholder support and have the potential for regional learning, exchange and potential harmonization.
	c. ***Requirement Analysis at national Level:*** After the selection of the participating public sector institutions in the selected HoA member states, an individual requirement analysis will be conducted for the selected services to be digitalised. This requirement analysis will serve to thoroughly evaluate all necessary technical, legal and organizational requirements, as basis for the local adaptation process of the government e-building blocks.
	d. ***Implementation Roadmap:*** Based on the requirement analysis, an implementation roadmap will be established with each participating public sector organization, clarifying the piloting and roll-out process, including an agreement on roles and responsibilities, evaluation methods and recommendations for the regional harmonization after the completion of the Action.

Output 2 (GIZ)	**Key Activities**
E-government building blocks are technically adapted for the	a. ***Local Adaptation of GovStack Building Blocks:*** Based on the local requirements and specifications, five of the existing GovStack Building blocks will be adjusted to meet the needs in the selected public services to be digitalised in the HoA region.

use in selected member states of the Horn of Africa Region.	b. ***Development of the Digital Government Service Platform:*** Development of a Digital Government Service platform to host the localized building blocks and enable public sector agencies to initially test, and later develop concrete digital government services on this basis.
	c. ***Development of Pilot Government Digital Services:*** Technical design of concrete pilot digital government services, based on the digital government building blocks and on the priorisation (Output 1, Activity d)
	d. ***Piloting Support to Public Sector Organisations:*** Support to the participating public authorities, responsible for the selected regional digital government services on national level to ensure the needed technical and change management related capacities to pilot the digital services, evaluate the pilot results and develop a clear strategy for rolling out the services.

Output 3 (FIIAPP & GIZ)	**Key Activities**
The technical and methodological competences of civil servants in the Horn of Africa Region to implement the e-government building blocks have been strengthened	a. ***Needs Identification (GIZ & FIIAPP):*** Needs identification in accordance with the selected GovStack building blocks, based on the assessment of relevant capacity gaps towards the introduction and piloting of the digital government services.
	b. ***Training Curricula Development (GIZ & FIIAPP):*** Curricula development, based on identified needs of implementing government agencies and working realities of civil servants responsible for the introduction and piloting of digital government services in fields such as Citizen-centred, design, Standardisation and Interoperability, data governance and management.
	c. ***Training Execution (GIZ & FIIAPP):*** Execution of trainings in blended-formats, including the production of didactically adequate e-learning formats, complemented by on the job trainings.
	d. ***Concept Development for the Communities of Practice (GIZ):*** Development of vision and mission statement for the diverse Communities of Practice. Development of didactical concept for the Communities of Practices, including identification of technical focus points, selection of focus areas, design of meeting and exchange structure, virtual collaboration channels and knowledge management structures.
	e. ***Community Management (GIZ):*** Community building and day-to-day management of the Communities of Practice, including ensuring synergies between the communities, active participation of the respective members, external communication and liaison with related global GovStack Communities.

Note: Output 3 is jointly implemented by GIZ and FIIAPP. Activities a-c will be carried out by GIZ and FIAPP jointly. GIZ will be responsible for the needs-identification, training curricula development and execution of trainings for 3 training modules related to the technical aspects of the digital government building blocks. Likewise, FIAPP will be responsible for the needs identification, training curricula development and execution of trainings for 3 training modules related digital change management aspects around the introduction of digital government services. These different training modules are reflected in two different indicators, to be achieved by GIZ (Output Indicator 3.1) and FIIAPP (Output Indicator 3.2). Activities d-e will be carried out by GIZ solely.

Description of activities FIIAPP

FIIAPP will focus the capacity building interventions on general change management related skills needed to master the digital transformation in the public sector for three main target groups: IT-specialists in the public sector, executive staff in the public sector, and regulators. This group of activities will address capacity building and the acquisition of digital competences in the digital environment. Firstly, the Training Programme for senior officials will be strengthened with mentoring and monitoring of digitisation projects. Secondly, there will be training on digital policy and regulation. Finally, specialised training for IT staff is foreseen.

Description of activities GIZ

GIZ will focus the capacity building interventions on the more specific technical and organisational skills needed to concretely design, pilot and implement the GovStack building blocks. This will encompass specific trainings for the IT staff and respective officers working with the e-government building blocks, in order to ensure a sound technical knowledge of the potentials of the e-government building blocks, the local GovStack platform and the design and piloting process of the building blocks and the development of concrete digital government services on their basis.

3.3.2 Indicative Activities Specific Objective 2 (EF)

Key activities to **Specific objective 2** (implemented by EF)**:** Horn of Africa countries develop and improve national and regional cybersecurity, promoting a single regional market in HoA countries.

Output 1	**Key Activities**
Strategic and institutional cybersecurity frameworks are reinforced and converging towards shared regional standards	**a.** ***Assessment national cybersecurity readiness:*** *Identify the critical gaps in each country's current situation during the inception phase in relation to a comprehensive baseline of internationally recognized principles and good practices in cybersecurity.*
	b. ***Set up of a regional technical committee (RTC):*** *Create a network of Project Contact Points (PCPs)* supported as much as feasible by the HoA Secretariat and national focal points*, nominated by each beneficiary country to ensures close relationships between each beneficiary institution and the Project Team and facilitates the exchanges and the participation to regional activities.*
	c. ***Design of national strategies and shared regional standards in alignment with international good practices on security of networks and information systems:*** *The regional standards shall be designed taking into consideration what has already been developed in the region and will be aligned with international good practices. They will be then promoted as a common baseline to be transposed into the national cybersecurity strategies of the region. These strategies will then be operationalised through specific action plans.*

Output 2	**Key Activities**

Cybersecurity awareness and capacities government officials and IT professionals as well as the general public are strengthened.	**a.** ***Establishment of a high-level dialogue on cybersecurity stakes:*** *Involve engagement of decision-makers and private sector is necessary for increasing awareness on cyber security and the protection of critical information infrastructures. Awareness raising activities will include as necessary the judiciary and law enforcement agencies.*
	b. ***Promotion digital hygiene awareness:*** *Promote digital hygiene with broader campaigns to the public at large on cybersecurity and internet safety, in cooperation with the local media*;
	c. Capacities improvement of IT ***professional on cybersecurity:*** Strengthen capacities of IT professional) who will be working on a daily basis on the topic through/within CSIRTs and those who ensure Critical Information Infrastructure Protection (CIIP) through trainings – including train the trainers approach-, online trainings and MOOCs (Massive Open Online Course) in line with international standards

Output 3	**Key Activities**
Operational capacities to handle cybersecurity incidents are enhanced	**a.** **Set-up or strengthening** ***of a national CSIRT in member states:*** *Identify gaps and improvements to be made to build capacity for Computer Security Incidents Response Teams (CSIRTs) Institutional and organisational requirements and arrangements for the establishment of a CSIRT*
	b. ***Set-up of a platform:*** *Maintaining a trusted contact network of computer security experts in the Horn of Africa region and enhancing information sharing and pooling of training resources to build up the region's awareness and competency in relation to computer security incidents. The platform will allow to disseminate, transfer and share knowledge on cybersecurity by providing the HoA countries with information, documentation and training materials for the beneficiaries. It will also host a glossary to provide all countries with a common language and thus facilitate regional cooperation. It may also include virtual training.*
	c. ***Introduction of regional operational and monitoring tools and systems:*** *Assessment and potential deployment of existing tools and measures to facilitate coordinated responses to large-scale network security incidents, information sharing and technology exchange.* • *Tools for Team cooperation and info sharing* • *Tools for Incident handling and response* • *Tools for Monitoring, detection -Tools for Forensic.* *Convergence of tools for sustainability of the action in addition to the Involvement of state to secure local office and environment as well as adequate HR.*

3.4 Main Partners, Target Group, Direct Beneficiaries

There are different groups of stakeholders to be considered for the Action, depending on the potential entry and impact points for the intervention(s).

The main target group of this Action are governments from the six partner countries involved in the HoAI (*duty bearers*). This target group, being represented by different national public sector authorities in the member states of the HoA region, e.g. Ministries, subordinate bodies, such as executive agencies, regional public sector agencies, etc, will be supported by the Action towards developing digital public services and to enhance cybersecurity in their operations. The Action considers the differences between the six countries in terms of capacity and operational readiness of the public and private sector to engage in designing, implementing, using actively, and maintaining outputs of the proposed activities. The Action

plans to address the differences in Specific Objective 1 Output 3 and Specific Objective 2 Output 2 around capacity and awareness building.

Another target group of this Action are civil society organizations, academic organisations and private sector entities (*duty bearers*) that will be involved in the Action to ensure the accountability, effectiveness and transparency of the digitalization and cybersecurity interventions pursued in the Action, through an involvement in consultation and cooperation processeses. These target groups encompass for example mobile network operators, software development firms and system integrators, market research agencies (either local entities or or locally operated divisions of international entities), or Civil Society Organisations working in related fields to the digital transformation of public services, e.g. focussing on digital rights, vulnerable populations, data protection.

The final target group of this Action (*rights holders*) are the citizens and residing populations of HoA countries who will be the ultimate beneficiaries from the improved conditions resulting from the outcomes achieved in this Action long-term, specifically improved digital public service delivery, and a secure cyberspace.

International partners to be mobilized for the implementation of the action are the following:

(i) From Europe:
- EU Member States (Germany and France specifically and indirectly others in the EU D4D hub), their development agencies and other relevant Member States Organisations (MSOs)
- Relevant EU institutions, such as the European Commission and other public sector actors

(ii) From the region:
- The African Union Commission (AUC), and especially the Infrastructure and Energy Directorate, as well as other affiliated entities
- The Smart Africa Alliance and respective working groups
- Local EU Delegations (EUD) and UN agencies' delegations
- Other partners, multilateral or local, with complementary activities or efforts underway in target countries, e.g. World Bank Group

3.5 Resource Allocation

Project Offices

For the Organisation (GIZ)

The Action has two project offices, one in Nairobi (Kenya), one in Bonn (Germany). The existing GIZ project office in Bonn supports the Action with administrative, contractual, procurement and finance related activities, which the country project office in Nairobi directly implements. All project offices have the primary responsibility and purpose of actively following up, monitoring, checking quality, delivery, and timeliness of activities.

For all above-mentioned offices, the proposed Action requires office equipment as well as the covering of set-up and operating costs (e.g. water, electricity, insurances, maintenance, telephone, security, and ICT related costs, travel costs, fuel, etc.).

For the Partner (Expertise France)

The Action has two project offices, one in Paris, one in Nairobi. The project office in Paris supports the Action with administrative, contractual, procurement and finance related activities, which the country project office in Nairobi directly implements. All project offices teams have the primary responsibility and purpose of actively following up, monitoring, checking quality, delivery and timeliness of activities.

For the Partner (FIIAPP)

The existing office of FIIAPP in Madrid will support the Action with administrative, contractual, procurement and finance related activities. There is no project budget earmarked for the purpose of maintaining the office at FIIAPP.

Personnel

The Action will be implemented by a team of seven GIZ staff in two different project locations, one FIIAPP staff in one project location and five EF staff in two different project locations.

For the Organisation (GIZ)

At the start of the project, the GIZ team will consist of one Project Coordinator (15% FTE, Bonn), one International Project Manager (100% FTE, Nairobi), one National Technical Coordinator (100% FTE, Nairobi), one National Project Assistant (100% FTE, Nairobi), one Project Assistant (100% FTE, Bonn); one National Support Staff Manager (50% FTE, Nairobi), one Financial Manager (50% FTE, Bonn). The configuration of the team may change over time according to the needs of the Action. GIZ will report on changes of the team through its progress reports.

The Project Coordinator (Bonn) will be responsible for the overall coordination of the Action (according to Article 2 of Annex II. a), including closure activities after the end of the implementation period.

The International Project Manager (Kenya) will regularly liaise with project partners to ensure a holistic implementation of GIZ's part of the Action and the other parts of the Action implemented by other partners. She/He will be coordinating the subcontractors and will oversee the reporting of the part of the Action implemented by GIZ. She/He will be in charge of supervising all administrative and financial activities of the part of the Action implemented by GIZ, including contractual management and budgetary control. Regularly liaises with project partners (EF and FIIAPP) to ensure a holistic implementation of the different components of the action (including e. g. coordination of visibility activities and liaising with relevant stakeholders in the beneficiary countries to ensure coherence of the Action).

The National Technical Coordinator (Kenya) will be in charge of the coordination and the smooth running and timely implementation of the part of the Action implemented by GIZ. She/He will ensure the successful technical implementation of the activities of the part of the Action implemented by GIZ and for the achievement of the expected results; analyses on trends in the subject matter; formulation of recommendations on appropriate adjustments and

programming; maintain a working relationship with local authorities; provide technical assistance to beneficiary countries, formulate training programmes and control their execution.

The National Project Assistant (Kenya) will support the coordination and the smooth running and timely implementation of the part of the Action implemented by GIZ. She/He will support the successful technical implementation of the activities of the part of the Action implemented by GIZ and for the achievement of the expected results.

The Project Assistant (Bonn) will support the coordination of the subcontractors and will support the reporting of the part of the Action implemented by GIZ. She/He will support the overall coordination of the Action (according to Article 2 of Annex II. a).

The National Support Staff (Kenya) will be in charge of financial and administrative tasks for the part of the Action implemented by GIZ Action, including grants, workshops and events and logistics associated with the implementation period.

Financial Manager (Bonn) will be in charge of financial and administrative tasks for the part of the Action implemented by GIZ Action, as well as tasks associated with the role of the Organization (according to Article 2 of Annex II. a) such as transferral of funds to partners of the Action and closure activities after the end of the implementation period.

The staffing in the project will be complemented by procurement of expertise, consultancy contracts and grants as well as budgets for workshops, trainings and procurement of equipment as specified in the budget.

Financing / Grants

To provide technical support to the component different Grants to international organisations or institutions are foreseen. Already identified financing recipients are the founding partner of the GovStack Initiative (ITU, Estonia and DIAL), each representing a different part of the digital ecosystem and supporting the action with special competency. Details on the objective and main activities foreseen for the planned grants and an explanation on the determined amount for each grant will be provided in the inception report.

ITU will support the technical leadership of the component. That includes the overall management of the technical parts, including engagement with experts, advisory to experts and guiding the technical work.

The Estonian Centre for International Development (EstDev) will mainly support with assessments and strategic advocacy and events, for example with overall PR and awareness-raising in various forums relevant to the component.

DIAL will support the overall strategy of the component.

Together, these partners will ensure alignment with agreed-upon country and perspective regional objectives. Other possible financing recipients such as KictaNet, Estonian E-Academy and Oxford Digital Pathways supporting the component with capacity strengthening activities and change management will be identified in the inception phase.

For the Partner (Expertise France)

The partner will staff the project with one Project Manager (100% FTE, Kenya), one Technical Coordinator (100% FTE, Kenya) and one project assistant (100% FTE, Kenya). The project office will be supported by HQ with one Back office HQ Project Officer (50% FTE, Paris) and one HQ Back office Project Assistant (50% FTE, Paris).

The Project Manager (Kenya) will regularly liaise with project partners to ensure a holistic implementation of EF's part of the Action. She/He will be coordinating the subcontractors and will oversee the reporting of the part of the Action implemented by EF. She/He will be in charge of supervising all administrative and financial activities of the part of the Action implemented by EF, including contractual management and budgetary control. Regularly liaises with project partners (GIZ and FIIAPP) to ensure a holistic implementation of the different components of the action (including e. g. coordination of visibility activities and liaising with relevant stakeholders in the beneficiary countries to ensure coherence of the Action).

The Technical Coordinator (Kenya) will be in charge of the coordination and the smooth running and timely implementation of the part of the Action implemented by EF. She/He will ensure the successful technical implementation of the activities of the part of the Action implemented by EF and for the achievement of the expected results; analyses on trends in the subject matter; formulation of recommendations on appropriate adjustments and programming; maintain a working relationship with local authorities; provide technical assistance to beneficiary countries, formulate training programmes and control their execution.

The Project Assistant (Kenya) is in charge of local expenses, the office expenses and activities expenses in the beneficiary countries (if needed), she/he will also be in charge of carrying out administrative duties, managing logistics, making arrangements for steering committees, meetings, presentations, workshops and trainings being organized in relation to the part of the Action implemented by EF, in close coordination with the project manager and the HQ project officer based in Paris.

HQ Back-office Project Officer (Paris) ensures synergies and consistency with similar projects managed by EF. She/he will be in charge of supervising all administrative and financial activities of the part of the Action implemented by EF (e.g. contractual management, budgetary control and audits). She/he will ensure quality control of narrative and financial reports as well as all deliverables part of the Action implemented by EF and contribute to solving any difficulty raised by the PMU.

HQ Back-office Project Assistant (Paris) is in charge of administrative duties and logistics of the part of the Action implemented by EF in close coordination with the Assistant based in Kenya. She/he will be in charge of review field expenses, carrying budgetary control measures, and supporting the project officer for audits in close coordination with the project assistant and manager based in Kenya.

Pool of Non-Key Experts will be available for providing a punctual expertise in the project. The experts will be hired according to the needs of implementation of the project's activities. All experts will be independent and free from conflict of interest in the responsibilities they take on.

For the Partner (FIIAPP)

The partner will staff the project with one Project Manager (50% Project Manager in Madrid). Regular backstopping services are provided by FIIAPP's Project Managers based in Madrid, chosen based on previous specialised technical expertise. FIIAPP will provide adequate support facilities to the team of experts and/or civil servants from the different Spanish Institutions (Spanish data protection agency (AEPD); Red.es; Centre for the Development of Industrial Technology (CDTI); Ministry of Internal Affairs; National Cryptologic Centre (CCN);EOI – Escuela de Organización Industrial – Industrial Organization School;ISDEFE;INCIBE;INAP – National Institute of Public Administration; CIJA-UAM; Ministry of Economic Affairs and Digital Transformation of Spain; Ministry of Industry, trade, and tourism of Spain; City Council of Madrid; City Council of Barcelona; Ministry of Foreign Affairs, European Union, and Cooperation of Spain; Ministry of Territorial Policy and Public Function of Spain; Ministry of Education and Vocational Training of Spain; Ministry of Health of Spain; National Statistics Institute (INE);Ministry of Culture and Sports of Spain; Ministry of Finance of Spain; Ministry of Consumer Affairs of Spain; National Consumer Institute; Department of Education of the Regional Council of Castile and León; National Commission of Markets and Competition (CNMC);Official College of Telecommunication Engineers (COIT); Madrid Autonomous Community) during the implementation of the contract, including logistic support in case of travelling. This support and backstopping should also include quality reviews of the training materials in all the different languages, when necessary.

The Project Manager (Madrid)

The Project Manager will ensure quick action and that all results are accomplished within the timeframe. She/he will prepare terms of reference, methodological notes, identification of institutions and search for experts for the activities of the Action implemented by FIIAPP. She/he will monitor and supervise contract compliance, review of financial deliverables from experts and suppliers, she/he will prepare follow-up documentation, consolidation of information and knowledge management. She/he will follow-up of the correct execution of the activities' funds and supervise the preparation and presentation of financial reports. She/he will prepare reports and internal notes on FIIAPP responsibilities in coordination with GIZ and EF.

Overview

The Organisation GIZ*		
Staff (% of working time)*	**Function, Tasks and Responsibilities***	**Location***
15%	Project Coordinator • Responsible for the overall coordination of the Action (according to Article 2 of Annex II. a), including closure activities after the end of the implementation period.	Bonn
100%	International Project Manager • Responsible for the overall management of the part of the Action implemented by GIZ including	Nairobi

	• Regular liaising with project partners (EF, FIIAPP) to ensure a holistic implementation of the different parts of the Action (including e. g. coordination of communication and visibility activities and liaising with relevant stakeholders in the beneficiary countries	
100%	National Technical Coordinator • Responsible for the coordination and the smooth running and timely implementation of the part of the Action implemented by GIZ. • Ensure the successful technical implementation of the activities of the part of the Action implemented by GIZ. • Responsible for achievement of results; analyses on trends; programming; working relationship with local authorities; technical assistance to beneficiary countries, training programmes and execution.	Nairobi
100%	National Project Assistant • Support the coordination and the smooth running and timely implementation of the part of the Action implemented by GIZ. • Support the successful technical implementation of the activities of the part of the Action implemented by GIZ and for the achievement of the expected results.	Nairobi
100%	Project Assistant • Support the coordination of the subcontractors and will support the reporting of the part of the Action implemented by GIZ. • Support the overall coordination of the Action (according to Article 2 of Annex II. a).	Bonn
50 %	National Support Staff Manager • Financial and administrative tasks for the part of the Action implemented by GIZ Action, including grants, workshops, events and logistics associated with the implementation period.	Nairobi
50 %	Financial Manager • Financial and administrative tasks for the part of the Action implemented by GIZ Action • Tasks associated with the role of the Organization (according to Article 2 of Annex II. a) such as transferral of funds to partners of the Action and closure activities after the end of the implementation period.	Bonn

Staff (% of working time)	Function, Tasks and Responsibilities	Location
The Partner EF		
100%	Project Manager • Responsible for the overall management of the part of the Action implemented by EF including • Regular liaising with project partners (GIZ, FIIAPP) to ensure a holistic implementation of the different parts of the Action (including e. g. coordination of visibility activities and liaising with relevant stakeholders in the beneficiary countries)	Kenya
100%	Technical Coordinator • Responsible for the coordination and the smooth running and timely implementation of the part of the Action implemented by GIZ. • Ensure the successful technical implementation of the activities of the part of the Action implemented by GIZ. • Responsible for achievement of results; analyses on trends; programming; working relationship with local authorities; technical assistance to beneficiary countries, training programmes and execution.	Kenya
100%	Project Assistant • In charge of expenses in the beneficiary countries (if needed) • In charge of carrying out administrative duties, managing logistics, making arrangements for steering committees, meetings, presentations, workshops and trainings being organized in relation to the part of the Action implemented by EF	Kenya
50%	HQ Back office Project Officer • Ensure synergies and consistency with similar projects managed by EF. • In charge of supervising all administrative and financial activities of the part of the Action implemented by EF • Ensure quality control of narrative and financial reports as well as all deliverables part of the Action implemented by EF	Paris
50%	HQ Back office Project Assistant • In charge of administrative duties and logistics of the part of the Action implemented by EF	Paris

	• She/he will be in charge of review field expenses, carrying budgetary control measures, and supporting the project officer for audits	
	Pool of Non-Key Experts	tbd
Staff (% of working time)	**Function, Tasks and Responsibilities**	**Location**
The Partner FIIAPP		
50%	Project Manager • Ensure quick action and that all results are accomplished within the timeframe. • Prepare terms of reference, methodological notes, identification of institutions and search for experts for the activities of the Action implemented by FIIAPP. • Monitor and supervise contract compliance, review of financial deliverables from experts and suppliers • Prepare follow-up documentation, consolidation of information and knowledge management. • Follow-up of the correct execution of the activities' funds and supervise the preparation and presentation of financial reports • Prepare reports and internal notes on FIIAPP responsibilities in coordination with GIZ and EF.	Madrid

***** Configuration of the team at the start of the project. The configuration of the team can change over time according to the needs of the Action. GIZ will report on changes of the team through its progress reports.

4 Project Governance

Under this Action, GIZ coordinates the digital government component (Specific Objective 1 – Digital Public Service Delivery through e-Government Building Blocks) while Expertise France will be responsible for the cybersecurity component. A common project management unit (which consists of the Project Managers of GIZ, EF and FIIAPP) will oversee the implementation of both components. DIAL, EstDev and ITU will provide technical support to the project. Together, these partners will ensure alignment with agreed-upon country and regional objectives.

The governance of the project will be adapted to the needs of the beneficiaries to implement the relevant actions in a timely manner. Especially, a collaborative governance mechanism will be set up between GIZ, EF and FIIAPP to ensure good coordination between the different components of the project and a smooth implementation of all activities.

4.1 Steering Committee (SC)

A Steering Committee (SC) chaired on rotational basis by members representing all the involved partners (Minister or someone directly delegated by the Minister, as appropriate) and other relevant stakeholders will be set up. The BMZ, EF, FIIAPP and the EU as contracting authorities will be part of the SC. In addition to the SC members, the Board is accompanied by SC Observers composed of representatives from relevant partner organisations and institutions (e.g. ITU, DIAL, EstDev, D4D Hub).

The SC is the political and strategic body of the Action. The SC reviews progress in the implementation of the components based on activities of the previous year, provides strategic guidance and recommendation to the management of the components on the upcoming activities and reflect on potential implementation risks. The SC will provide and mobilise diverse expertise and networks and share experiences from user or supplier side that can support the implementation and projects outcome. The SC will receive, review and discuss external monitoring reports and evaluations, when applicable. The SC shall meet once a year either in person in the premises of the Commission or the HoAI Secretariat or virtually, starting with a kick-off meeting at the start of the project. Ad-hoc meetings can be organised when necessary.

The preparation of Steering Committee meetings will be coordinated by the Project Management Unit (see description below).

Role of the Steering Committee

- Review of the overall project progress by the implementing parties, the general engagement by the partners, the work plan and logical framework
- Review the progress of activities implemented during the previous period and as well as the M&E progress made by the partners, which are detailed in the logframe and the Communication and Visibility Plan (CVP)
- Provide strategic guidance and recommendations to the management of the project
- Inform the Steering Committee Observers about updates and running activities

Role of the Steering Committee Observers

- Give feedback on activities of the previous year
- Give advice and orientation on the upcoming year programmed activities by providing and mobilising diverse expertise and networks
- Share experiences from user or supplier side that can support the implementation and projects outcome
- Advise and reflect on potential implementation risks

Steering Committee Members

The steering committee will be composed of the following members:

1. HOA country representatives
2. An EU representative (Project Officer)
3. A representative of BMZ / GIZ
4. A representative of EF
5. A representative of FIIAPP

Steering Committee Observers

1. Representative from the HoAI secretariat

2. Representative of EstDev
3. Representative of ITU
4. Representative of DIAL
5. Representative of D4D Hub
6. Other EU agency representatives (FPI, SEAE, EUD) can be invited to attend SC meetings

4.2 Project Management Unit (PMU)

The Project Management Unit (PMU) works together on a daily basis and will be responsible for the day to day implementation of the Multi Donor Action. The PMU is composed of the three International Project Managers from GIZ, EF and FIIAPP. The PMU convenes at least once a month, if necessary and on an ad-hoc basis for urgent/priority requests. The PMU is responsible for the overall execution of the Action and ensures smooth implementation of the action and reporting.

Role of the PMU

- Ensure the overall and results-oriented coordination of the project
- Implement, execute and review activities and monitor follow-up and flag any concern related to the implementation of action
- Review the upcoming action plan in relation with the expected results of the project
- Review, propose and monitor activities for the two project components, especially in terms of monitoring and evaluation, communication and visibility, and joint activities/events (when relevant)
- Prepare the Steering Committee (SC) meetings and ensure the communication process

5 Sustainability, Complementarity and Cross-Cutting Issues

5.1 Sustainability of the Action

The sustainability of the Action is ensured across several dimensions, ranging from financial aspects, to institutional, policy and environmental sustainability.

Development of long-term policy frameworks and action plans

The policy sustainability of the Action will be ensured through the development of regional approaches such as the regional Cybersecurity Strategy and the recommendations for the possible regional harmonisation of digitalised national services, which will document the concrete and measurable actions undertaken to develop the digital government services and cybersecurity capacities in the HoA region. These include harmonisation of legal policies or proposal to do so.

Interoperable software, platforms and tools

The Action aims to ensure access to license-free, interoperable, and reusable software products on a permanent basis. Further, the provided GovStack building blocks, which will be localized to the specifications in the selected HoA member states, can serve as basis for the design and development of the main government services in different sectors and for different government agencies. Through the Action, five digital government services will be piloted across selected member states. Given the open access and interoperability of the GovStack building blocks, additional digital government services could be developed, allowing interested government agencies to test and pilot services on the model platform without having to design, test and operate the underlying systems and infrastructure themselves.

Long-term training capacities

The human capacity development modules created during the Action will be made available as e-learning products that can likewise be reused and provide guidance for the training of additional public servants. The continuous exchange between relevant actors in different communities of practice, complementing the formal capacity building program, will be designed in such a way that the communities of practice can be further anchored locally and sustainably. An exchange with further communities of practice from the global GovStack project or through the cybersecurity Regional Technical Committee will ensure international exchange and knowledge transfer even after the implementation of the Action.

Success factors also include a comprehensive sustainable capacity building approach to ensure the operationalisation of national institutions and expertise, so that cyber-attacks and vulnerabilities can be addressed permanently. The train-the-trainer programme will be able to ensure a coherent and sustainable capacity building programmes within the region.

Environmental sustainability

With regards to environmental sustainability, the Action will contribute to a reduction in travel costs, for example when citizens and businesses are enabled to access government services online and handle them end-to-end digitally.

5.2 Complementarity, Synergy with other relevant Actions

This section briefly highlights the complementarity of this action with other actions in the sector funded by the EU, as well as other initiatives, projects, and actions taken by other possible donors and entities (both public and private).

GIZ and Expertise France Partners

In order to swiftly implement the *D4D Collaboration for a Horn of Africa Initiative on Digital Government and Cybersecurity* project while building on existing efforts regarding cybersecurity capacity building and awareness raising in the region, GIZ and Expertise France will further rely on local partners and networks, such as African Development Bank (AfDB), the East African Community (EAC) or the Regional Internet Registry for Africa and the Indian Ocean (AFRINIC), which aims at strengthening Internet self-governance in Africa, as well as the Cybersecurity Alliance for Mutual Progress (CAMP), which consists of a network platform

to lift up the overall digital government transformation cybersecurity of its members (including Ethiopia and Kenya).

African Development Bank (AfDB)
The Regional Integration strategy of AfDB is well-aligned with the two HoAI pillars concerning Infrastructure Connectivity (including elements of the battle against climate change) and Trade and Investment. There are potential synergies here, both on GovStack and on cybersecurity, especially in discussing and developing core elements of a Strategic and Institutional Framework for the region.

BMZ Digital Transformation Center (DTC) Kenya
The BMZ DTC will focus on the partner needs of the Ministry of ICT (MoICT) in Kenya in the area of digital government and will pursue a whole-of-government advisory approach to further develop e-government approaches. The DTC supports the government in implementing concepts and approaches to operationalise the Digital Economy Blueprint and will advise MoICT on the development of the HUDUMA administrative platform, based on secure and human-centred online services as well as the technological basis through reusable applications (e.g., digital ID, e-payment, registration, information exchange, security). The DTC also supports the government in implementing data protection compliant approaches.

Business Environment and Investment Climate (BECI)
The project Business Environment & Investment Climate including e-government (BECI) is funded by the European Union and implemented by GIZ in Ethiopia. The overall objective of the project is to contribute to the improvement of the business environment in Ethiopia, to foster private sector development, and the generation of employment and income opportunities in the context of the Ease of Doing Business (EODB) programme of the government. The project is focused on three objectives that are complementary with the planned actions around the GovStack component:

(i) Providing technical assistance and capacity-building to public sector entities in Ethiopia for implementing reforms to improve the business environment;
(ii) Supporting the establishment or modernisation of e-government systems and provide capacity-building and implementation support for the e-government systems; and,
(iii) Supporting public-private dialogue in Ethiopia with existing and potential investors.

East African Community (EAC)
The planned activities are complementary with the East African Community (EAC). The digital building blocks are anchored in the regional programming of the EAC under “Block 1: One single digital market” (cf. regional programming working paper).[21]

[21] Regarding “Block 1: One single digital market” the regional programming of the EAC states that: *"To achieve these efficiency gains in the EAC region, the IT infrastructure must be improved. This can be done by developing, using and advising on appropriate ICT building blocks for the various subject areas. This is about designing and implementing generic digital goods, which will simplify the costs, time, and*

International Telecommunications Union (ITU)

The ITU regional presence in the African and Arab regions will be key to facilitate smooth coordination and collaboration with the ministries of ICT of the HoA countries who are members of ITU. The joint project will also synergize and benefit from several current initiatives and activities that are currently held by ITU including the following:

- **Capacity Development Programme[22]:** Aims to achieve a digitally competent society where all people use knowledge and skills on digital technologies to improve their livelihoods.
- **ITU Academy[23]:** Offers a large selection of online, face-to-face and blended courses covering a wide range of digital skills and competencies.
- **Digital Transformation Centres:** An initiative that seeks to create a global network of centres to develop basic and intermediate digital skills among citizens.

Additionally, the work of ITU in the area of Policy and Regulation[24] will provide useful resources, platforms and tools that could be leveraged to support regulators and policymakers in driving inclusive and cross-sectoral collaboration to create a virtuous dynamic for the digital transformation. Moreover, ITU as an ICT Standardization Organization provides handful of standards in relevant areas such as security, identity management, smart cities, digital payments, etc. that will be used to inform the design of products and services that will be developed in the context of this project.

The ITU Cybersecurity Programme[25] offers also a wide variety of resources and tools to increase cybersecurity capabilities at the national level, in order to enhance security and resilience, build confidence and trust in the use of ICTs – making the digital realm more safe and secure for everyone. Tools and resources include support to develop national cybersecurity strategies, National CIRTs, Child Online Protection among others.

World Bank Group

The Regional Integration and Cooperation Assistance Strategy of the World Bank Group makes explicit reference to the Horn of Africa while also covering key program areas as broader priorities.

The World Bank GovTech, Global Partnership approach, emphasizes three aspects of public sector modernization:

1. Whole-of-government-approach to digital transformation

---

resources needed for building digital government solutions. This approach, known as "digital building blocks", will enable any government to easily create and modify their own digital platforms, systems, services, and applications."

[22] https://www.itu.int/itu-d/sites/cybersecurity/
[23] https://academy.itu.int/home
[24] ITU-Development Policy and Regulation
[25] https://www.itu.int/itu-d/sites/cybersecurity/

2. Citizen centric services that are universally accessible
3. Efficient and straightforward government systems

The D4D Collaboration for a Horn of Africa Initiative on Cybersecurity project could also be complementary to other initiatives implemented by diverse donors in the region who are pursuing the same goals. The World Bank is particularly active in several of the Horn of Africa countries on ICT and cybersecurity topics.

The World Bank is currently implementing several projects in the HoA region. Some examples include:

Djibouti:

1. Public Administration Modernization Project (PAMAP)[26]: A project to strengthen the foundations of e-government and to support the creation of an adequate cybersecurity framework.
2. Djibouti Digital Foundations Project[27]: A project which includes a component on the necessary digital transformation and skills.

Somalia:

1. ICT Sector Support[28]: A project to improve the national ICT legal and regulatory framework
2. SCALED-UP[29]: A project focusing on the digitalization of the country in order to foster the development of its economy.

Kenya:

1. Kenya Digital Economy Acceleration Project[30]: A project that aims at expanding digital inclusion and fostering development of the digital infrastructure, institutions and capabilities for the economy, jobs and government of the future.

Ethiopia:

1. Ethiopia Digital Foundations Project[31]: A project that aims to increase the inclusiveness and affordability of digital services and digital job creation in Ethiopia.

The Global Forum on Cyber Expertise (GFCE)

The Global Forum for Cybersecurity Expertise (GFCE), a multi-stakeholder community of 115 members and partners worldwide, aiming to strengthen cyber capacities and expertise, has also been active in the region. Created in 2015, the Forum notably published a Delhi

[26] https://projects.worldbank.org/en/projects-operations/project-detail/P162904?lang=en
[27] https://projects.banquemondiale.org/fr/projects-operations/project-detail/P174461
[28] https://projects.worldbank.org/en/projects-operations/project-detail/P148588
[29] https://projects.worldbank.org/en/projects-operations/project-detail/P168115?lang=en
[30] https://projects.worldbank.org/en/projects-operations/project-detail/P170941
[31] https://projects.worldbank.org/en/projects-operations/project-detail/P171034

Communiqué in 2017 detailing its global agenda for cyber capacity building encompassing five key themes:

1. Cybersecurity policy and strategy
2. Cyber incident management and critical infrastructure protection
3. Cybercrime
4. Cybersecurity culture and skills
5. Cybersecurity standards

The cyber security component of the Action will contribute to developing and expanding measures to combat the five key themes listed above.

5.3 Mainstreaming

In the areas of the environment, climate change mitigation and adaptation, human rights, conflict and context sensitivity, and gender equality, the safeguard and gender system of GIZ allows unintended negative impacts to be identified at an early stage and addressed in the design and implementation of projects through targeted mitigation measures. In the area of climate change adaptation, this approach extends to external risks based on climatic parameters (climate change), while in the area of gender equality it also involves identifying potential support measures.

In an initial screening, a standardised checklist is used to assess if there are potential considerable risks or unintended negative impacts for the proposed Action in the areas of environment, climate change adaption and mitigation, and human rights. The screening also checks whether a gender analysis is already available and whether it must be adapted for the specific Action. For the conflict and context sensitivity safeguard, the screening will assess if the proposed Action is being planned in a country which is characterised by fragility, violence or conflict.

If the screening indicates that there are potential considerable risks for one or more of the safeguards, an in-depth assessment must be performed for the relevant safeguard(s). An in-depth assessment will also be performed if the initial screening cannot be satisfactorily completed due to inadequate data. The mandatory gender analysis will be used to examine risks and potentials for the promotion of gender equality. Depending on the results of the in-depth assessment(s), the proposed Action will be assigned to one of the three safeguard risk categories (high risk, medium risk, low risk). Based on the in-depth analyses and in line with the assigned risk category, response, prevention, and mitigation efforts will be considered to adjust planning and effectively monitor the progress of the proposed Action.

The Action will adopt a proactive approach on gender equality in its implementation. The Action will seek to ensure that female government officials, officers, prosecutors, etc. be included in all trainings, mentoring, workshop, and other operational activities linked to the project to increase effectiveness of the interventions. In a similar vein, beneficiary countries will be advised on their recruitment policies for staff such as human resources, in line with gender equality principles and guidelines as to fair and non-discriminatory treatment. The project will also ensure that tenderers involved in its procurement activities will favour, in all cases, when legally possible, equal opportunity policies.

The action will adopt appropriate human-rights and privacy-by-design based approaches which will be integrated in the design of any tools and activities from the start. Human rights, including freedom of speech, privacy and equality of arms, as well as the best practices and safeguards offered by international data protection law will be at the base of any software, activities and interventions delivered by the project.

When designing public policies, for example developing new digital government services, the Action will ensure a citizen-centred approach that takes into account different perspectives with regards to different end-user groups and requirements to the provision of public services, in accordance with a rights-based approach and the principle of leave-no-one-behind. With the development of further digital government services in the future, the Action lays the groundwork to reduce administrative burdens and increase the efficiency of government services. This can contribute to an increased trust and reliance of citizens in the service delivery capacity of the public sector and lead to stronger public institutions that cater the needs of all citizens.

6 Risks and Assumptions

Several risks are identified and will have to be mitigated to ensure a successful implementation, both on a general level for the two Specific Objectives of the Action, as well as specific risks, relating to only the Digital Government Component (Specific Objective 1) and to the Cybersecurity Component (Specific Objective 2).

Risks	Risk level (H/M/L)	Mitigating measures
A deterioration of the security situation, due to factors such as conflict or the influences of the COVID-19 pandemic can adversely affect the possibility to implementing activities in certain countries of the HoA and/or severely affect the planned timing.	High	Implementation partners will constantly monitor these aspects in liaison with their own security department, the Ministry of Foreign Affairs as well as the EUDEL of the HoA region.
Significant variations in methods, organisation and legal frameworks from one country to another can hinder a harmonized procedure and development of strategies and capacities.	High	Specific assessment will be part of the inception phase in order to evaluate state of play of the HoAI countries and design appropriate instruments and approaches. National-first approaches to set the right incentives for other countries to follow-suit and be motivated will be likewise pursued.
Delays in implementation given slow decision-making processes, the need for regional stakeholder coordination and the need to build trust and close working relations with	High	Working closely with the country focal points and establishing a Project Director function (PMU) in order to quickly identify and anticipate administrative obstacles and bottlenecks. Implementation partner will ensure that the completion of activities at regional level are not treated as a prerequisite for implementation at national level. As an example, a national activity will not have to wait for the

many different public sector partners with diverging interests.		regional policy to be fully approved: national deployment will start in parallel with work at regional level, in full coordination and with support from the implementation partner.
Low consideration by decision makers on the need for national strategies on Digital Government Services and Cybersecurity harmonisation.	Moderate	Implementation partner will constantly promote strategies that are impact-oriented and that have a clear potential to enhance performances at an operational level. Will seek coordination with relevant EUDs and regional partners to escalate at the political level, as required.
Learning is not sustained due to staff change or lack of use of acquired knowledge	Moderate	Implementation partner will ensure a blended approach to learning including traditional face-to-face, online, on-the-job, etc. to ensure that acquired learning is reinforced and not limited to theoretical approaches but well assimilated through learning by doing and learning by example. All learning materials will be also available online with recordings of the sessions to ease the replication of the trainings to additional staff who might not have participated in the initial sessions.
Gender: not enough proactive actions in favour of ensuring women participate and benefit.	Moderate	Implementation partners will systematically monitor gender inclusion and balance in all proposed activities including trainings, consultations, uptake and adoption of digital services, etc. They will be required to report regularly on gender inclusiveness through all reporting activities including suggesting measures to address any gender gap or unbalance.
Specific Risks related to Specific Objective 1		
A national-first approach towards the digitalization of public services with potential for regional harmonisation could impede the willingness of other HoA countries to participate in the process.	Moderate	Awareness-raising activities, close political and technical dialogues and regular information exchange with regards to the developed digital services based on the GovStack building blocks will be shared also with the other HoA member states, that do not participate in the first wave of piloting.
Low willingness of public sector entities in selected HoA member states to allocate sufficient resources and time for the development of digital government services based on the building blocks.	High	Constant stakeholder engagement and clear communication of the added-value proposition of the e-government building blocks, including possible synergies between digitalisation processes in country and with the international GovStack community can reduce the risk and increase the willingness of public sector entities to allocate resources.
Specific Risks related to Specific Objective 2		
Ambition to design the perfect legal framework at the risk of delaying the implementation phase	Moderate	Implementation partner will showcase experiences from other countries where legislation using standard provisions have been enacted swiftly and then improved later. The partner will also provide guidance on strategies which include a continuous improvement process.

Equipment and software solutions are not maintained (including recurring payment of licenses).	Moderate	Implementation partner will negotiate Long Term Agreements (LTA) to ensure sustainability of delivered equipment and solutions that will also include knowledge transfer to local staff. Local providers will be encouraged and preferred to participate in the delivery of services. Open-Source Software (OSS) and Digital Public Goods (PDGs) will be the preferred choice for the selection of products to be used to deliver government services
Disagreement over where common facilities should be localised (e.g., data centres)	Moderate	Implementation partner will facilitate regional dialogues to identify opportunities to leverage infrastructure sharing across the region whenever there is a strong case for it for economies of scale, sustainability, lower maintenance cost, scalability, etc. Appropriate legal and regulatory frameworks will be proposed as well to ensure secure information flow and privacy and data protection across borders. This will ease the negotiation among concerned countries. Choices of location will be done based on rational and objective criteria that countries will have to agree upon.
Access to documents and data as well as to CSRTs is granted for the effective estimation of the national frameworks and needs	Moderate	Implementation partner will engage national authorities during the inception phase, in order to explain the overall objective of the component, the added-value expected for the beneficiary countries, taking example on the work carried out through the OCWAR programme in Western Africa.
Assumptions		
Clear division of labour and responsibility for activities, efficient cooperation and trust among the implementing partners and Parties to this Agreement.		
Each Party to the MPCA (GIZ, EF and FIIAPP) fully implements those activities that it was assigned according to this Agreement.		
Assumptions related to Specific Objective 1		
The complex political context in the Horn of Africa region is stable and allows engagement and completion of the activities foreseen in the component.		
Public Sector entities in the HoA region are willing to allocate personal and financial resources to support the development of e-services based on the e-government building blocks.		
The sequencing approach, focusing first on national digital services and evaluating their potential for regional harmonization does not impede further HoA member states to become involved in the introduction of digital government services based on the e-government building blocks at a later stage.		
Selected Member states of the HoA Initiative are willing to contribute to the technical, regulatory, and legal preparation process for the introduction of digital government services, based on the e-government building blocks.		

Different national priorities and levels of digital readiness do not impede the selection of digital services with a potential for regional harmonization.
Other actors from the private sector and civil society are willing to contribute a consultation process around the introduction of digital government services.
HoA governments are willing and able to contribute to the procurement process for mobilizing private sector support to specifying and localizing e-government building blocks.
Diverging interests, priorities and needs by the different HoA member states do not impede the specification and localization of the selected e-government building blocks.
A sustainable operating model to offer e-government building blocks freely can be locally rooted.
Civil servants in the HoA countries can allocate sufficient time resources to participate in the competence building.
Government institutions recognize the need to engage in cross-country communities of practice to foster the regional digital learning.
Assumptions related to Specific Objective 2
The structures created will embrace the tools made available to setup appropriate environment for an enhancement of cybersecurity.
National authorities' political will and commitment to engage in the drafting or update of their cybersecurity frameworks.
National authorities' willingness to grant access to or communicate sensitive information and documents
Availability of relevant expertise and/or point of contacts to engage in strategic discussions.
National authorities' political will and commitment to engage their staff in awareness activities
Availability and engagement of relevant participants in the workshops – among which women can be identified.
Access to relevant media is granted to promote cybersecurity hygiene.
Access to the CIRTS granted for effective estimation of the needs
Willingness of the authorities to authorise access to the said databases.
Human resources for the CSIRTs are hired and functioning budget secured.
Beneficiary countries see the added value of using and maintaining the platform to exchange relevant information.

Beneficiary countries see the added value of using the operational tools and having their staff trained to use them.

7 Monitoring, Evaluation, Reporting and Audits

A results-based monitoring system will be established to generate data on the progress of the Action on a regular basis. The monitoring tasks and responsibilities are distributed as follows between the Organisation and each Partner: each partner's project manager (EF, FI-IAPP, GIZ) is responsible for the monitoring of the activities of their component. All partners will submit their inputs to the reports according to the agreed format at the stated intervals to the Organisation's project coordinator in Bonn. The Organisation's project coordinator will compile the inputs and submit the reports to the EU.

Data will be used for programme steering as well as for annual progress reporting. All monitoring activities and plans shall be shared with the EU to strengthen joint monitoring efforts. Basis for the monitoring system is the Action's logframe with its underlying indicators for specific objectives and outputs. The logframe will be used as management tool, allowing the Organisation and Partners for adjustments and revisions at the output, activity, and indicator level to effectively achieve the expected specific objective.

Firstly, a project inception report will be prepared at the start of implementation of the project. During the inception phase (6 months), a baseline study will be carried out to feed differentiated data into the logical framework. During project implementation, a variety of tools and methods will be applied to regularly assess both quantitative and qualitative progress indicators. This includes among others gender-disaggregated participation documentation, training evaluations, tracer studies, comparative and retrospective surveys as well as focus group discussions and stakeholder consultations. Where possible, it is intended to harmonise data collection with national partners systems and present indicators disaggregated by sex, age, urban/rural, disability, any disadvantaged group, income quintile etc.

Reporting

Each report shall provide an account of all relevant aspects of the implementation of the Action for the reporting period, activities envisaged, difficulties encountered, changes introduced, as well as the degree of achievement of results as measured by corresponding indicators, using as reference the Logical Framework. The report shall be presented to allow monitoring of the objectives, the means envisaged and employed, and of the budget details of the Action. The final report, narrative and financial, will cover the entire period of the Action implementation.

The following reports will be submitted by the Organisation to the EU:

- One inception phase report (narrative)
- Two annual reports (narrative and financial) recapitulating on the progress made in the achievement of the results (outputs and outcomes); listing activities carried out during the reporting period, difficulties encountered and measures taken to overcome

problems and eventual changes introduced; providing information on the implementation of the Visibility and Communication Plan; and outlining the work plan for the coming 12 months.

- The final report shall cover the entire period of the Action, providing information on achievements of the Action, including an outlook on measures undertaken to ensure sustainability of results and further dissemination/up-scaling.

8 Communication and Visibility

GIZ, EF and FIIAPP will develop a set of suitable communication activities that relate to the different target groups and stakeholders such as project beneficiaries, implementing partners at national and sub-national level, local media and other donors and embassies. GIZ, EF and FIIAPP will consider the EU's visibility requirements as set out in the Communication and Visibility Manual for EU External Actions as well as the visibility guidelines of the German Ministry for Economic Cooperation and Development. See Annex VI "Communication and Visibility Plan" for detailed planned activities.

GIZ, EF and FIIAPP will develop a set of suitable communication activities widely promoted in the targeted countries. The activities will also stand as a communication multiplier of the previously funded projects in the region, such as The Emergency Locust Response Program, Ethiopia–Djibouti Second Power Interconnection and others. GovStack will also be used as a communication and dissemination channel of the D4D launch and its activities and future results. Regular efforts to promote and ensure visibility of the achievements of the project is also a success factor, as is the identification of potential replication opportunities of activities deemed most effective. The target groups and stakeholders of the project will be positioned at the centre of the communication activities, and the implementing partners, local media, other donors, and embassies will further disseminate the project's results.

The Communication and Visibility Plan (Annex VI) serves as basis for the communication strategy, which will be further developed during the inception phase and presented to the Steering Committee at the meeting following the end of the inception phase. A detailed communications monitoring system will allow to measure communication results and to adjust the strategies where necessary.

Appendix 1: Indicative Work Plan

The implementation period of this project starts in 01/2022 and runs until 02/2025. The project will start with an inception phase of maximum 6 months, which include the following activities (for each component):

Inception Phase
Activities
Recruitment of staff
Preparation of detailed operational plans
Establishment of a baseline monitoring system
Review Communication and Visibility Plan
Needs Assessment
Initiate country engagement
Outputs
Inception Report including operational plan and grant description
Refined Communication & Visibility Plan
Needs Assessment Report

Overall indicative work plan: 38 months implementation

Year 1

	Semester 1						Semester 2						
Activity	Month 1	2	3	4	5	6	7	8	9	10	11	12	Implementing body
Inception phase													
Recruitment of staff													GIZ, EF, FIIAPP
Preparation of detailed Operational- Plan													GIZ and FIIAPP component 1, EF component 2
Initiate country engagement													GIZ, FIIAPP, EF
Establishment of a baseline monitoring system													GIZ and FIIAPP component 1, EF component 2
Review Communication and Visibility Plan													GIZ, EF, FIIAPP
Needs Assessments													GIZ component 1, EF component 2
Digital Government 1: Strategic, Technical and Legal Evaluation of Government Services to be digitalised													

Selection of Services to be digitalised													GIZ
Requirement Analysis and Implementation Roadmap Drafting													GIZ
Digital Government 2: Local Adaptation of E-Government Building Blocks and Piloting of digital Government Services													
Design and Procurement													GIZ
Local Adaptation of Building Blocks													GIZ
Digital Government 3: Digital Government Capacity Building													
Core Digital Government Capacity Building Pro-gramme (Part I)													FIIAPP
Advanced Digital Govern-ment Capacity Building Pro-gramme (Part II)													GIZ

Establishing and managing a regional Digital Government Community of Practice CoP													GIZ
Cybersecurity 1: Strategic and Institutional Framework													
Preparedness analysis and assessment phase													EF
Draft regional cybersecurity strategy and framework													EF
Set up regional technical coordination forum (RTF)													EF
Adopt regional policy and guidelines													EF
Cybersecurity 2: Awareness and capacity building													
High level dialogues													EF
Drafting of cybersecurity training catalogue													EF
Develop model awareness campaigns													EF

Implement trainings													EF
Cybersecurity 3: Technical tools and support													
Set up of online platform for information sharing and training													EF
Create audit framework for existing C-SIRTs and infra-structure													EF
Set up national C-SIRTs in two countries													EF
Audit existing CSIRTs													EF
Create benchmark for (open source) CSIRT tooling													EF
Create model/pilot imple-mentation and tools based on benchmark.													EF

Appendix 2: Logframe Matrix

Meeting indicators on impact level will not be part of the responsibility of the Organisation and Partners. Indicators will be monitored regarding data availability. The activities expected outputs and all indicators, targets and baselines included in the logframe matrix are indicative and may be updated during the implementation of the Action in consultation with the Contracting Authority. The indicative logframe matrix will evolve during the lifetime of the Action: New lines will be added for listing the activities as well as new columns for intermediary targets (milestones) when it is relevant and for reporting purpose on the achievement of results as measured by indicators.

	Intervention logic	**Indicators**	**Baseline (incl. 2021)**	**Targets (incl. 2024)**	**Sources and means of verification**	**Assumptions**
Overall objective: Impact level	Member states of the Horn of Africa region effectively apply digital technologies towards an efficient, people-centred and harmonised digital public service delivery.	Number of harmonised policies and regulations fostering regional digital integration Number of digital services available to citizens and businesses Gains in efficiency in public service provision (financial resources, time) Number of harmonised cross-national digital procedures			National/regional statistics Data from e-government / cyber-security studies	Not applicable

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
Specific objective 1: **Outcome level** **(GIZ and FIIAPP)**	Selected Horn of Africa countries enhanced their service delivery through implementing digital government services.	SOI 1: 5 national digital government services, with a potential for regional harmonization, based on the e-government building blocks are piloted in selected member states of the Horn of Africa Initiative	0 (no systematic evaluation of digital government services in the HoA region available)	5 new government services with potential for regional harmonization piloted (02/2025)	Documentation of the piloting process per each participating institution, including description of the piloting process, achieved outcomes, learning experiences and recommendations for adaptations for the roll-out phase.	Public Sector entities in the HoA region are willing to allocate personal and financial resources to support the development of e-services based on the e-government building blocks. The sequencing approach, focusing first on national digital services and evaluating their potential for regional harmonization does not impede further HoA member states to become involved in the introduction of digital government services based on the e-government building blocks at a later stage.
		SOI 2: 20 Public Sector Units, applying the e-government building blocks, demonstrate through concrete examples, how their service delivery can improve through the application of the e-government building blocks	0 (no digital government services based on the e-government building blocks available)	20 public sector organisations confirm improvement in service delivery through concrete examples (01/2025)	Qualitative interviews with respective public officials responsible for the piloting process in 20 different public sector units, with regards to the concrete improvements in service delivery based on the digital government services.	

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
					Verification will be ensured by GIZ at the end of the intervention.	
Output 1 (GIZ)	The strategic, technical, and regulatory prerequisites to introduce government e-services in selected countries of the Horn of Africa Region are evaluated	OI 1.1: Across selected Horn of Africa countries, 5 national government e-services with a potential for regional harmonization are identified.	OI 1.1: 0 (no identification of government e-services with a potential for regional harmonization)	OI 1.1: 5 national government e-services identified (12/2022)	Evaluation of the minutes of the HoA Steering Committee Meetings with regards to the presentation of the Digital Government Strategy and the Regional Interoperability Framework, country specific remarks and objections and agreements on next steps towards implementation. Verification will be ensured by GIZ after the respective Steering Committee	Selected Member states of the HoA Initiative are willing to contribute to the technical, regulatory, and legal preparation process for the introduction of digital government services, based on the e-government building blocks. Different national priorities and levels of digital readiness do not impede the selection of digital services with a potential for regional harmonization.
		OI 1.2: 3 Implementation roadmaps for the introduction of national e-government services, including the piloting and roll-out phase, as well as possibilities for regional harmonisation, are developed with participating public sector entities from	OI 1.2: 0 (no implementation roadmaps agreed upon)	OI 1.2: 3 implementation roadmaps agreed upon with participating Ministries form selected Horn of Africa member		

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
		selected Horn of Africa member states.		states (01/2023)	Meetings (once in 2022, once in 2023)	Other actors from the private sector and civil society are willing to contribute a consultation process around the introduction of digital government services.
Output 2 (GIZ)	E-government building blocks are technically adapted for the use in selected member states of the Horn of Africa Region	OI .2.1: 5 e-government building blocks are adapted, based on the specification of local requirements with the participating public sector units in selected Horn of Africa member states.	OI 2.1: 0 (no building blocks locally adapted)	OI 2.1: 5 e-government building blocks locally adapted (12/2023)	Evaluation of the specification analysis and the outcome of the localization process for each e-government building block separately. Verification will be ensured by GIZ after the competition of the specification and localization process. Evaluation of the free accessibility of the e-government building blocks on the GovStack portal at	HoA governments are willing and able to contribute to the procurement process for mobilizing private sector support to specifying and localizing e-government building blocks. Diverging interests, priorities and needs by the different HoA member states do not impede the specification and localization of
		OI 2.2: 5 e-government building blocks are freely accessible on a regional and/or national service platform (GovStack).	OI 2.2: 0 (no regional e-government building blocks available)	OI 2.2: 5 e-government building blocks freely accessible (08/2024)		

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
					the end of implementation.	the selected e-government building blocks. A sustainable operating model to offer e-government building blocks freely can be locally rooted.
Output 3 **(GIZ and FIIAPP)**	The technical and methodological competences of civil servants in the Horn of Africa Region to implement the e-government building blocks have been strengthened	OI 3.1: 160 of 200 participants, 40% of the latter being women, participating in one of the three technical training modules on e-government building blocks, rate the training as useful.	OI 3.1: 0 (no training modules available)	OI 3.1: 160 participants rate one training as useful. (08/2024)	Evaluation of the training module curricula, as well as the accessibility to public servants, and users completing the module. Evaluation will be ensured by GIZ on a bi-yearly basis. The usefulness of the training is evaluated on a scale of 1 to 6; 1 being poor, 4 being useful and 6 being excellent.	Civil servants in the HoA countries can allocate sufficient time resources to participate in the competence building. Government institutions recognize the need to engage in cross-country communities of practice in order to foster the regional digital learning.

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
		OI 3.2 120 of 150 participants, 40% of the latter being women, participating in one of the three technical training modules on to digital change management, rate the training as useful.	OI 3.2: 0 (no training modules available)	OI 3.2: 120 participants, rate one of the trainings as useful. (08/2024)	Evaluation of the training module curricula, as well as the accessibility to public servants, and users completing the module. Evaluation will be ensured by FI-IAPP on a bi-yearly basis. The usefulness of the training is evaluated on a scale of 1 to 6; 1 being poor, 4 being useful and 6 being excellent.	
		OI 3.3: 4 cross-country communities of practice for the long-term exchange of experiences and to foster the regional digital learning have been established.	OI 3.3: 0 (no communities of practice established)	OI 3.3: 4 regional communities of practices established (09/2022)	Evaluation of the minutes of meetings of the cross-country communities of practices, with regards to topics, members and frequency of meetings. Evaluation will	

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
					be ensured by GIZ on a bi-yearly basis.	
Specific objective 2: **Outcome level** **(France(EF))**	Horn of Africa countries develop and improve national and regional cybersecurity	SOI 1: Country level of commitment in ITU's Global Cybersecurity Index SOI 2: Country score in ITU's Global Security	ITU CGI 2020 High Commitment: Medium Commitment Low Commitment	ITU CGI 2024 High Commitment: Medium Commitment Low Commitment	Global Cybersecurity Index published by ITU in year Y for the year Y-1	Democracy, political stability and economic growth improving. The HoAI countries keep benefiting from the rapid growth of ICT in all sectors of economy and public sector Commitment of the beneficiary countries to identify the relevant point of contacts and fully engage in the assessment and revision of their legal and strategic frameworks The structures created will embrace the tools made available to setup appropriate environment for an enhancement of cybersecurity.

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
Output 1 (France(EF))	Strategic and institutional cybersecurity frameworks are reinforced and converging towards shared regional standards	OI 1.1: Number of Cybersecurity National Readiness assessments conducted	0 National readiness assessments done	6 National readiness assessments done	Project update reports; Minutes of the Regional Technical Committee Kick-Off National Readiness Assessments National cybersecurity strategy documents Regional guidelines	National authorities' political will and commitment to engage in the drafting or update of their cybersecuriy frameworks. National authorities' willingness to grant access to or communicate sensitive information and documents Availability of relevant expertise and/or point of contacts to engage in strategic discussions.
		OI 1.2: Regional Technical Committee set-up	0 RTC	1 RTC		
		OI 1.3: Regional guidelines and priorities agreed upon	0 HoAI document on cybersecurity	1 HoAI document on cybersecurity		
Output 2 **(France(EF))**	Cybersecurity awareness and empowerment of stakeholders are improved to secure the internet .	OI 2.1: Number of Cybersecurity awareness workshops conducted. 25 % of the participants are women	0 awareness workshop 0 participants trained – among which 0 woman	XXX awareness workshops XXX participants trained – among	Project update reports; List of participants	National authorities' political will and commitment to engage their staff in awareness activities

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
				which XXX women (numbers to be determined during the inception phase)		Availability and engagement of relevant participants in the workshops – among which women can be identified.
		OI 2.2: Number of awareness campaigns and communication materials developed	0 awareness campaign 0 communication materials	Number of awareness campaign and communication materials to be determined during the inception phase	Project update reports; Awareness campaign's documents	Access to relevant media is granted to promote cybersecurity hygiene.
		OI 2.3: Number of Capacity-Building Trainings delivered. 25% of the participants are women	0 capacity-building training 0 participants – among	XXX capacity-building trainings XXX participants – among which	Inception phase report Project update reports	Availability and engagement of relevant participants in the workshops – among which women can be identified.

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
			which 0 woman	XXXX women (numbers to be determined during the inception phase)	List of participants	
Output 3 (France (EF))	Operational capacities to handle cybersecurity incidents are enhanced	OI 3.1: Number of CSIRTs set up or equipped according to the conclusions of the national audits.	4 existing CSIRT in 6 countries	XXX CSIRTS in countries (numbers to be determined during the inception phase	Inception phase report Project update reports; CSIRTs reports	Access to the CIRTS granted for effective estimation of the needs Willingness of the authorities to authorise access to the said databases. Human resources for the CSIRTs are hired and functioning budget secured. Adoption and use of the tools made available
		OI 3.2 Platform set up	0 platform	1 platform	Report on the launch of the platform	Beneficiary countries see the added-valued

	Intervention logic	Indicators	Baseline (incl. 2021)	Targets (incl. 2024)	Sources and means of verification	Assumptions
						of using and maintaining the platform to exchange relevant information.
		OI 3.3: Operational tools feasibility assessed	0 feasibility studies	1 feasibility study Pilot phase according to the results of the feasibility study	Inception phase report incl. feasibility study Project update reports	Beneficiary countries see the added-valued of using the operational tools and having their staff trained to use them.