Co-funded by the European Union

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

EXPERTISE FRANCE GROUPE AFD

FIIAPP COOPERACIÓN ESPAÑOLA

Initiative for Digital Government and Cybersecurity (IDGC)

Background

The Digital for Development (D4D) Hub is a strategic multi-stakeholder platform that promotes and aligns new international partnerships on digital transformation between the European Union (EU) and partner countries for example in Africa, Asia, Latin America.

As part of the activities of the Digital for Development (D4D) Hub, the EU is collaborating with the Germany, the Horn of Africa Initiative (HoAI), Expertise France (EF) and the International and Ibero-American Foundation for Administration and Public Policies (FIIAPP).

The Horn of Africa Initiative (HoAI) was launched in October 2019 by the governments of Somalia, Djibouti, Kenya, Ethiopia, and Eritrea to identify and harmonise regional approaches that address common challenges in the region. The seven present member states of the Initiative including Sudan (joined in May 2021) and South Sudan as the newest member (joined in May 2022) 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.

Project name	D4D Initiative for Digital Government and Cybersecurity (IDGC) for the Horn of Africa Initiative
Commissioned by	European Union (EU), Federal Ministry of Economic Cooperation and Development (BMZ)
Executing agency	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Expertise France (EF) and International and Ibero-American Foundation for Administration and Public Policies (FIIAPP)
Partner countries	Kenya, Somalia, Djibouti
Duration	01/2022 - 03/2025

Objective

The Multi Donor Project “Initiative for Digital Government and Cybersecurity” (IDGC) is jointly co-financed by the European Union and the Federal Ministry for Economic Cooperation and Development (BMZ). It aims to support selected member states of the Horn of Africa region, specifically Kenya, Somalia, and Djibouti, to enhance their public sector service delivery through improved and secure digital delivery channels. While the Gesellschaft für Internationale Zusammenarbeit (GIZ) and the International and Ibero-American Foundation for Administration and Public Policies (FIIAPP) are leading the effort on e-government, Expertise France (EF) focuses on cybersecurity.

Digital Government Component

The component on digital government will include the following three actions areas and key activities:

- **Digital Government Strategy and Roadmap:**
  Evaluation of the strategic, technical, and regulatory prerequisites to introduce government e-services, through the implementation of a digital readiness study and roadmap development for the introduction of government e-services.

- **Service Design of e-government Use Case:**
  Use case selection and design of priority digital public services based on the GovStack building block approach to the digitization of government services.

- **Capacity Development**:
  Capacity development measures on digital government and change management, including on- and offline trainings and workshops, for civil servants for the digitization of government services; regional and global communities of practice for peer-to-peer learning.

Core partners of the GovStack Initiative provide technical support to the digital government component. Each partner represents a different part of the digital ecosystem and will support the action with special competency. The International Telecommunication Union (ITU) supports the technical service design of priority use cases. The Estonian Centre for International Development (EstDev) supports the development of Digital Readiness Studies and Digital Government Roadmaps. The Digital Impact Alliance (DIAL) and FIIAPP support the work around capacity strengthening by setting up Communities of Practice and by developing capacity development measures.

Approach – GovStack

The above-mentioned activities which aim to support governments to enhance their public sector service delivery are based on the GovStack approach. Launched by Estonia, Germany, ITU and DIAL in 2020, the GovStack Initiative – together with partners such as Smart Africa, the World Bank, GSMA and SAP – aims to create a common framework and technical practice for developing reusable and interoperable digital components – so-called “digital building blocks” – needed for the digital transformation of governments.

The global GovStack community invests in digital building blocks that help governments reduce costs, time, and resources required to create or modify digital platforms, services, and applications. As these digital building blocks are interoperable and based on open-source software, they are easier to customize, design and implement, combine as needed, and scale across multiple sectors.

Examples of digital building blocks are:

- Digital registries
- Identification and authentication
- Payments
- Registration
- Security

In addition, GovStack supports partner governments in making their digital administration more efficient, faster, and more secure to reduce system duplication. By increasing the security and traceability of transactions and improving accountability, the aim is to prevent fraud and corruption. GovStack aims to increase country ownership of e-government solutions and digital sovereignty to improve social well-being services. Through the involvement of civil society and academia, human rights risks (such as lack of data protection or IT security) are reduced.

Finally, the GovStack Initiative is creating a model platform for digital government services that identifies elements that can be reused across services and sectors (i.e., use cases) – building on DIAL's Catalogue of Digital Solutions. The specifications and the derived model platform are intended to be openly accessible, as digital public goods (DPG).

Cybersecurity Component

The cybersecurity component includes the following three action areas and key activities that will be implemented by Expertise France:

- **Institutional framework**:
  Promotion, design and adoption of regional guidelines and national cybersecurity strategies based on international best practices on security and information systems. This aims towards a common comprehensive understanding of cybersecurity and the protection and increased resilience of critical information infrastructures.

- **Awareness and capacity building:**
  Based on high-level dialogue, support of national campaign awareness on cybersecurity, specialised trainings for IT professional and digital hygiene for public at large.

- **Technical tools and support:**
  Supporting knowledge platform, national C-SIRT in member states and introduction of monitoring tools and systems to enhance capacities to handle cybersecurity incidents, in order to secure and maintain the services and infrastructures that are vital to national security and economic growth.

The cybersecurity approach, developed through consultations with all relevant actors prioritises, support based on country needs and aim to align the countries' cybersecurity strategies with the EU's cybersecurity strategy by encouraging countries to comply with international standards. To address potential gaps and help operationalise and implement the cybersecurity strategies, comprehensive cybersecurity capacity strengthening in the HoA region will be offered as part of this Component. Capacity Strengthening activities are based on the national cybersecurity readiness of the three partner countries.

The cybersecurity component focuses on the regional and national level:

Regional level:

- The focus is on providing a common base (methodology, approach and tools) for all country action plans and activities.
- The action plan seeks to promote harmonisation and cooperation between countries, and thus provide specific regional activities.
- A regional technical committee (RTC) maintains the regional approach in the implementation of actions and ensures alignment with the countries' cybersecurity priorities.

National level:

- The activities at country level are based on a situation analysis conducted at the beginning of the project and support countries in meeting the identified needs.

Contact

Digital Government Component:

- Siri Snow: Project Coordinator Digital Government IDGC (GIZ) (siri.snow@giz.de)
- Christin Schulz-Kaunga: Project Manager Digital Government Component IDGC (GIZ) (christin.schulz@giz.de)
- Víctor Martínez Pavón: Project Manager Change Management IDGC (FIIAPP) (victor.martinez@fiiapp.es)

Cybersecurity Component:

- Emilie Ong: Project Coordinator Cybersecurity Component IDGC (EF) (emilie.ong@expertisefrance.fr)

Published by	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Expertise France (EF) and International and Ibero-American Foundation for Administration and Public Policies (FIIAPP)
As at	February 2023
On behalf of	The European Union and the German Federal Ministry of Economic Cooperation and Development (BMZ)

This publication was co-funded by the EU and the BMZ. Its contents are the sole responsibility of GIZ, EF and FIIAPP and do not necessarily reflect the views of the EU or the BMZ.