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

HORN OF AFRICA INITIATIVE

HoAI - Digital Technical Workshop under DIGITAL Integration (Pillar 1)

23.03.2022

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

1

PROJECT OVERVIEW

Project Overview

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

Volume: 11 Mio funded by EU and the German Federal Ministry of Economic Cooperation and Development

Duration: 01/2022 - 03/2025, Inception Phase: 01/2022 - 06/2022

Project Partners: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Expertise France (EF) & International and Ibero-American Foundation for Administration and Public Policies (FIIAPP)

Objective: 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.

Components:

1. Digital Government (GIZ/FIIAPP)
2. Cybersecurity (EF)

Partner Countries: Djibouti, Kenya, Somalia, Ethiopia (*component 2*)

2

DIGITAL GOVERNMENT

(COMPONENT 1)

Component 1 Digital Government

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

Objective: Support selected Horn of Africa countries to enhance their digital service delivery through implementing digital government services

Project Partners:

- GIZ
- FIIAPP

Implementing Partners: Digital Impact Alliance (DIAL), International Telecommunication Union (ITU), Estonian Centre for International Development (ESTDEV)

Approach: GovStack – Building Block approach to the digitization of government services:

- Interoperable, reusable building blocks: **GovStack**
- Easy customization, design and implementation
- Reduce **cost, time, and resources** required to create and modify digital services

Component 1 Digital Government

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

Strategy

Digital Government strategy and roadmap development
Evaluation of the strategic, technical and regulatory prerequisites to introduce government e-services.

Technical Design

Technical specification and design of e-government service use case
Technical design and proof of concept on how a use case could be implemented using the building block approach.

Capacity Strengthening

Capacity strengthening for digital government
Strengthen the technical and methodological skills of civil servants to implement e-government services

Component 1 Digital Government

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

Digital Government Strategy and Roadmap Development: Evaluation of the strategic, technical and regulatory prerequisites to introduce government e-services.

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Action Area 1 Activities

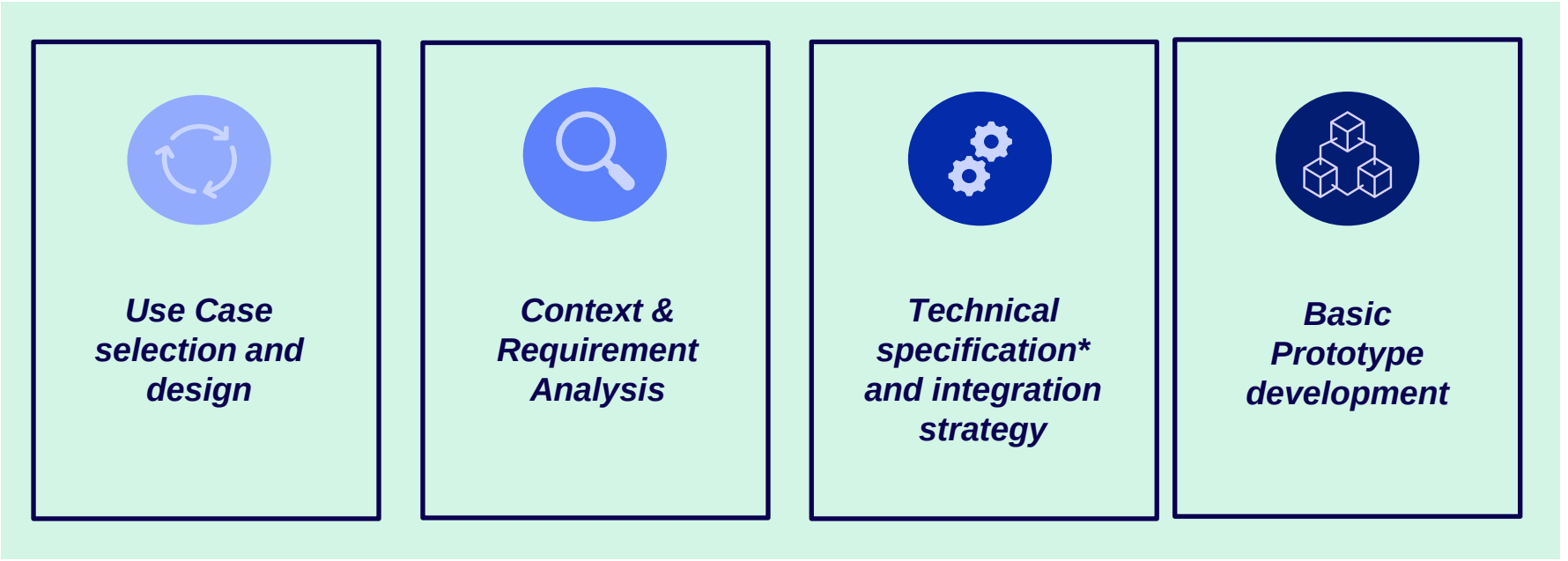
Component 1 Digital Government

Technical specification and design of e-government service use case:

Technical design and proof of concept on how a use case could be implemented using the building block approach.

Implemented by giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Action Area 2:
Activities



*Specifications = e.g., regulatory and technical requirements / standards

Component 1 Digital Government

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

Capacity Strengthening: Strengthen the technical and methodological skills of civil servants to digitize government services

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

FIIAPP COOPERACIÓN ESPAÑOLA

Action Area 3: Activities

- ***Comstumization of Capacity Development Plan***
- ***Training on e-government building blocks***
- ***Training on change management***
- ***Communities of Practice***

3

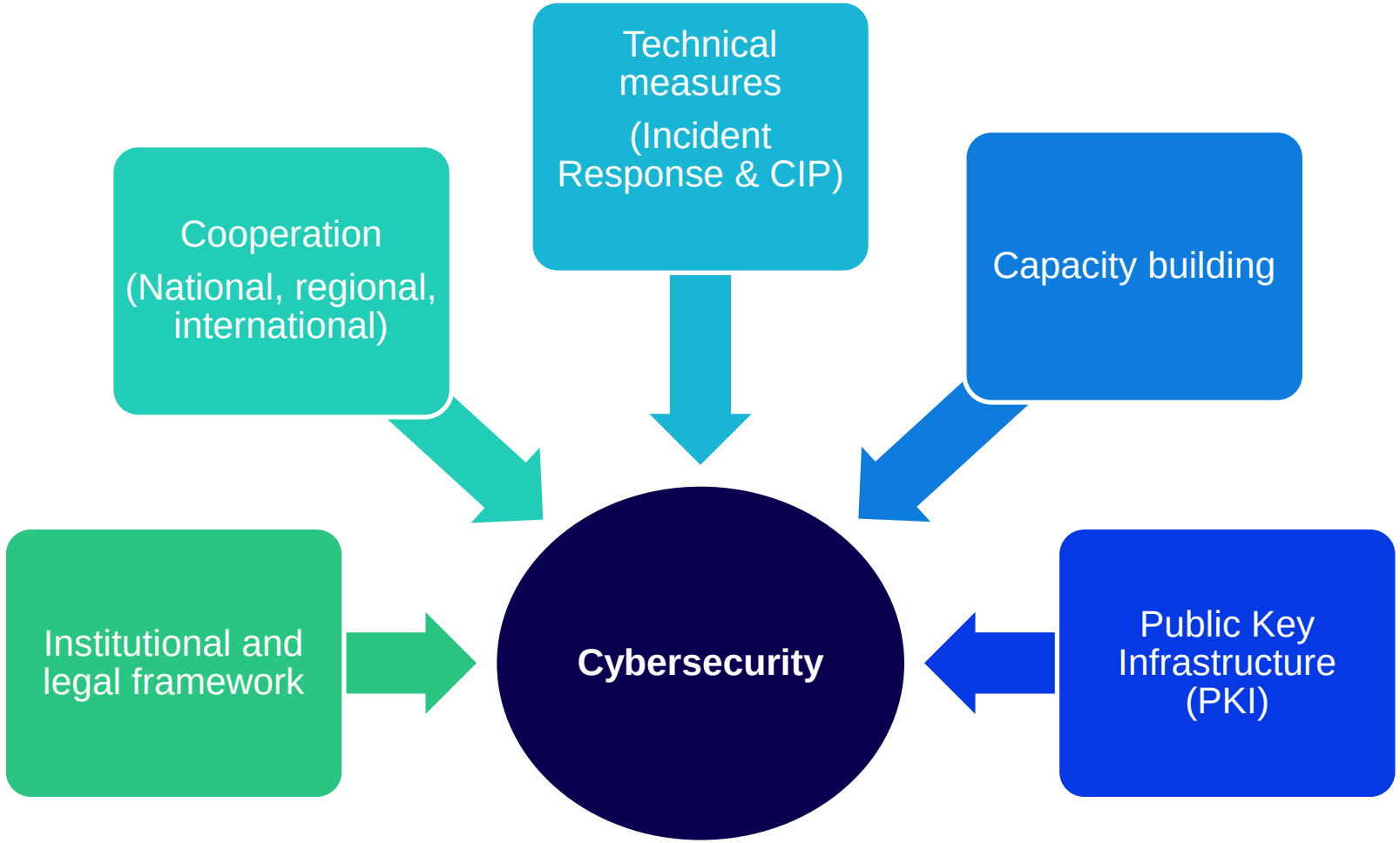
CYBERSECURITY

(Component 2)

Cybersecurity dimensions

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

EXPERTISE FRANCE
GROUPE AFD



Component 2 Cybersecurity

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

Specific objective 2:
Horn of Africa countries develop and improve national and regional cybersecurity

EXPERTISE FRANCE
GROUPE AFD

Output 1 : STRATEGIC AND INSTITUTIONAL FRAMEWORK	**Strategic and institutional cybersecurity frameworks** are reinforced and converging towards shared regional standards
Output 2: AWARENESS AND CAPACITY BUILDING	**Cybersecurity awareness and capacities** of government officials and IT professionals as well as the general public are strengthened
Output 3: TECHNICAL TOOLS AND SUPPORT	Operational capacities to **handle cybersecurity incidents** are enhanced

Component 2 Cybersecurity

OUTPUT 1 : STRATEGIC AND INSTITUTIONAL FRAMEWORK

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

DEFINITION OF A STRATEGIC AND INSTITUTIONAL FRAMEWORK IN INTERNATIONAL AND REGIONAL COOPERATION IN CYBERSECURITY

To increase the global resilience and security of national ICT assets, which support critical functions of the state or of the society as a whole, the project will support the promotion, the design and the adoption of regional guidelines and national cybersecurity strategies. These strategies should aim to converge towards a common comprehensive understanding of cybersecurity and the protection and increased resilience of critical information infrastructures.

A1: CONDUCT NATIONAL READINESS ASSESSMENTS

A2: SETUP A REGIONAL TECHNICAL COMMITTEE (RTC)

A3: DESIGN REGIONAL GUIDELINES IN ALIGNMENT WITH INTERNATIONAL BEST PRACTICES ON SECURITY OF NETWORKS AND INFORMATION SYSTEMS

- **Established forum network and events that convene cybersecurity community**
- **Regional guidelines are available for countries to use**
- **Countries have plans to implement regional guidelines**

Timeline: 24 months

Component 2 Cybersecurity
OUTPUT 2 : AWARENESS AND CAPACITY BUILDING

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

STRENGTHEN AWARENESS AND SKILLS ON KEY CYBERSECURITY ISSUES

In efforts to enhance cybersecurity, human resource is the most important actor success. It is important that citizens at large, decision makers and cybersecurity professionals, each at their own level, take responsibility and act accordingly.

- **A1. HIGH-LEVEL DIALOGUE ON CYBERSECURITY STAKES**
- **A2. DIGITAL HYGIENE AWARENESS AT LARGE**
- **A3. PROFESSIONAL TRAINING**

- **Decision makers champion cybersecurity activities**
- **Digital governance initiatives in member states have mainstreamed cybersecurity**

Timeline: 30 months

Component 2 Cybersecurity

OUTPUT 3 : TECHNICAL TOOLS AND SUPPORT

D4D Collaboration for the HoAI on Digital Government and Cybersecurity

PROVIDE ADEQUATE REGIONAL RESSOURCES FOR IMPLEMENTATION AT NATIONAL LEVEL

Technical measures are provided to technical institutions and frameworks dealing with cybersecurity, meant to enhance cybersecurity, to reduce vulnerability and to detect and respond to cyberattacks.
Operating a CSIRT forms a core component of a country's overall strategy to secure and maintain the services and infrastructures that are vital to national security and economic growth.

A1. SET-UP A REGIONAL KNOWLEDGE PLATFORM

A2. IMPLEMENTATION OF A NATIONAL C-SIRT IN MEMBER STATES

A3. INTRODUCTION OF MONITORING TOOLS AND SYSTEMS

- **Established mechanisms of information sharing is operational**
- **A National CSIRT is set up in at least one country**
- **Monitoring tools and systems are up and active.**

Timeline: 24 months