Cybersecurity development Areas of action - an overview

Farid Nakhli
Programme Officer, ITU Regional Office for CIS

BDT Cybersecurity Mandate

Enhancing security and building confidence in the use of ICTs is one of the priority domains for Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference.

ITU Plenipotentiary Conference (PP):

Resolution 130 (Rev. Dubai 2018) "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies"

Resolution 174 (Busan 2014) "ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies"

Resolution 179 (Rev. Dubai 2018) "ITU's role in child online protection"

ITU World Telecommunication Development Conference (WTDC):

Resolution 45 (Dubai 2014) "Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam“

Resolution 67 (Buenos Aires 2017) "The role of the ITU Telecommunication Development Sector in child online protection"

Resolution 69 (Buenos Aires 2017) "Facilitating creation of national computer incident response teams, particularly for developing countries, and cooperation between them"

ITU World Telecommunication Standardization Assembly (WTSA):

Resolution 50 (Hammamet 2016) "Cybersecurity“

Resolution 52 (Hammamet 2016) "Countering and combating spam“

Resolution 58 (Dubai 2012) "Encourage the creation of national computer incident response teams, particularly for developing countries"

Related Study Group :

ITU-D STUDY GROUP 2 (2018 - 2021): Question 3/2: "Securing information and communication networks: Best practices for developing a culture of cybersecurity"

Expected Results – Outlined @ WTDC 2017

Objective 2: Modern and secure telecommunication/ICT Infrastructure: Foster the development of infrastructure and services, including **building confidence and security in the use of telecommunications/ICTs**

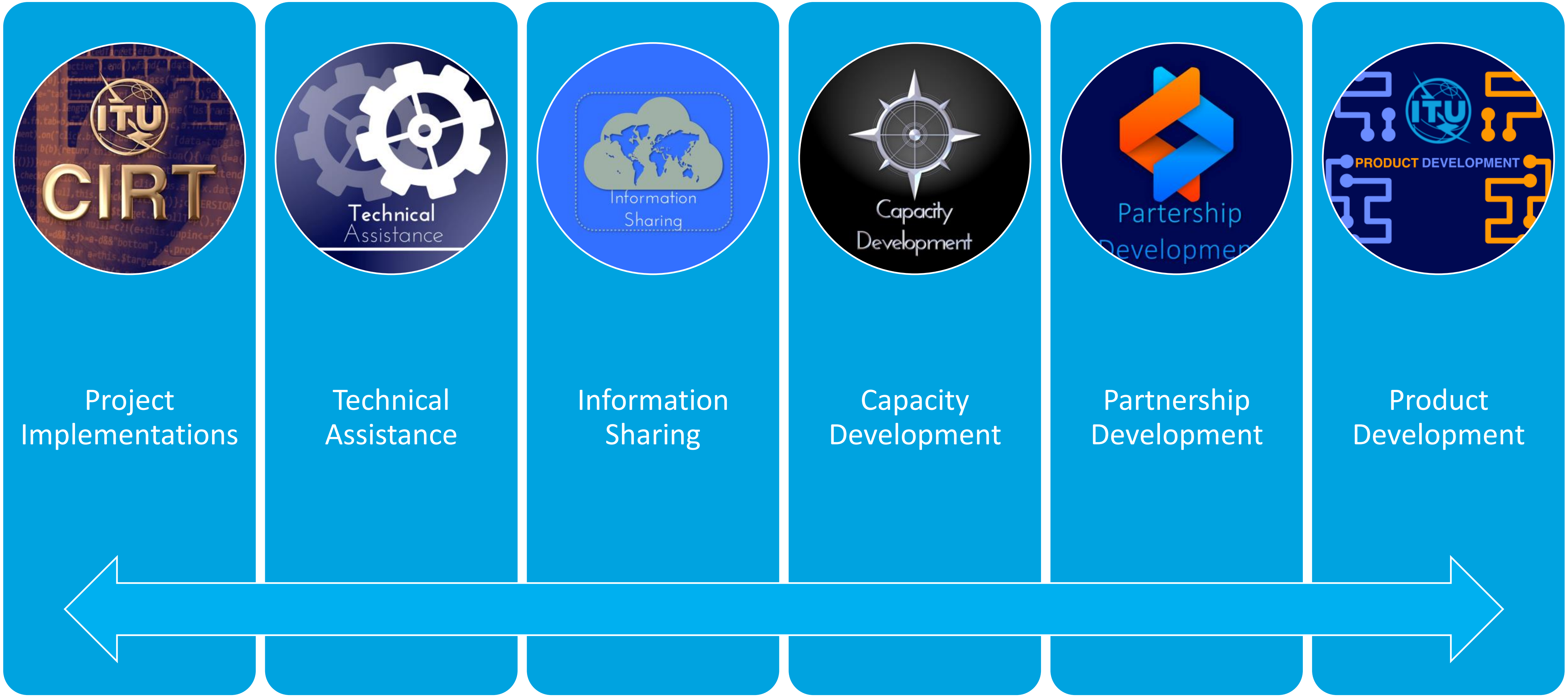
Outcomes 2.2: Strengthened **capacity** of Member States to effectively **share information**, find **solutions**, and **respond to threats** to cybersecurity, and to develop and implement **national strategies** and **capabilities**, including **capacity building**, encouraging national, regional and international **cooperation** towards enhanced engagement among Member States and relevant players

Output 2.2: Products and **services** for **building confidence and security** in the use of telecommunications/ICTs, such as **reports and publications**, and for **contributing to the implementation of national and global initiatives**

Expected Key Performance Indicators:

- Number of cybersecurity national strategies implemented in countries that BDT contributed to develop
- Number of CERTs that BDT has contributed to establish
- Number of countries where BDT provided technical assistance and improved cybersecurity capability and awareness
- Number of cyber attacks repelled by CERTs established with the support of BDT

Implementation Mechanisms



Project Implementations

Technical Assistance

Information Sharing

Capacity Development

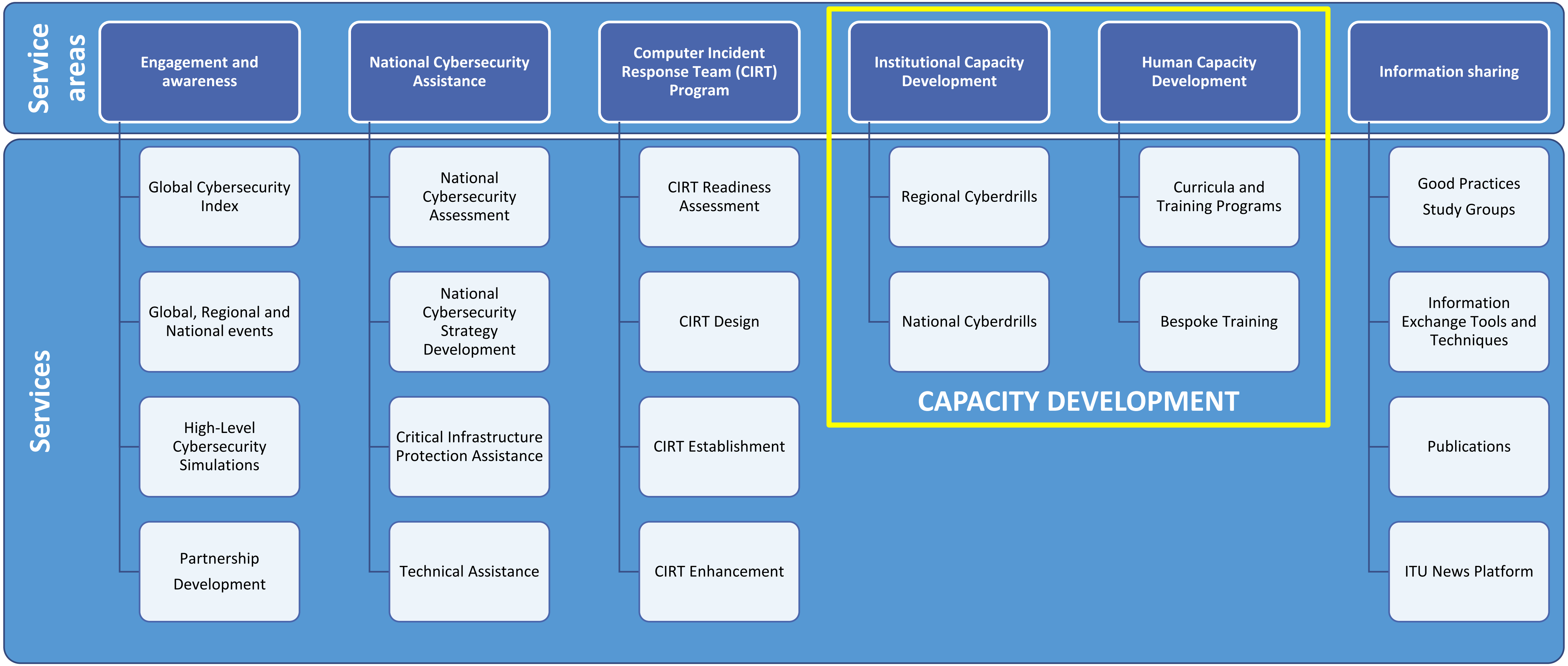
Partnership Development

Product Development

BDT Cybersecurity

Services Focus Areas

Cybersecurity Services Catalogue



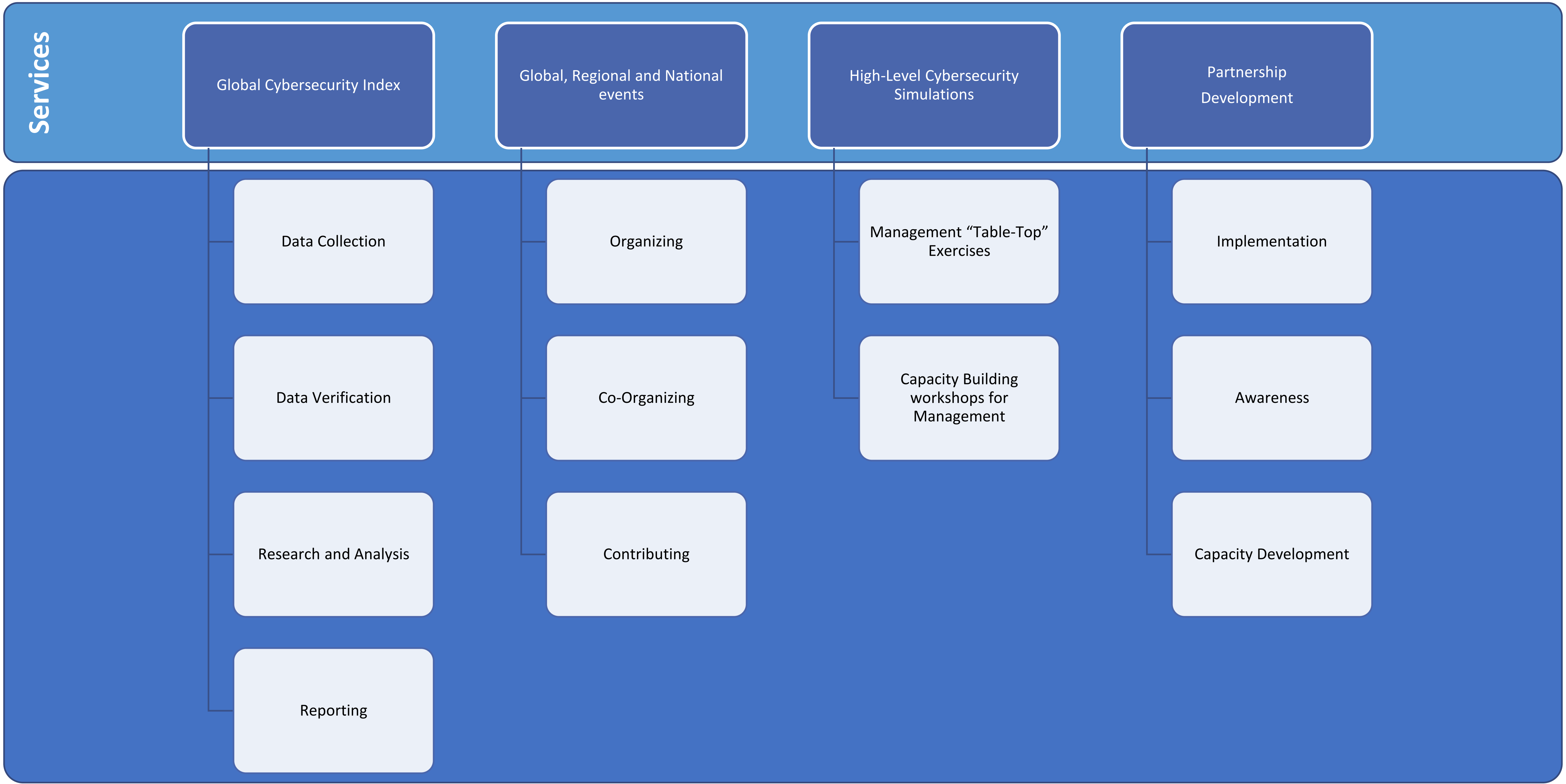
Service areas

Services

- **Engagement and awareness**
  - Global Cybersecurity Index
  - Global, Regional and National events
  - High-Level Cybersecurity Simulations
  - Partnership Development
- **National Cybersecurity Assistance**
  - National Cybersecurity Assessment
  - National Cybersecurity Strategy Development
  - Critical Infrastructure Protection Assistance
  - Technical Assistance
- **Computer Incident Response Team (CIRT) Program**
  - CIRT Readiness Assessment
  - CIRT Design
  - CIRT Establishment
  - CIRT Enhancement
- **Institutional Capacity Development**
  - Regional Cyberdrills
  - National Cyberdrills
- **Human Capacity Development**
  - Curricula and Training Programs
  - Bespoke Training
- **Information sharing**
  - Good Practices Study Groups
  - Information Exchange Tools and Techniques
  - Publications
  - ITU News Platform

CAPACITY DEVELOPMENT

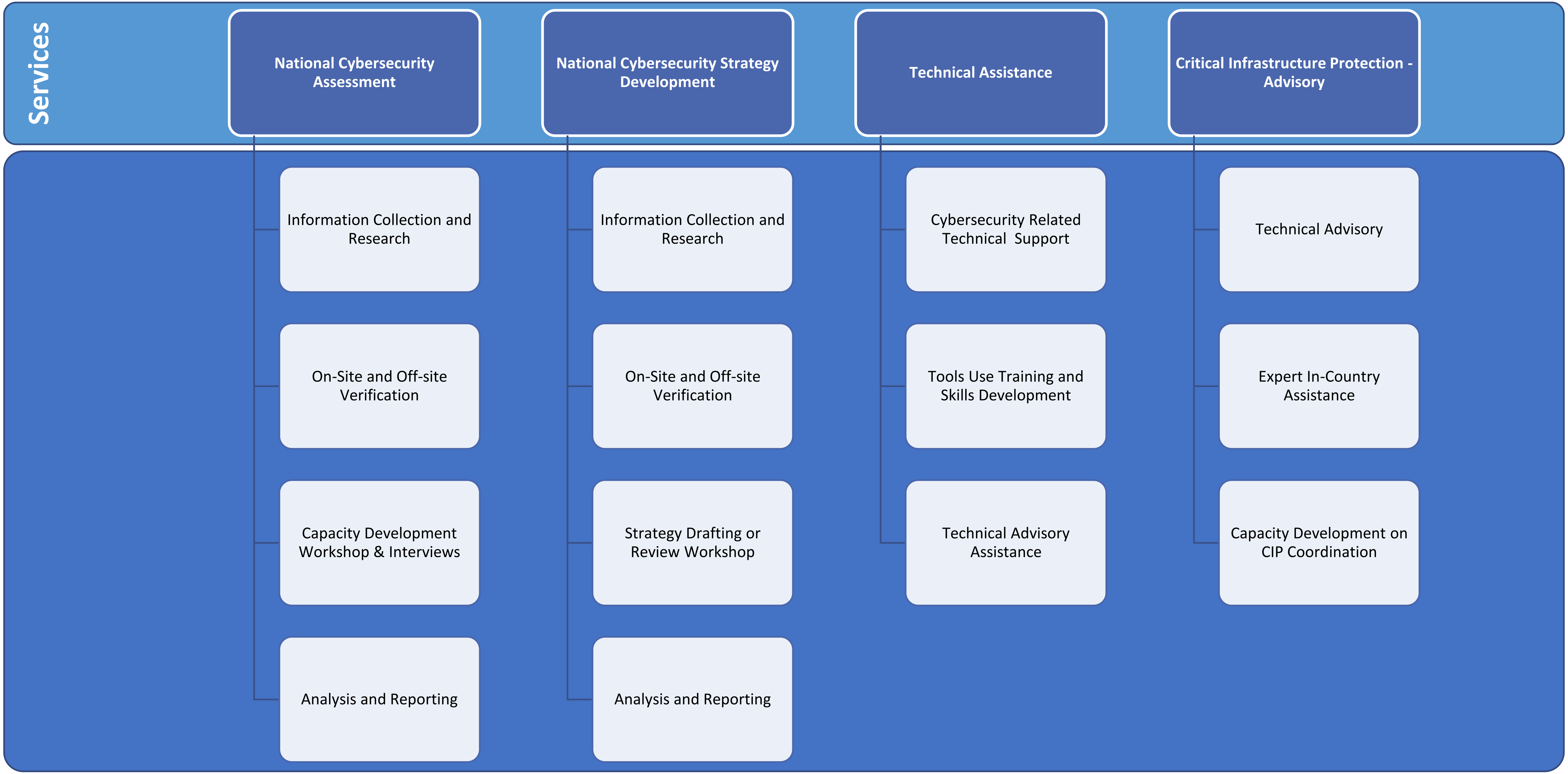
Engagement and Awareness



Services

- Global Cybersecurity Index
  - Data Collection
  - Data Verification
  - Research and Analysis
  - Reporting
- Global, Regional and National events
  - Organizing
  - Co-Organizing
  - Contributing
- High-Level Cybersecurity Simulations
  - Management “Table-Top” Exercises
  - Capacity Building workshops for Management
- Partnership Development
  - Implementation
  - Awareness
  - Capacity Development

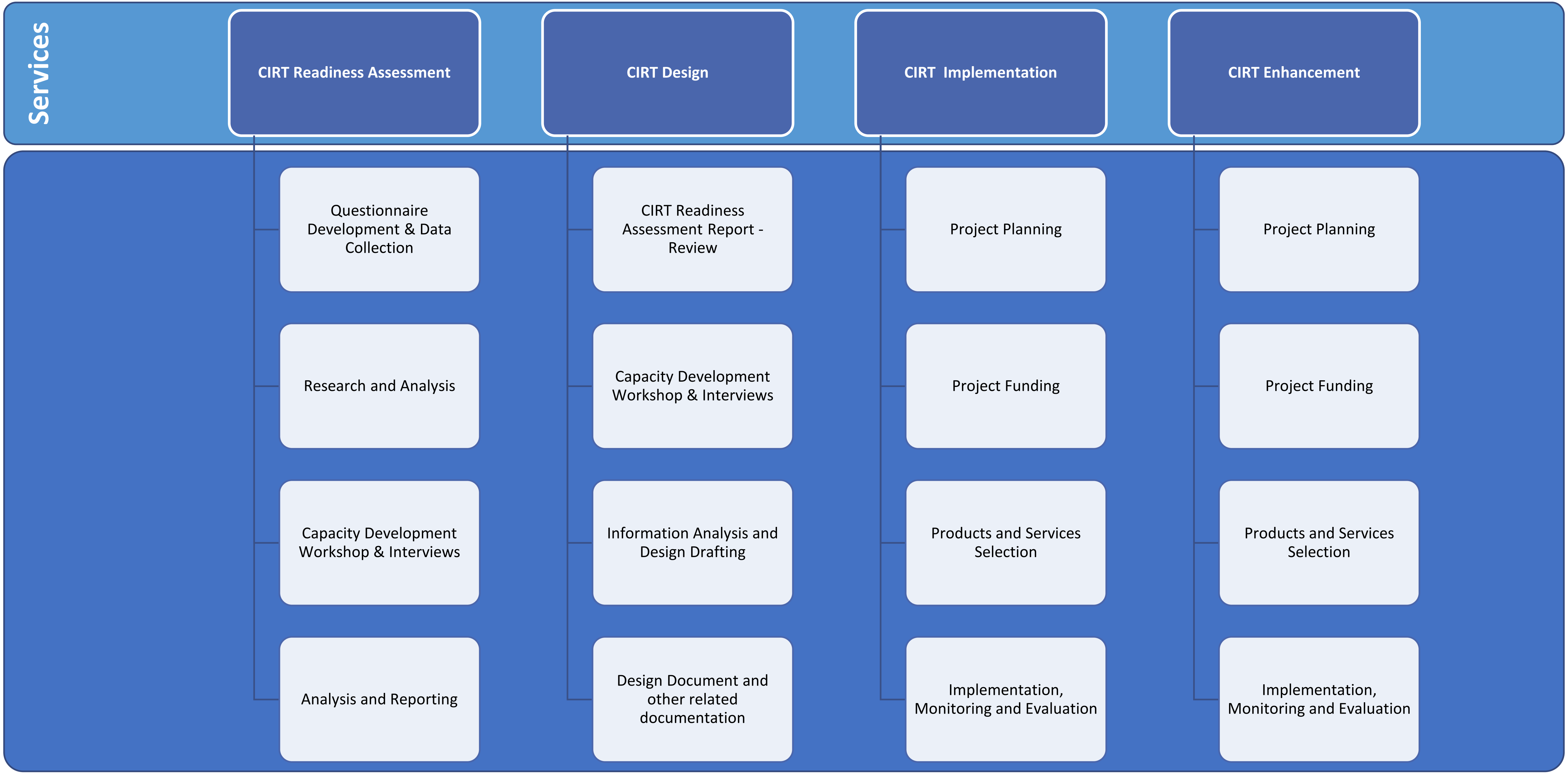
National Cybersecurity Assistance



Services

- National Cybersecurity Assessment
  - Information Collection and Research
  - On-Site and Off-site Verification
  - Capacity Development Workshop & Interviews
  - Analysis and Reporting
- National Cybersecurity Strategy Development
  - Information Collection and Research
  - On-Site and Off-site Verification
  - Strategy Drafting or Review Workshop
  - Analysis and Reporting
- Technical Assistance
  - Cybersecurity Related Technical Support
  - Tools Use Training and Skills Development
  - Technical Advisory Assistance
- Critical Infrastructure Protection - Advisory
  - Technical Advisory
  - Expert In-Country Assistance
  - Capacity Development on CIP Coordination

Computer Incident Response Team (CIRT) Program



Services

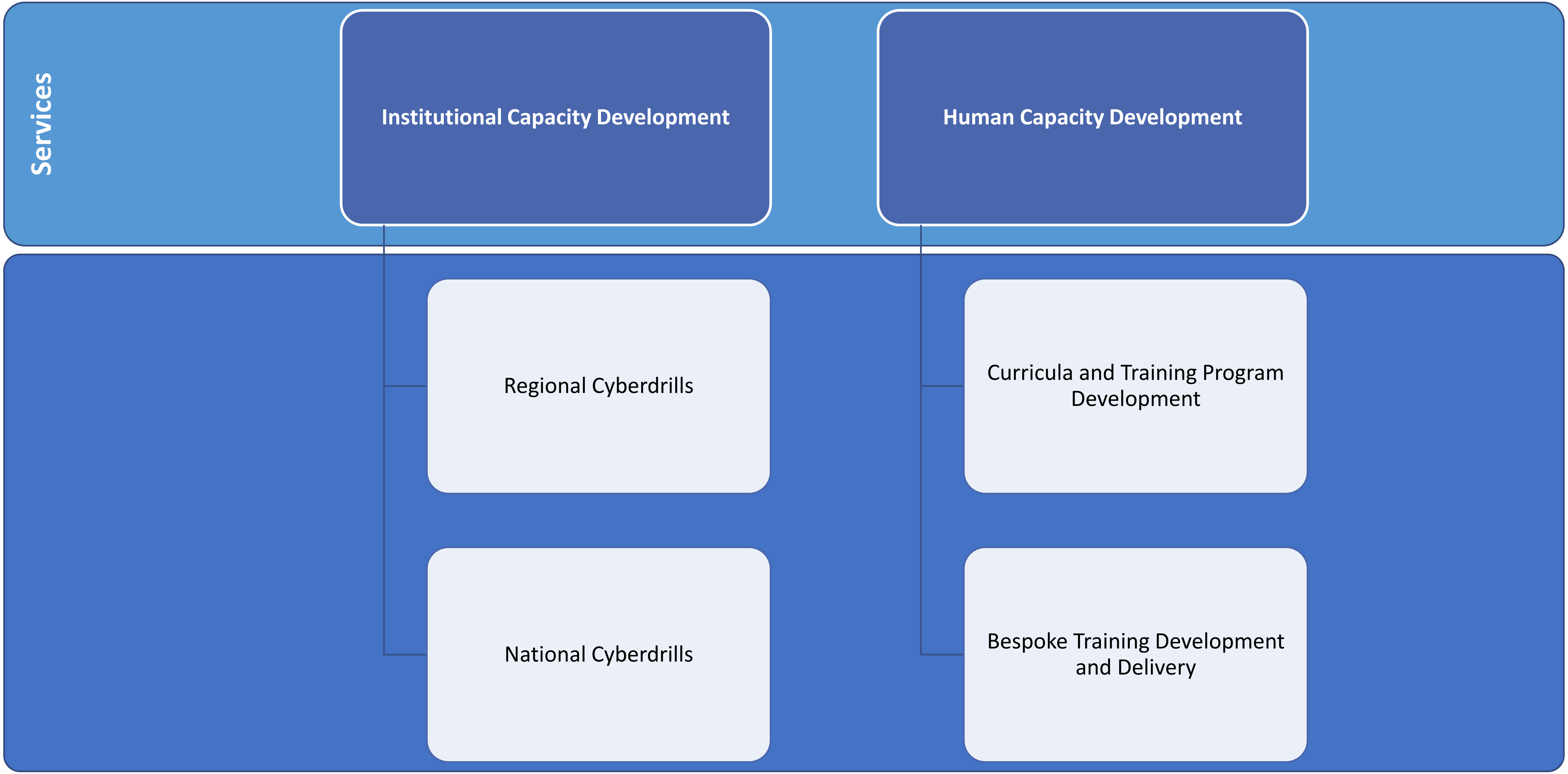
CIRT Readiness Assessment
- Questionnaire Development & Data Collection
- Research and Analysis
- Capacity Development Workshop & Interviews
- Analysis and Reporting

CIRT Design
- CIRT Readiness Assessment Report - Review
- Capacity Development Workshop & Interviews
- Information Analysis and Design Drafting
- Design Document and other related documentation

CIRT Implementation
- Project Planning
- Project Funding
- Products and Services Selection
- Implementation, Monitoring and Evaluation

CIRT Enhancement
- Project Planning
- Project Funding
- Products and Services Selection
- Implementation, Monitoring and Evaluation

Human and Institutional Capacity Development



Services

Institutional Capacity Development

Regional Cyberdrills

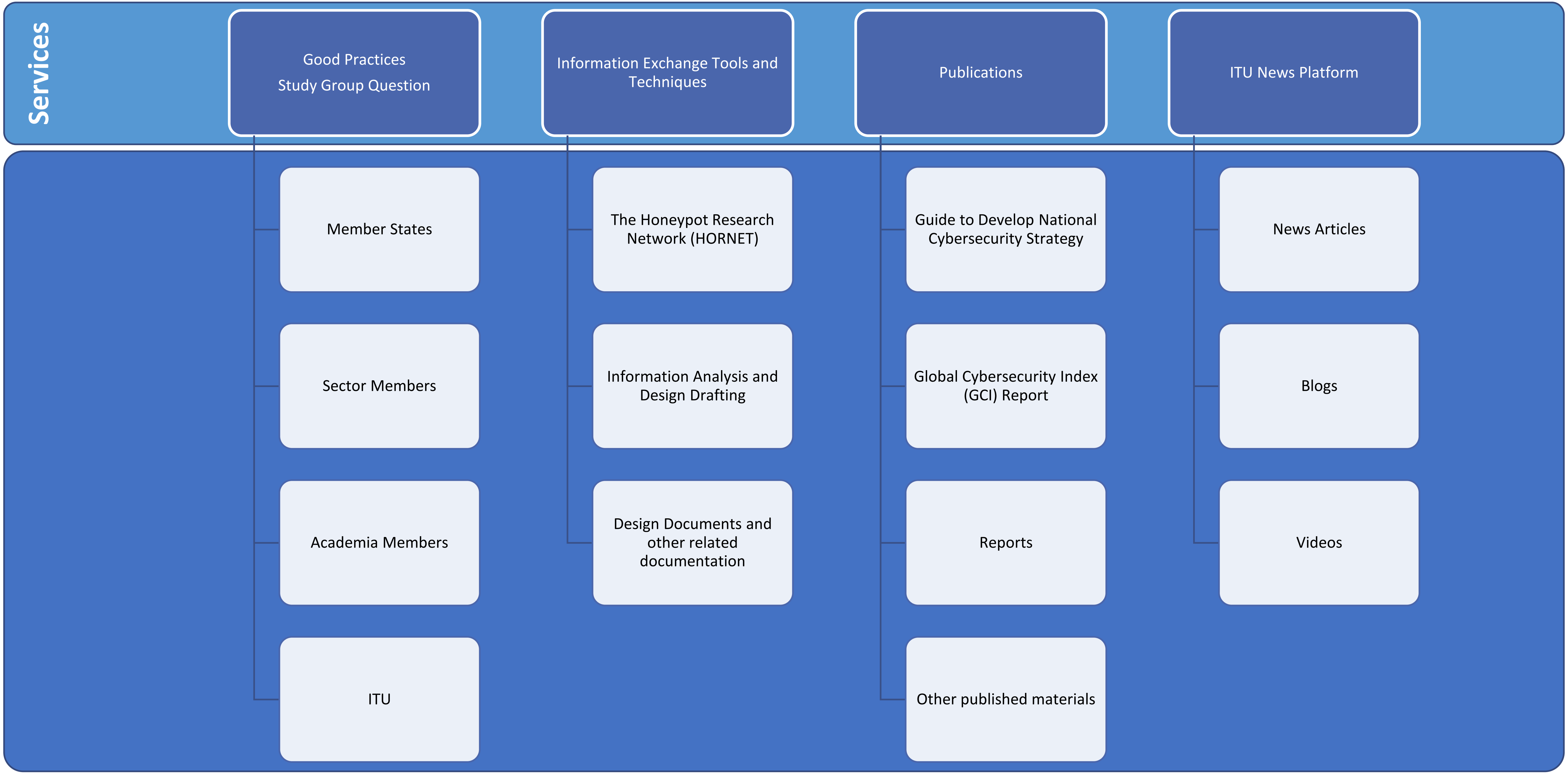
National Cyberdrills

Human Capacity Development

Curricula and Training Program Development

Bespoke Training Development and Delivery

Information Sharing



Services

Good Practices
Study Group Question

- Member States
- Sector Members
- Academia Members
- ITU

Information Exchange Tools and Techniques

- The Honeypot Research Network (HORNET)
- Information Analysis and Design Drafting
- Design Documents and other related documentation

Publications

- Guide to Develop National Cybersecurity Strategy
- Global Cybersecurity Index (GCI) Report
- Reports
- Other published materials

ITU News Platform

- News Articles
- Blogs
- Videos

Global Cybersecurity Index

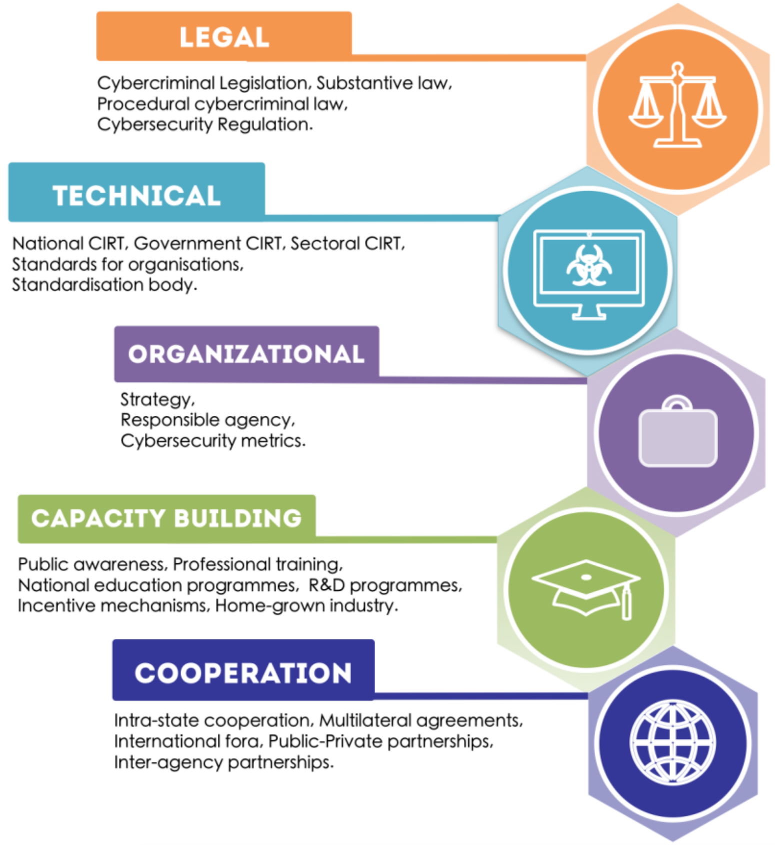
Global Cybersecurity Index - Background

- GCIv1 – the 1st iteration of the GCI has started in 2013-2014 period -**105** countries responded
- GCIv2 – the 2nd iteration covered 2016-2017 period – **134** countries responded
- **GCIv3 – 3rd iteration soon to be published** – **155** countries responded

- **All iterations include primary research in order to provide global coverage of the 194 Member States**

Global Cybersecurity Index - Goals

- Help countries identify areas for improvement
- Motivate action to improve relative GCI rankings
- Raise the level of cybersecurity worldwide
- Help to identify and promote best practices
- Foster a global culture of cybersecurity



LEGAL

Cybercriminal Legislation, Substantive law, Procedural cybercriminal law, Cybersecurity Regulation.

TECHNICAL

National CIRT, Government CIRT, Sectoral CIRT, Standards for organisations, Standardisation body.

ORGANIZATIONAL

Strategy, Responsible agency, Cybersecurity metrics.

CAPACITY BUILDING

Public awareness, Professional training, National education programmes, R&D programmes, Incentive mechanisms, Home-grown industry.

COOPERATION

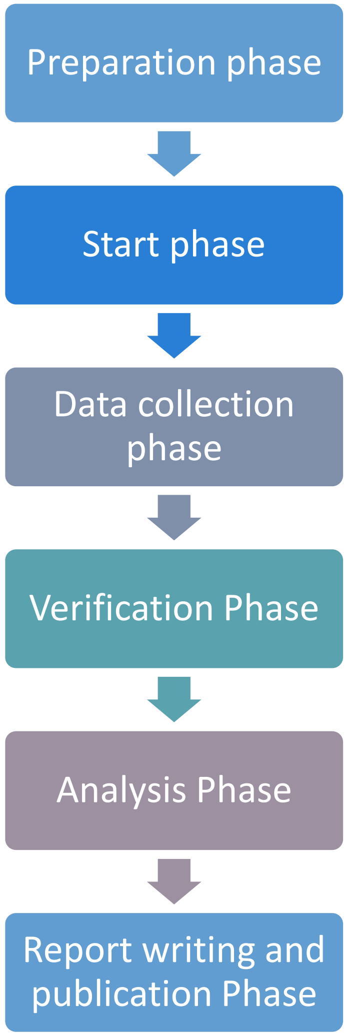
Intra-state cooperation, Multilateral agreements, International fora, Public-Private partnerships, Inter-agency partnerships.

Global Cybersecurity Index

The GCIv3 includes 25 indicators and 50 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

- Relevance to the five GCA (Global Cybersecurity Agenda) pillars and in contributing towards the main GCI objectives and conceptual framework;
- Data availability and quality;
- Possibility of cross verification through secondary data.

Global Cybersecurity Index - Phases



Preparation phase

Start phase

Data collection phase

Verification Phase

Analysis Phase

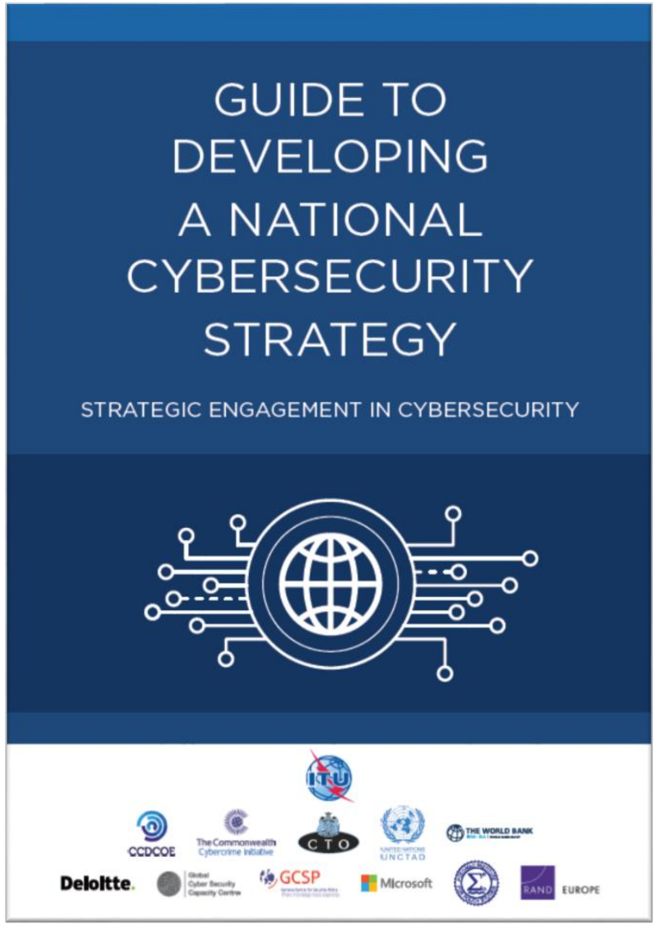
Report writing and publication Phase

- Preparation phase
  - Elaboration of the survey in collaboration with experts an partners
  - Development of online survey system
  - Preparation of supporting documentation (guides, conceptual framework, letters etc.)
  - Announcement on the ITU website
- Start phase
  - Informing/inviting Member States via official letter from the BDT Director to Administrations (Responsible Ministry, organization, agency…)
  - Collection of contact details of Focal Point(s) assigned by each Administration
  - Contacting FPs and providing access to the online survey, together with all necessary documents and instructions
  - Technical Support
- Data collection phase
  - Filling the questionnaire (FPs provide data, links, supporting documents etc.)
  - Collection of data from open sources for non-respondents (ITU helps Member States to appear in the Report)
- Verification Phase
  - ITU specialists verify and all provided data and contact FPs for more details if needed.
  - ITU shares the verified data with FPs
- Analysis Phase
  - Analysis of all collected data (for respondents and non-respondents).
  - Ranking. Preparation of comparison charts, maps, tables and other statistical elements.
  - Illustrative practices extraction.
- Report writing and publication Phase
  - Elaboration of the GCI Report
  - Publication on the ITU website and printing
  - Official launch and informing Member States
  - Follow-up

National Cybersecurity Assistance

National Cybersecurity Strategy (NCS)

This Guide has primarily been structured as a resource to help government stakeholders in preparing and reviewing their National Cybersecurity Strategy.

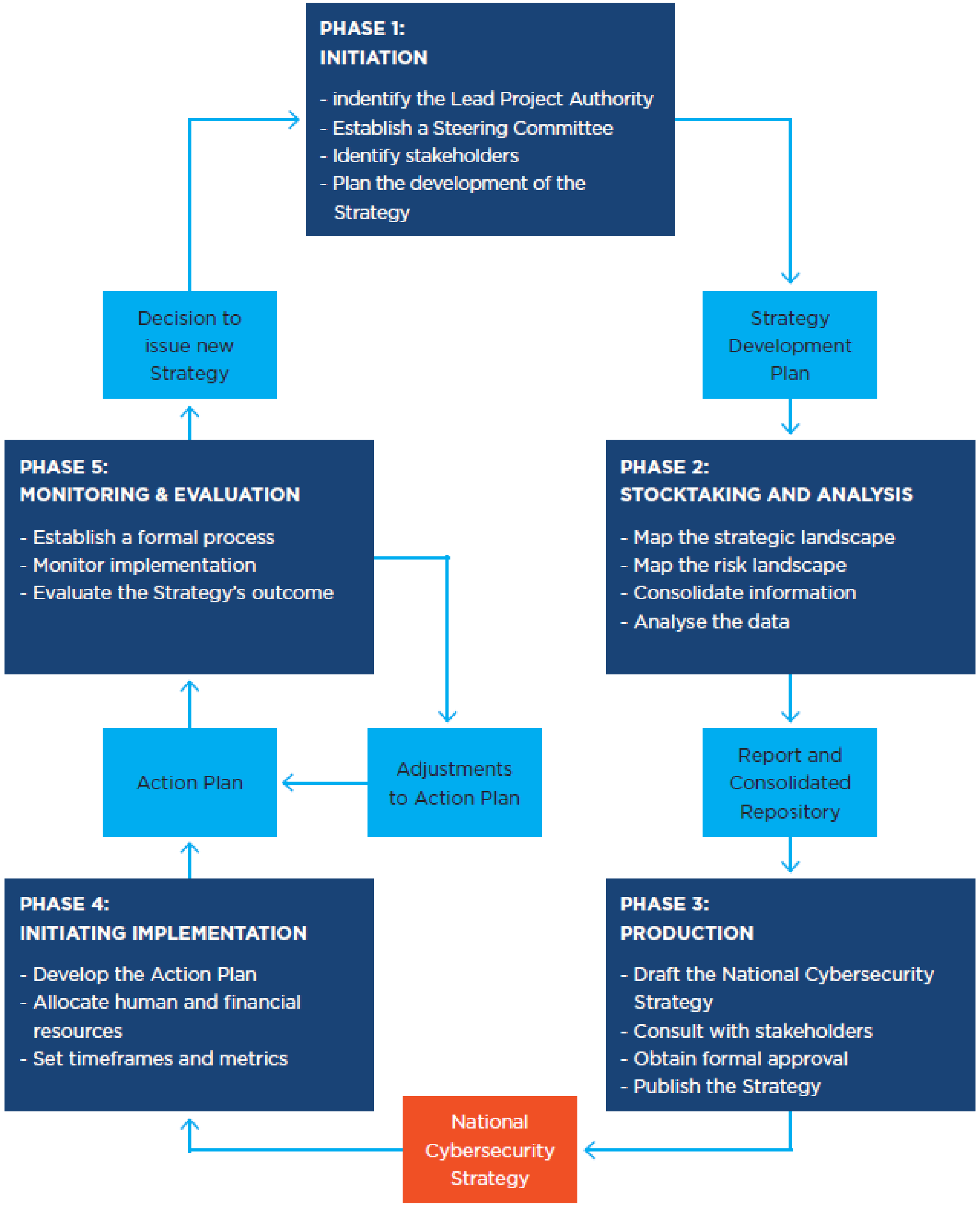


GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

STRATEGIC ENGAGEMENT IN CYBERSECURITY

National Cybersecurity Strategy (NCS) Lifecycle

1. Phase I – Initiation
2. Phase II - Stocktaking and analysis
3. Phase III – Production
4. Phase IV - Initiating and implementation
5. Phase V - Monitoring & evaluation



PHASE 1:
INITIATION

- indentify the Lead Project Authority
- Establish a Steering Committee
- Identify stakeholders
- Plan the development of the Strategy

Strategy Development Plan

PHASE 2:
STOCKTAKING AND ANALYSIS

- Map the strategic landscape
- Map the risk landscape
- Consolidate information
- Analyse the data

Report and Consolidated Repository

PHASE 3:
PRODUCTION

- Draft the National Cybersecurity Strategy
- Consult with stakeholders
- Obtain formal approval
- Publish the Strategy

National Cybersecurity Strategy

PHASE 4:
INITIATING IMPLEMENTATION

- Develop the Action Plan
- Allocate human and financial resources
- Set timeframes and metrics

Action Plan

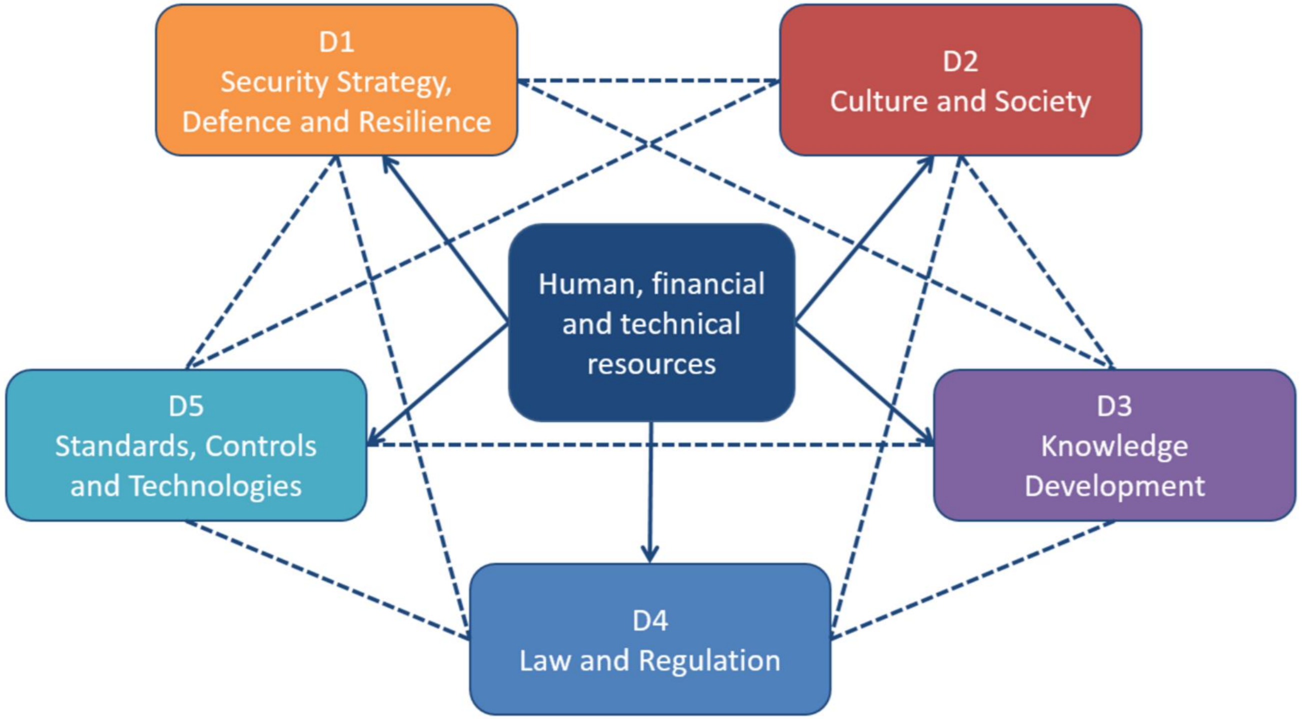
Adjustments to Action Plan

PHASE 5:
MONITORING & EVALUATION

- Establish a formal process
- Monitor implementation
- Evaluate the Strategy's outcome

Decision to issue new Strategy

Cybersecurity Capacity Maturity Model Assessments


D1
Security Strategy, Defence and Resilience
D2
Culture and Society
Human, financial and technical resources
D5
Standards, Controls and Technologies
D3
Knowledge Development
D4
Law and Regulation

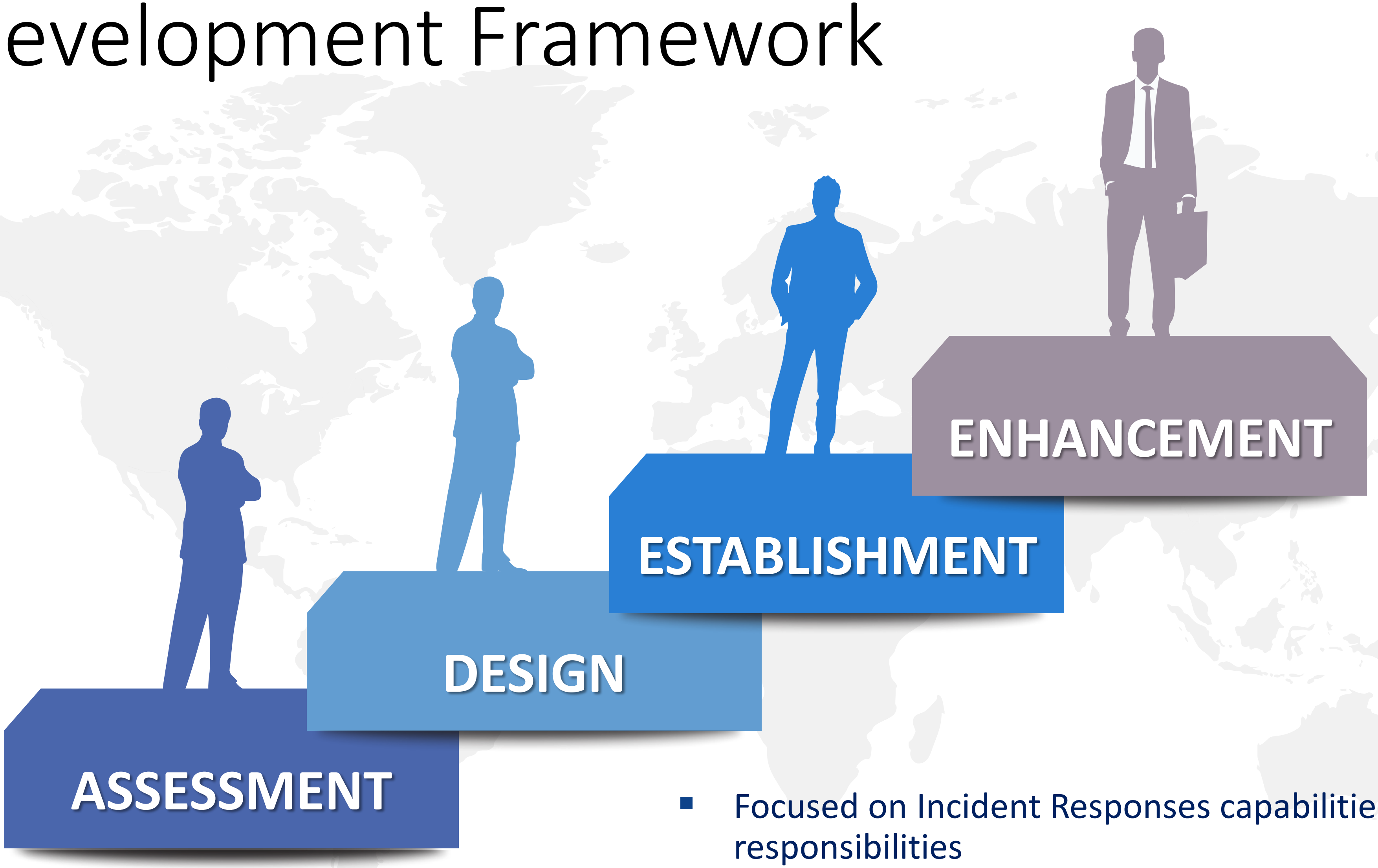
Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CIRT Framework

CIRT Development Framework



- Focused on Incident Responses capabilities with National responsibilities
- Aligned with the FIRST Service Framework

CIRT Assessment

Assessment Service	
Description	Review the current incident response capabilities present at the national level
Activities	▪ Administering CIRT questionnaire ▪ Analyzing response/s ▪ Performing on-site visit for review and finalization ▪ On-site workshop
Key Deliverables	Assessment report with basic recommendations
Modality	Off-site and On-site
Costs	Covered by ITU or donor

CIRT Design

	Design Service
Description	Develop a blueprint of the National CIRT project, with the related implementation processes
Activities	▪ Defining of CIRT positioning ▪ Identify CIRT services required ▪ Identify processes and related workflows ▪ Identify policies and procedures required (draft) ▪ Relationships with constituency and communication strategy ▪ Define technology requirements ▪ Define premises required ▪ Identify HR skills required
Key Deliverables	CIRT design document and implementation plan
Modality	Off-site and On-site
Costs	Covered by the beneficiary Member State or donor

CIRT Establishment

Typical basic services that a National CIRT may provide to its constituents:

- Incident handling
- Incident analysis
- Outreach and communication

	Establishment Service
Description	Execute the project as agreed with the Member States and based on the outcomes of the Design Service’s deliverables
Activities	▪ Capabilities development (human and technological) ▪ Hardware and software acquisition ▪ Capabilities deployment and testing ▪ Operations training ▪ Customization, fine tuning and training ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material ▪ Tools
Modality	Off-site and On-site
Costs	Covered by the beneficiary Member State or donor

CIRT Enhancement

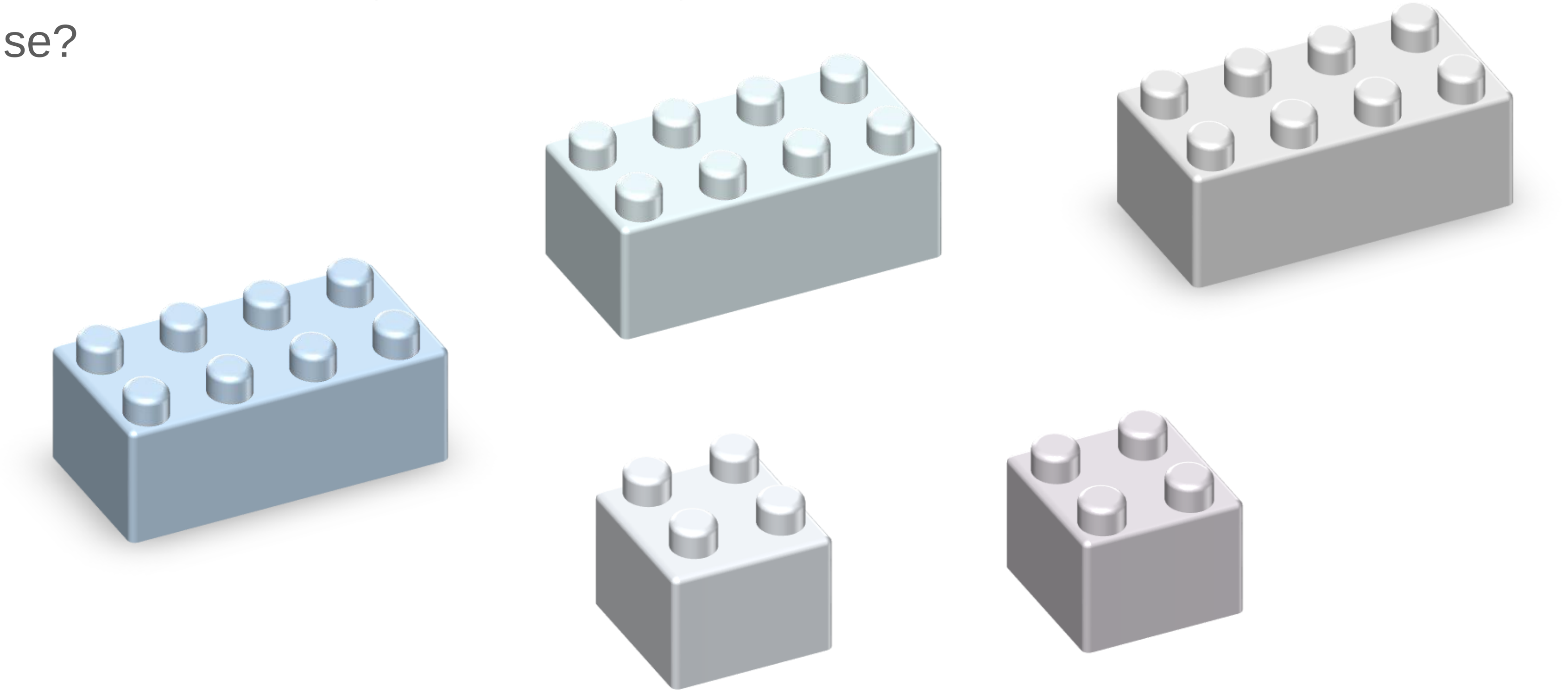
Typical enhanced services that a National CIRT may provide to its constituents:

- Incident handling
- Incident analysis
- Outreach and communication
- Analysis (Artifact, media)
- Situational Awareness (Sensor operation, fusion and correlation)

Enhancement Services	
Description	Enhance capabilities and services of the National CIRT
Activities	▪ Evaluation and analysis of the quality for the current capabilities and services ▪ Define the required enhancements ▪ Additional capabilities deployment and testing ▪ Enhanced services - operations training ▪ Customization, fine tuning and training ▪ Handover and closure
Key Deliverables	▪ Additional SOPs ▪ Additional operating manuals ▪ Additional training materials ▪ Additional tools
Modality	Off-site and On-site
Costs	Covered by the beneficiary Member State or donor

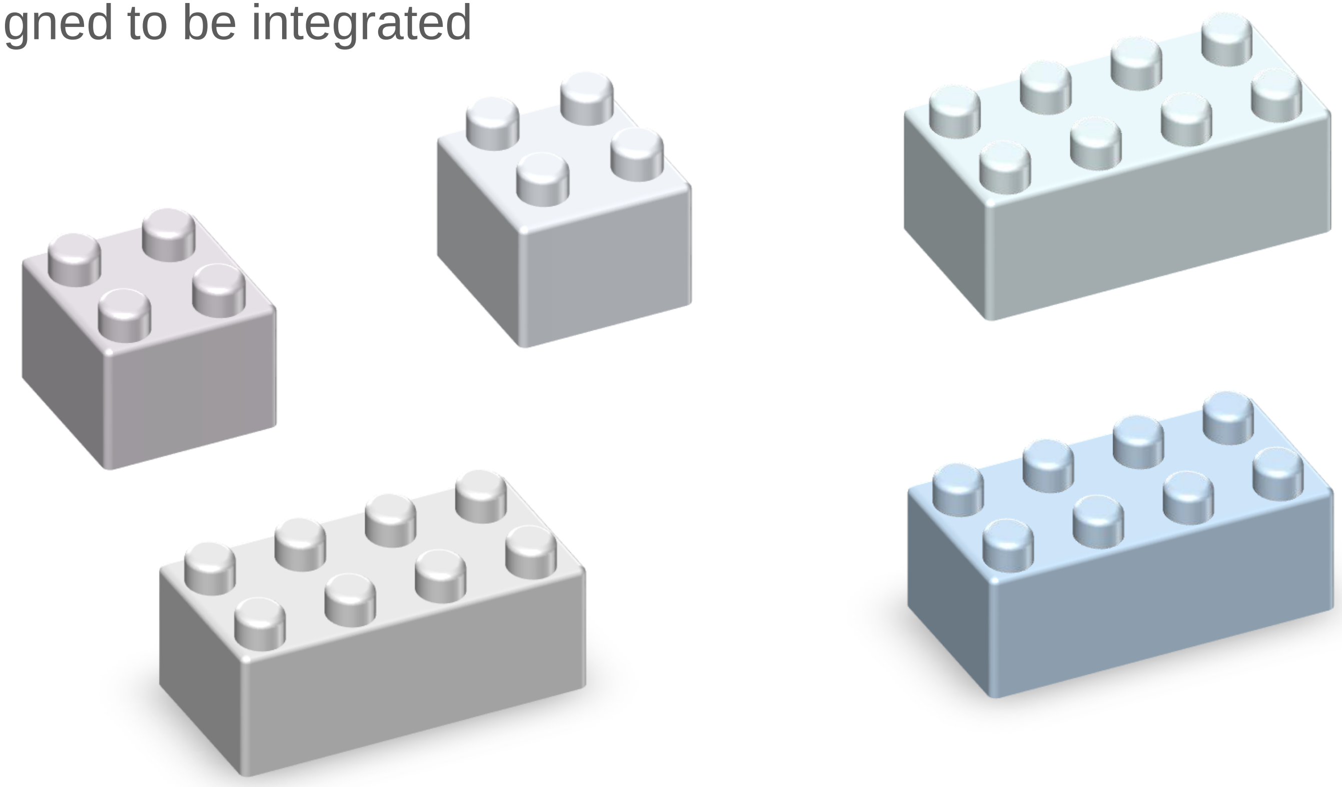
Notion of building blocks

- A building block is an atomic element (piece of HW, document, training course, etc.) that can be used to produce a deliverable
- Building blocks are cross cutting to all processes used to provide assistance as well as to the services that the CIRT will provide to the constituency
- Interchangeable, modular, designed to be integrated
- Something else?



Notion of building blocks

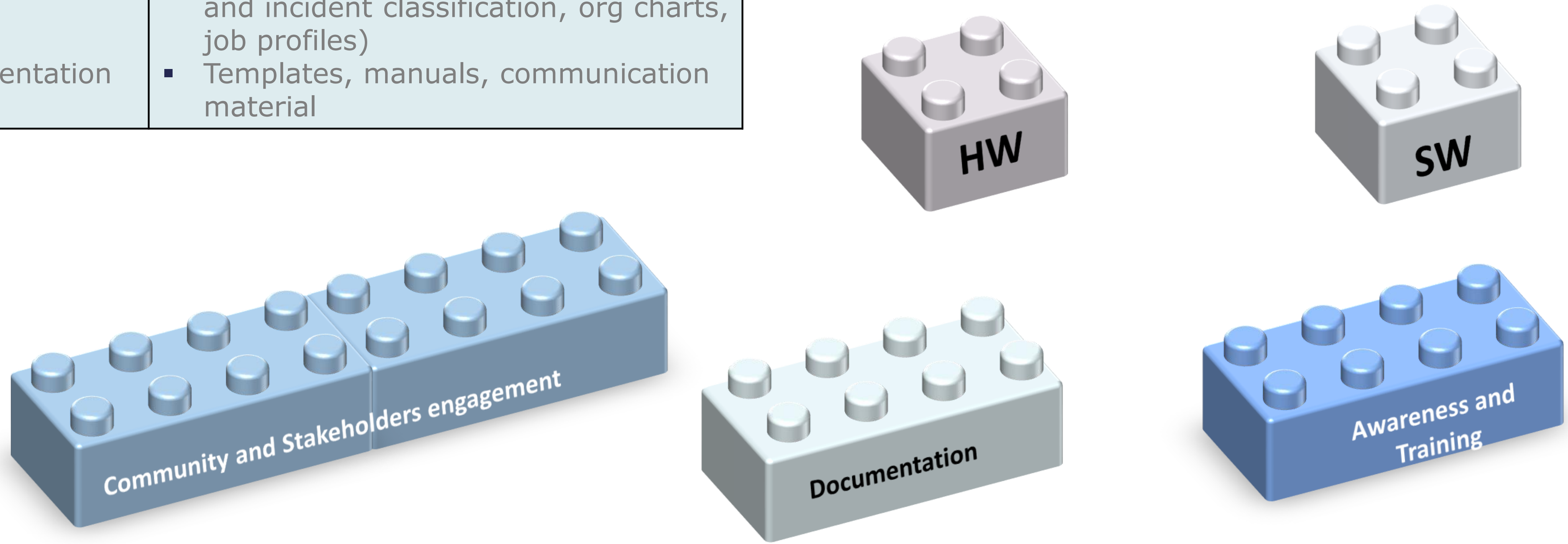
- A building block is an atomic element (piece of HW, document, training course, etc.) that can be used to produce a deliverable
- Building blocks are cross cutting to all processes used to provide assistance as well as to the services that the CIRT will provide to the constituency
- Interchangeable, modular, designed to be integrated
- Something else?



Typology of Building Blocks

HW	▪ Appliances ▪ Network devices ▪ Desktops, laptops ▪ Cables
SW	▪ RTIR ▪ Tools for malware analysis ▪ Office automation tools
Documentation	▪ Policies (internal security policy, data and incident classification, org charts, job profiles) ▪ Templates, manuals, communication material

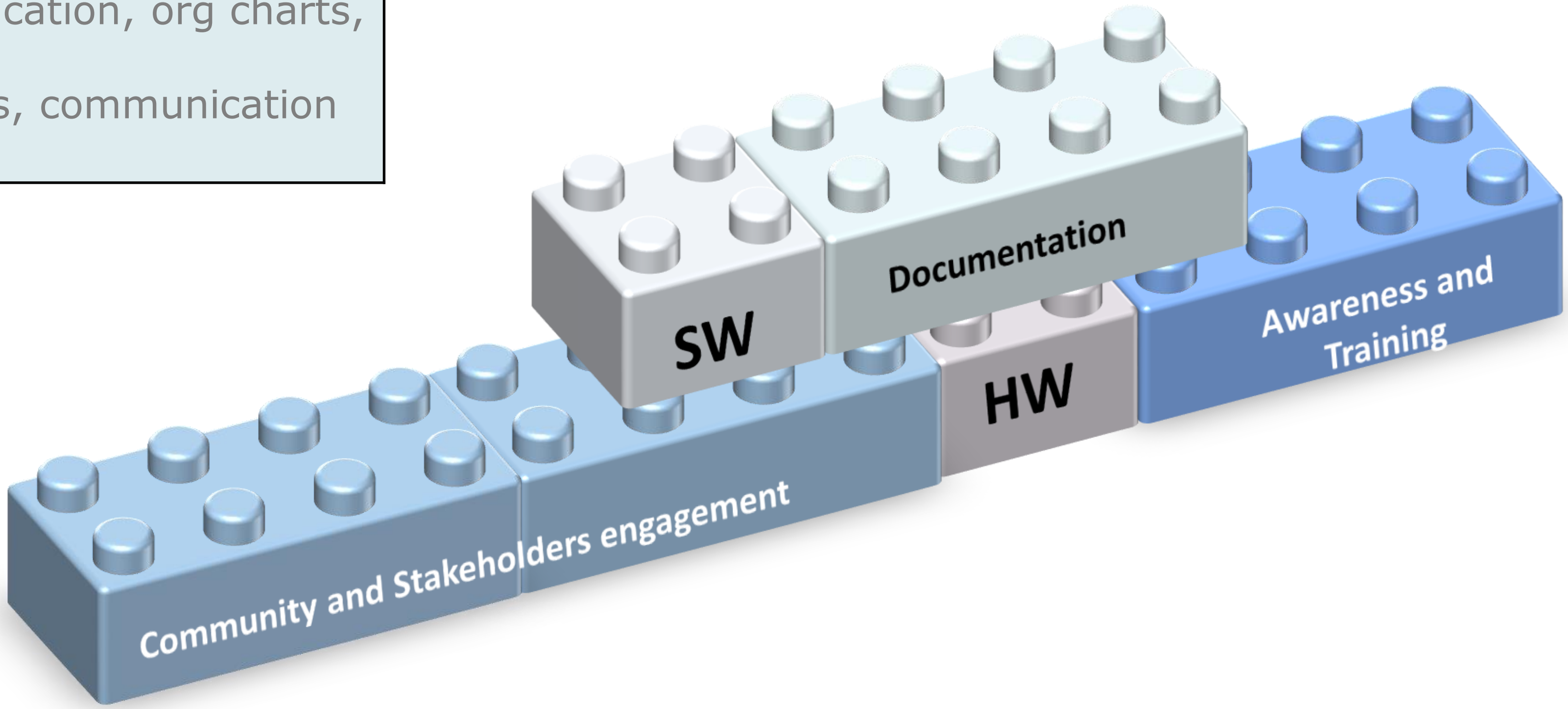
Awareness and training	▪ Presentations ▪ Books ▪ Training lab ▪ Manuals ▪ Communication material
Community and stakeholders engagement	▪ FIRST Membership ▪ Outreach plan ▪ Announcement plan



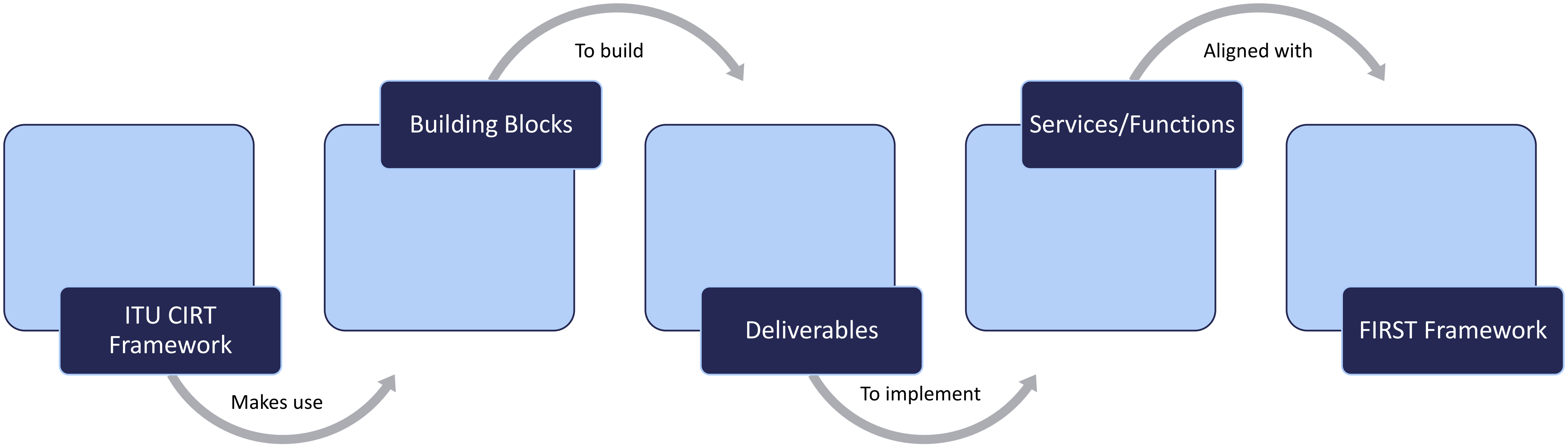
Typology of Building Blocks

HW	▪ Appliances ▪ Network devices ▪ Desktops, laptops ▪ Cables
SW	▪ RTIR ▪ Tools for malware analysis ▪ Office automation tools
Documentation	▪ Policies (Internal security policy, data and incident classification, org charts, job profiles) ▪ Templates, manuals, communication material

Awareness and training	▪ Presentations ▪ Books ▪ Training lab ▪ Manuals ▪ Communication material
Community and stakeholders engagement	▪ FIRST Membership ▪ Outreach plan ▪ Announcement plan



ITU CIRT Framework applied



ITU CIRT Framework

Makes use

Building Blocks

To build

Deliverables

To implement

Services/Functions

Aligned with

FIRST Framework

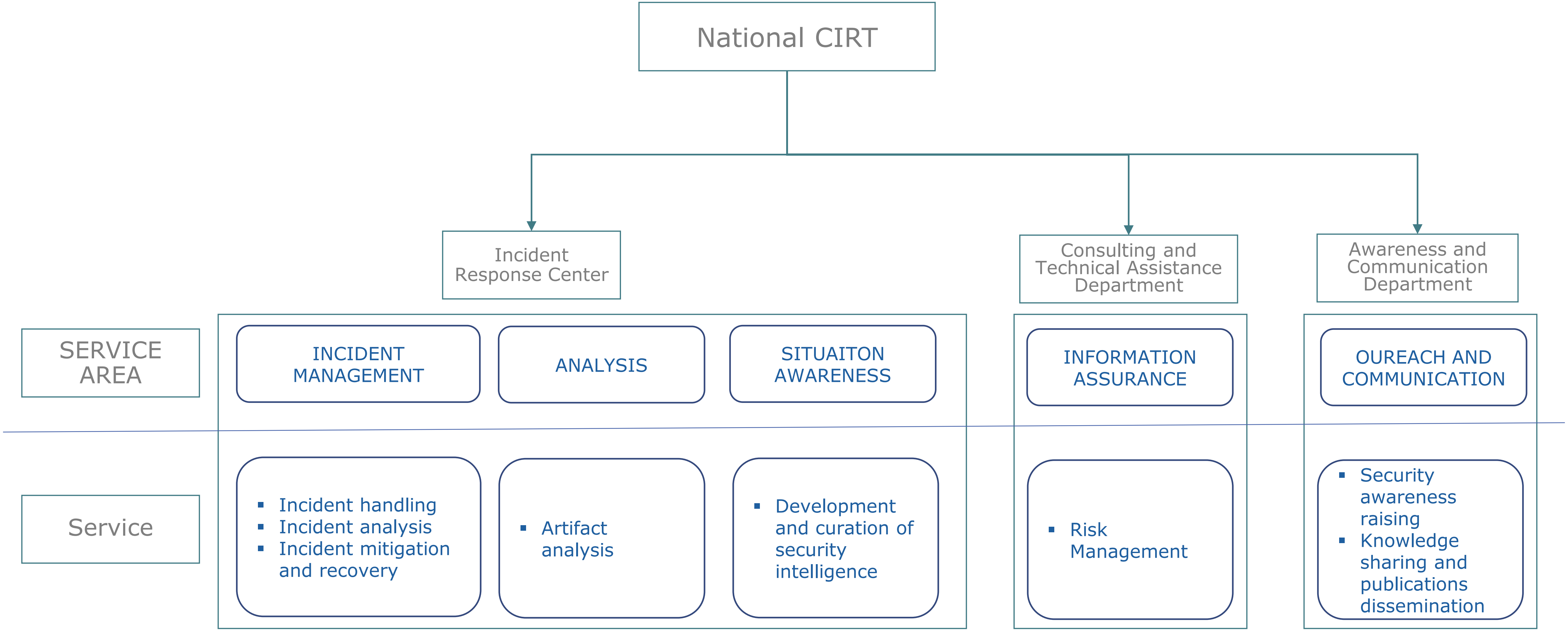
CIRT Basic Services Portfolio

Effective incident handling capability

Provide services to reduce the vulnerability of networks to cyber–attacks

Provide services to support an effective response to cyber–attacks

The Basic Services Offered by a National CIRT



National CIRT

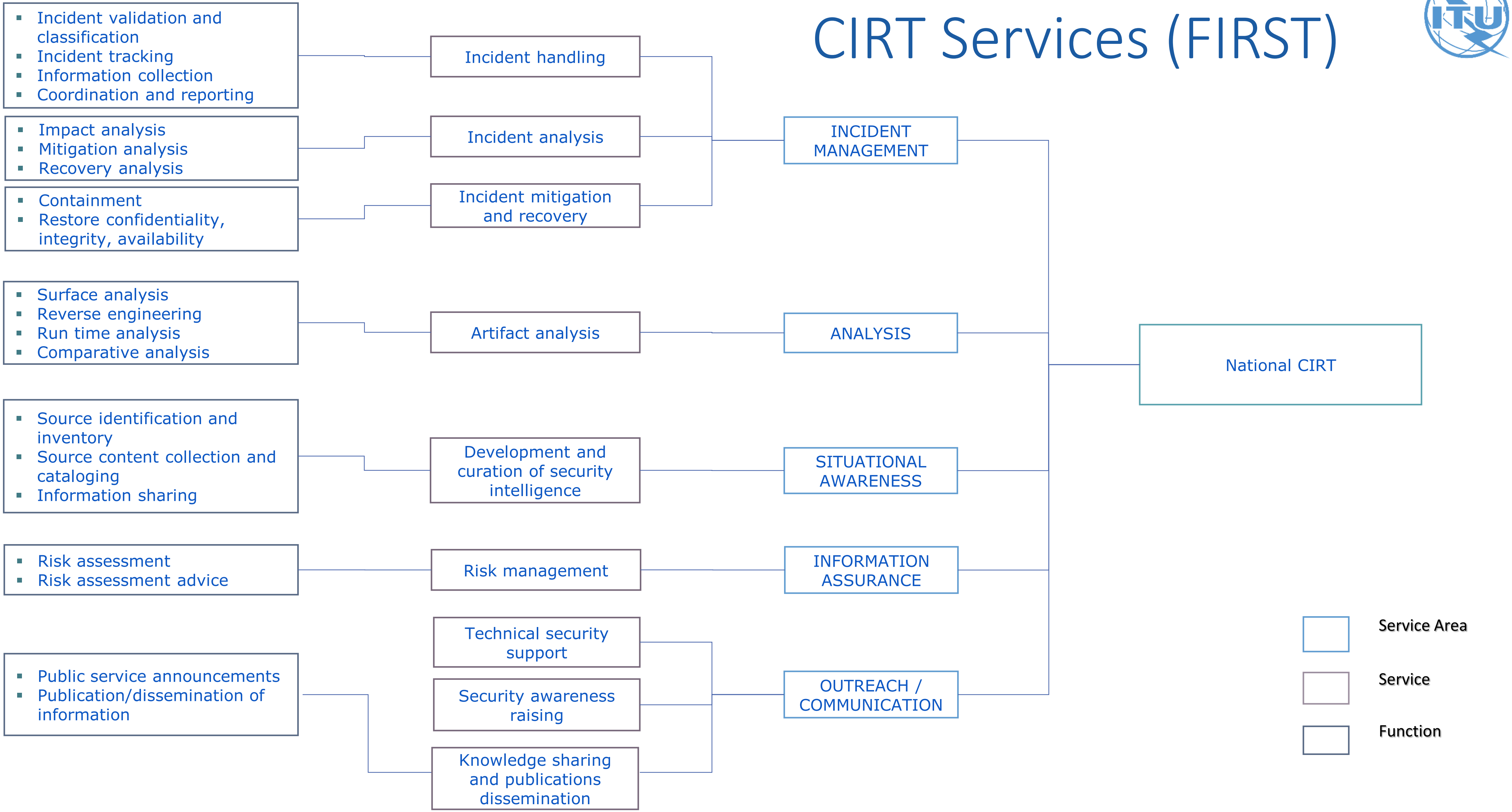
Incident Response Center

Consulting and Technical Assistance Department

Awareness and Communication Department

SERVICE AREA	INCIDENT MANAGEMENT	ANALYSIS	SITUAITON AWARENESS	INFORMATION ASSURANCE	OUREACH AND COMMUNICATION
Service	▪ Incident handling ▪ Incident analysis ▪ Incident mitigation and recovery	▪ Artifact analysis	▪ Development and curation of security intelligence	▪ Risk Management	▪ Security awareness raising ▪ Knowledge sharing and publications dissemination

CIRT Services (FIRST)



- Incident validation and classification
- Incident tracking
- Information collection
- Coordination and reporting

Incident handling

- Impact analysis
- Mitigation analysis
- Recovery analysis

Incident analysis

- Containment
- Restore confidentiality, integrity, availability

Incident mitigation and recovery

INCIDENT MANAGEMENT

- Surface analysis
- Reverse engineering
- Run time analysis
- Comparative analysis

Artifact analysis

ANALYSIS

- Source identification and inventory
- Source content collection and cataloging
- Information sharing

Development and curation of security intelligence

SITUATIONAL AWARENESS

- Risk assessment
- Risk assessment advice

Risk management

INFORMATION ASSURANCE

Technical security support

Security awareness raising

- Public service announcements
- Publication/dissemination of information

Knowledge sharing and publications dissemination

OUTREACH / COMMUNICATION

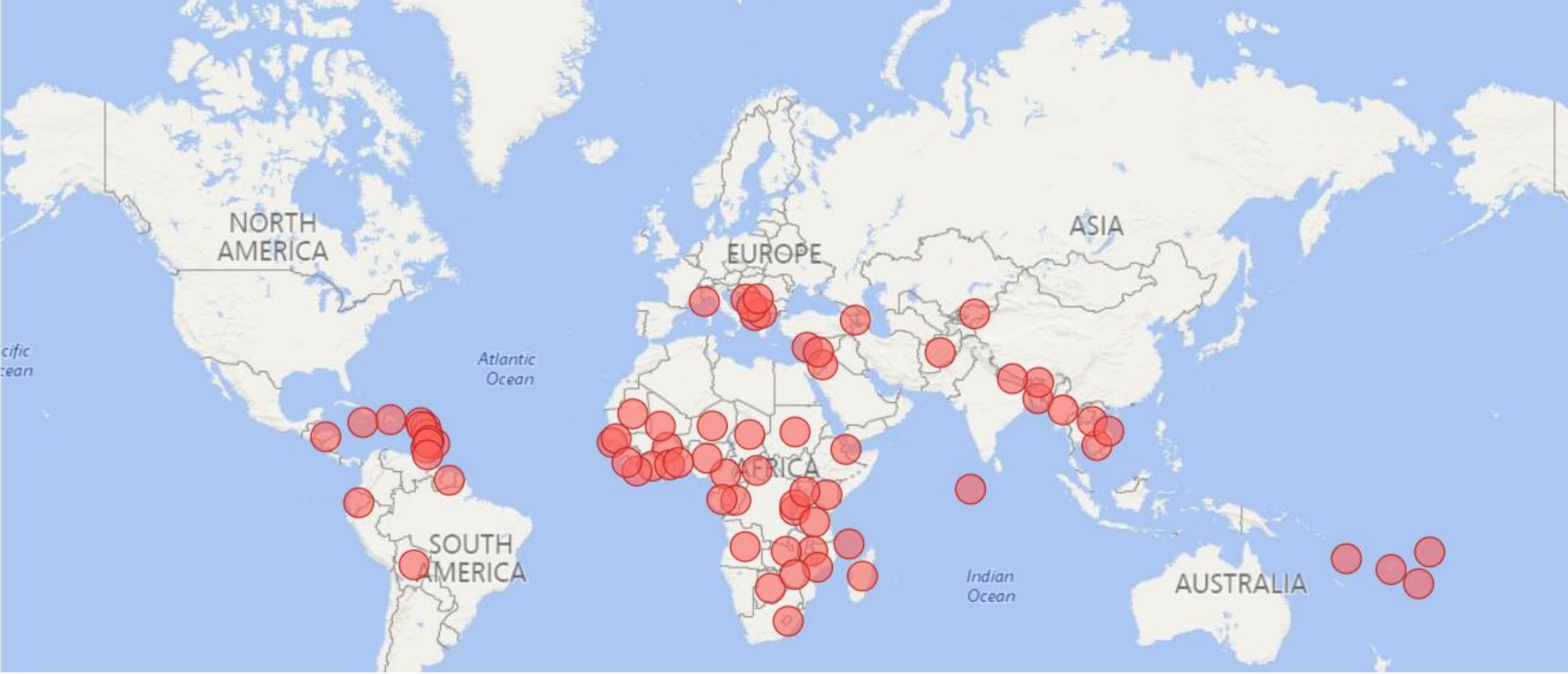
National CIRT

□ Service Area

□ Service

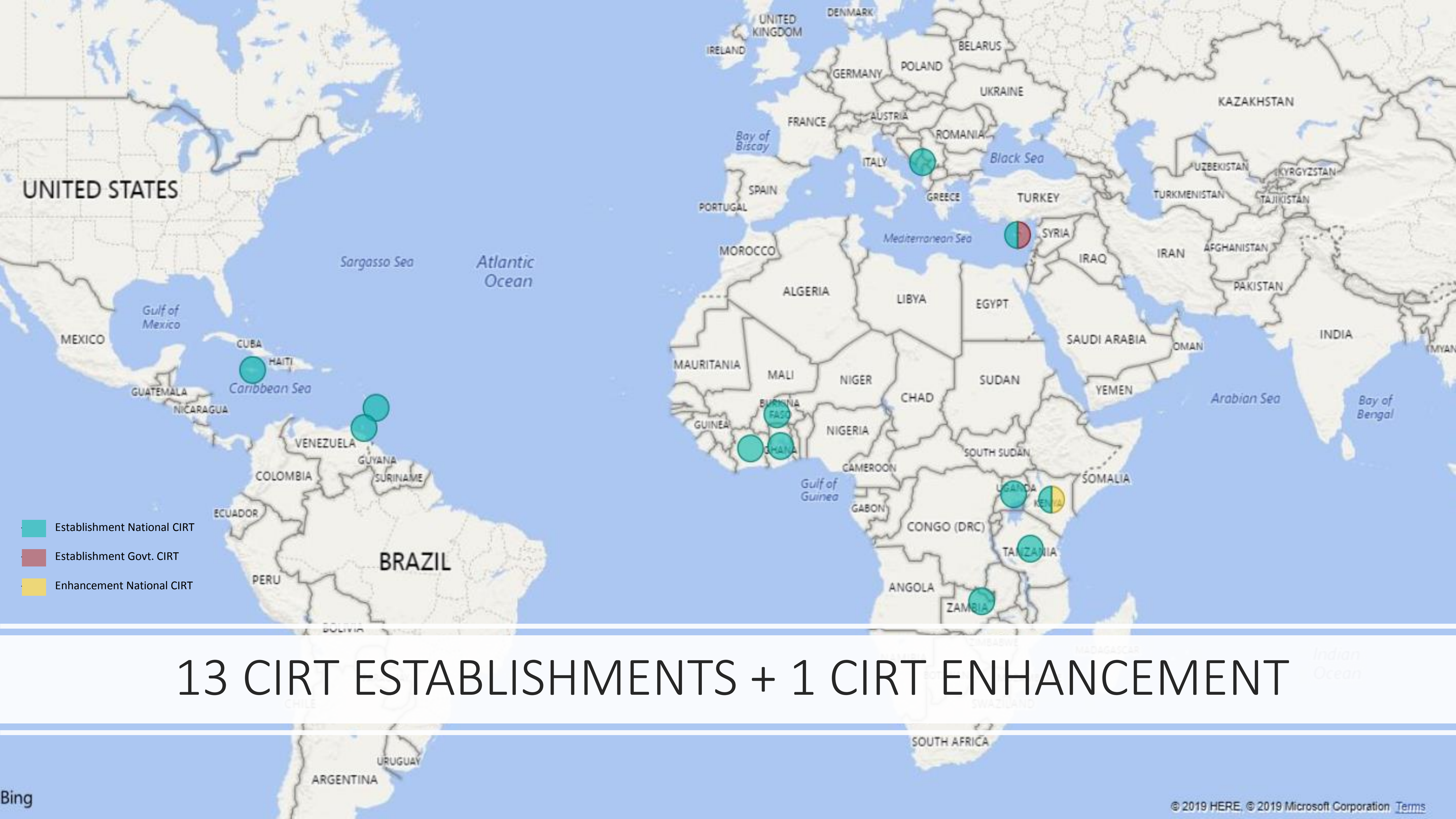
□ Function

ITU CIRT Framework Activities

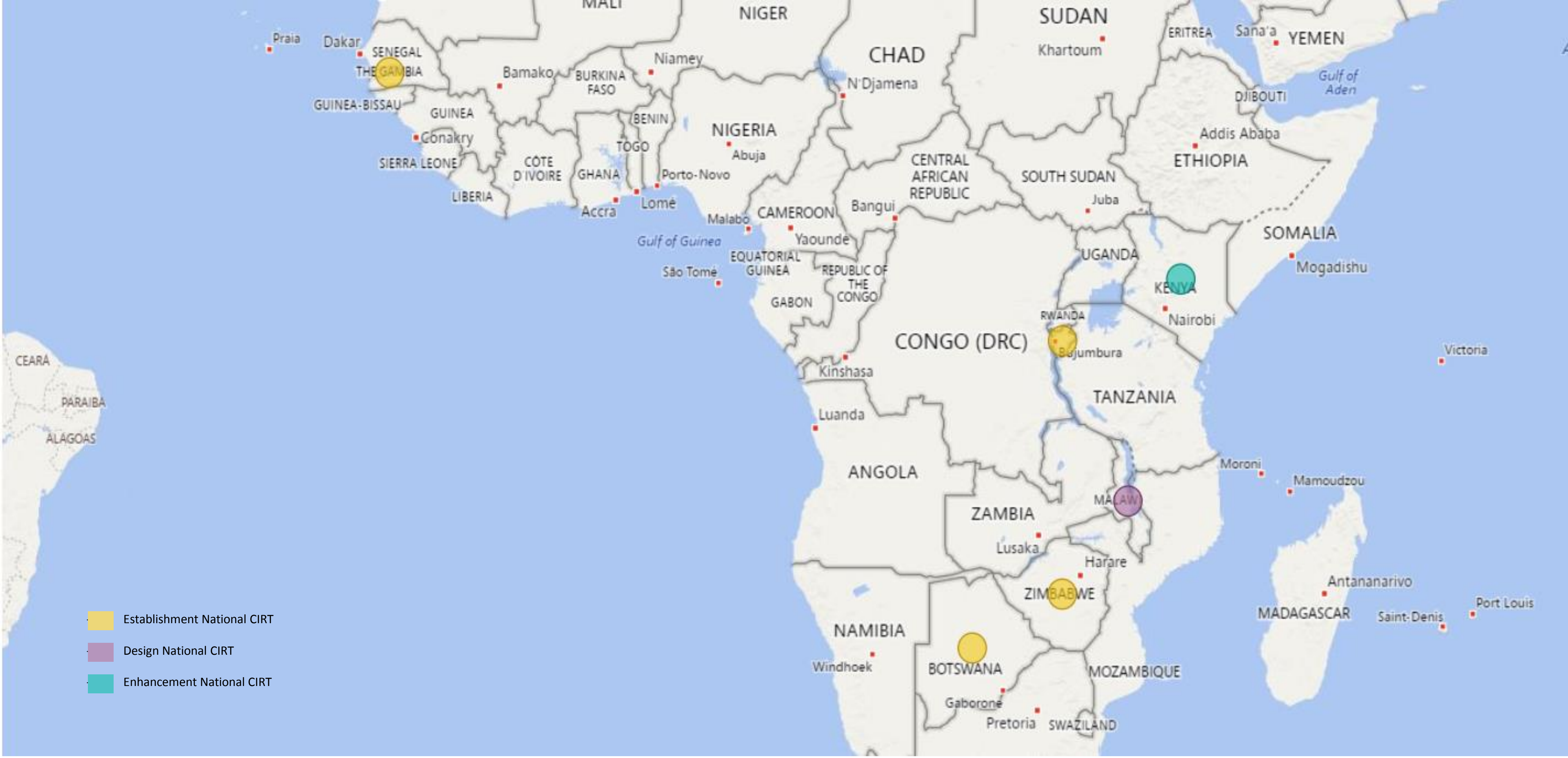


75 CIRT READINESS ASSESSMENTS

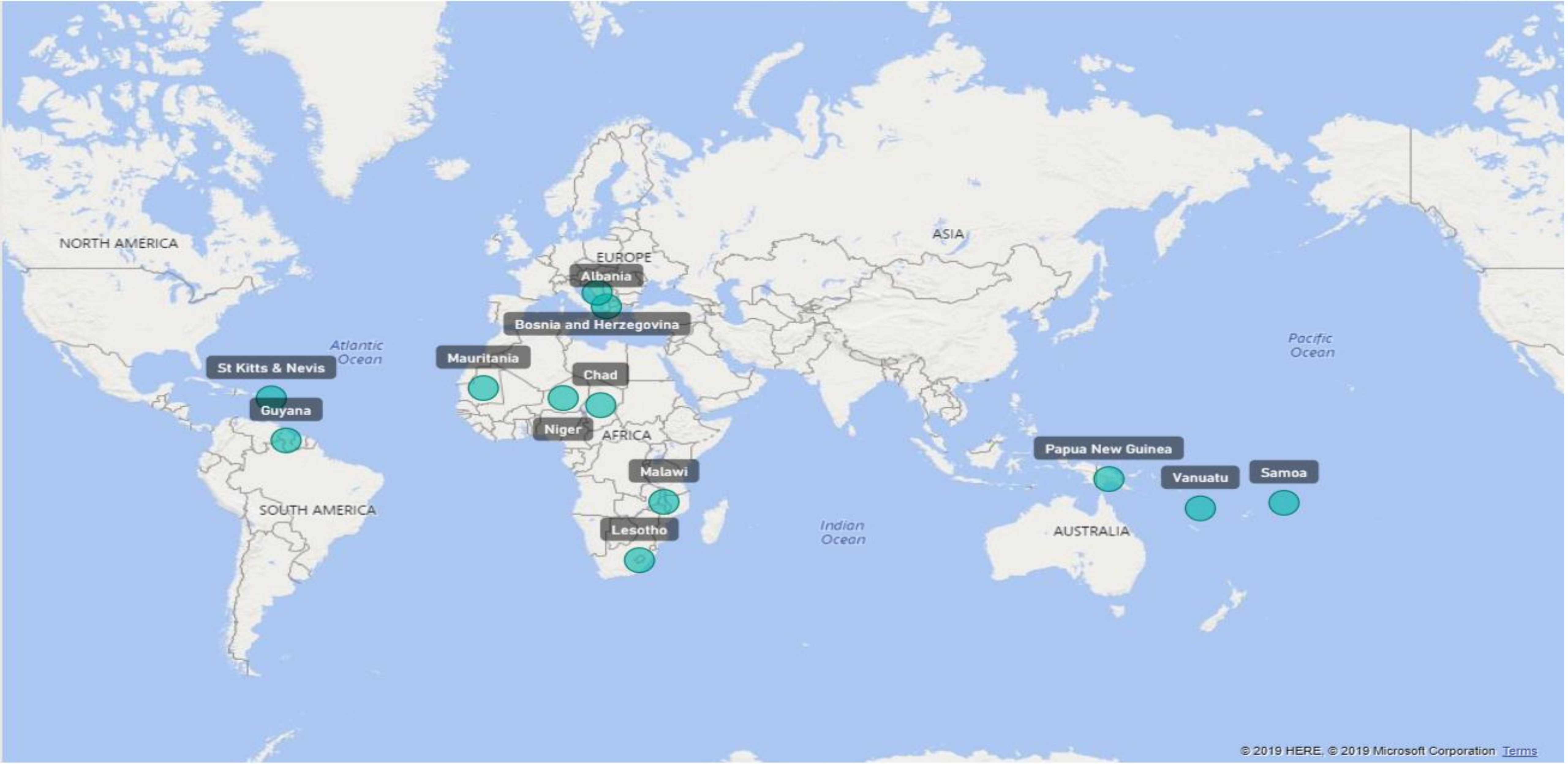
© 2019 HERE, © 2019 Microsoft Corporation Terms



13 CIRT ESTABLISHMENTS + 1 CIRT ENHANCEMENT



2019 CIRT ACTIVITIES IN AFRICA REGION



National CIRT Establishment – Interests Around the World

Cyberdrills

Regional Cyberdrills -Objectives

1 Enhancing cybersecurity capacity and capabilities through regional collaborations and cooperation;

2 Enhancing the awareness and the capability of countries to participate and to contribute to the development and deployment of a strategy of defeating a cyber threat;

3 Strengthening international cooperation between Member States to ensure continued collective efforts against cyber threats;

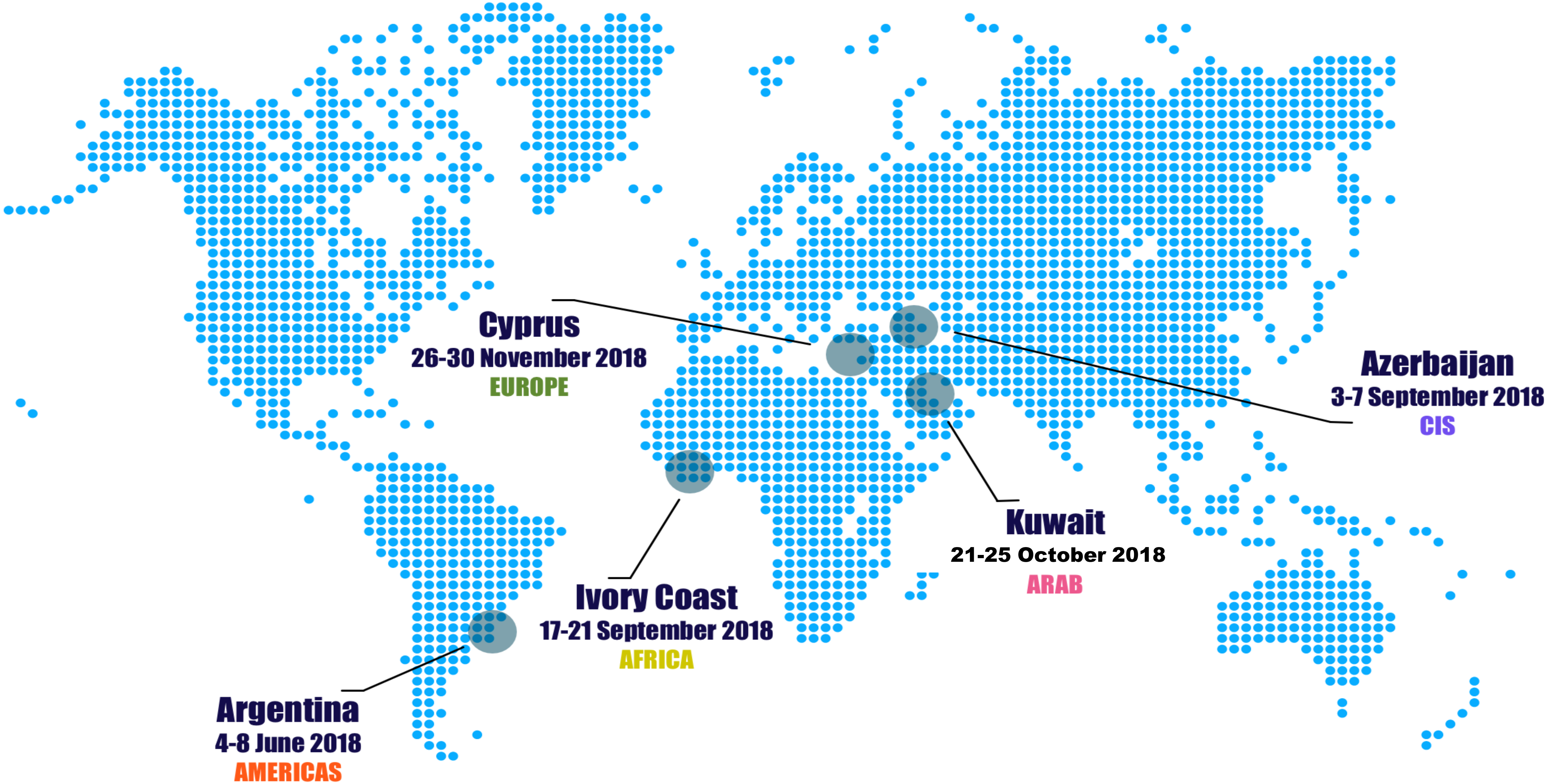
4 Enhancing Member States’ and incident response capabilities and communication;

5 Assisting Member States to develop and implement operational procedures to respond better to various cyber incidents, identify improvements for future planning CIRT processes and operational procedures

Regional Cyberdrills - Programme

1. Days 1 and 2 are dedicated to the organization of capacity building sessions, case studies or other themes-related training requirements, as well as COP-related issues, etc.
2. Day 3 is a conference day that includes presentations and panel discussions on current issues, latest assessment and current and emerging trends in cybersecurity threats and solutions.
3. Days 4 and 5 are structured around scenarios that consist of several incidents involving the most common types of attacks and possible resolutions.

CYBERDRILLS 2018



Cyprus
26-30 November 2018
EUROPE

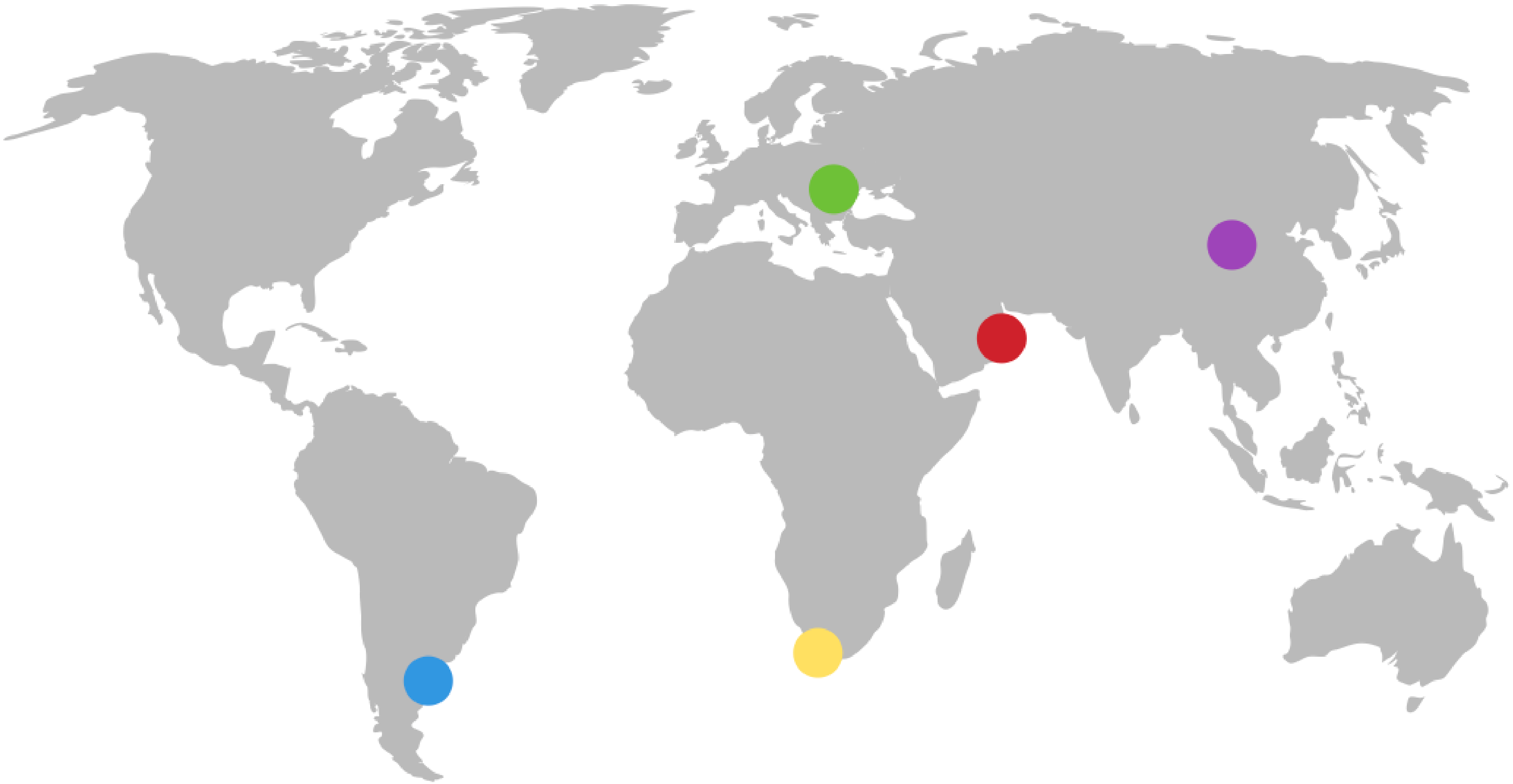
Azerbaijan
3-7 September 2018
CIS

Kuwait
21-25 October 2018
ARAB

Ivory Coast
17-21 September 2018
AFRICA

Argentina
4-8 June 2018
AMERICAS

CYBERDRILLS 2019



Europe

21-31 May 2019

Americas

26-30 August 2019

Asia-Pacific & CIS

9-13 September 2019

Arab States

27-31 October 2019

Africa

18-22 November 2019

Cyberdrills

SOME OF ORGANIZATIONS WE WORK WITH

ABIresearch®
for visionaries

Bitdefender®

COMTECH
TELECOMMUNICATIONS CORP.

RCC
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

KASPERSKY lab

nuix

Symantec.

lacnic

AfricaCERT
United in promoting cyber security in Africa

silensec

CyberServices

ACTIONABLE THREAT INTELLIGENCE
REDTEAM
CYBER

FORTINET®

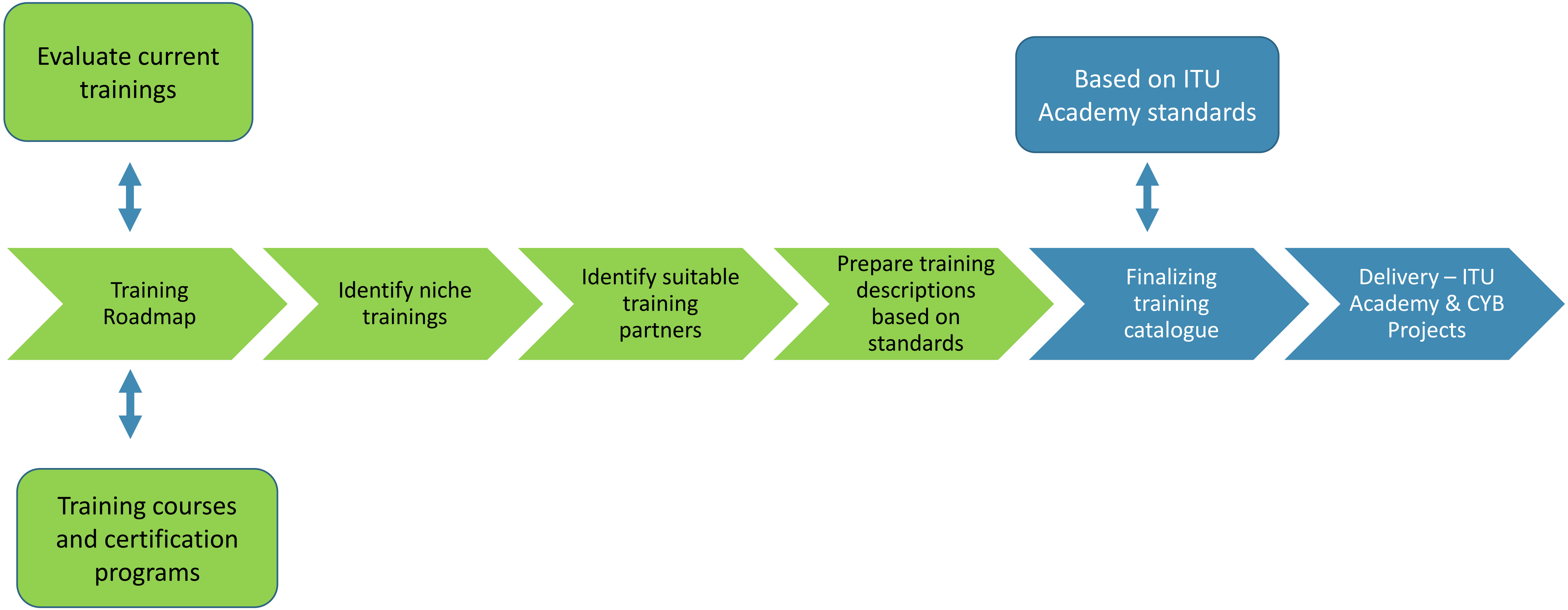
guardtime

Deloitte.

WORLD BANK GROUP

Human Capacity Development

Cybersecurity Training Catalogue



Evaluate current trainings

Training Roadmap

Identify niche trainings

Identify suitable training partners

Prepare training descriptions based on standards

Finalizing training catalogue

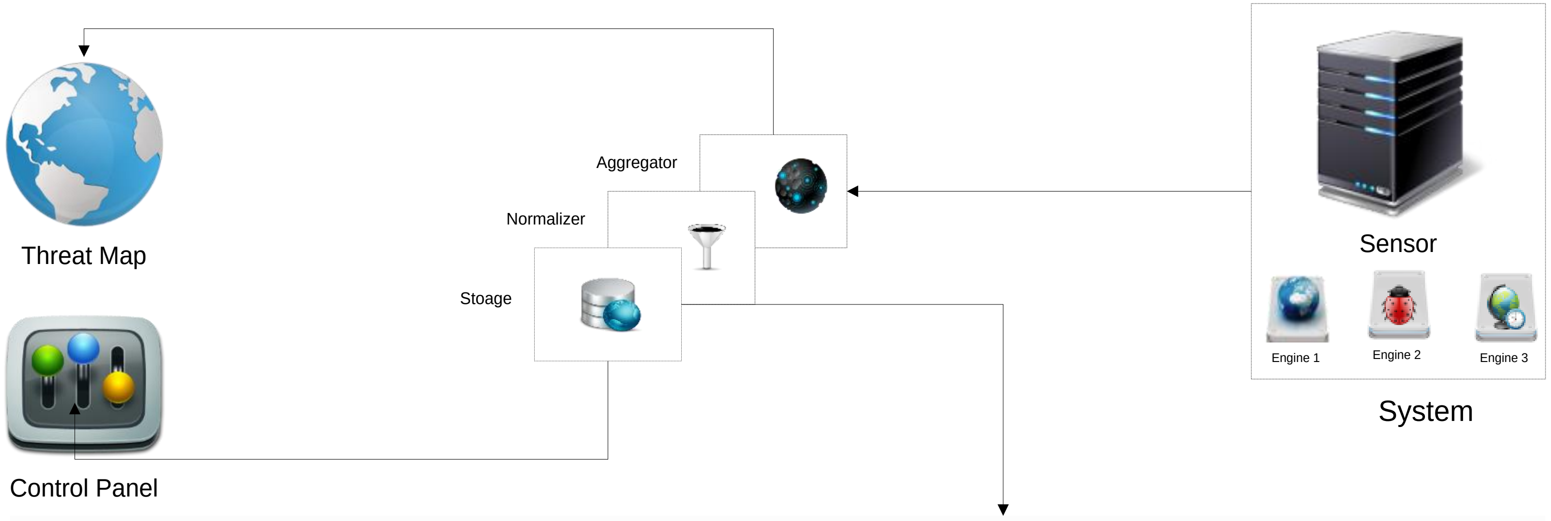
Delivery – ITU Academy & CYB Projects

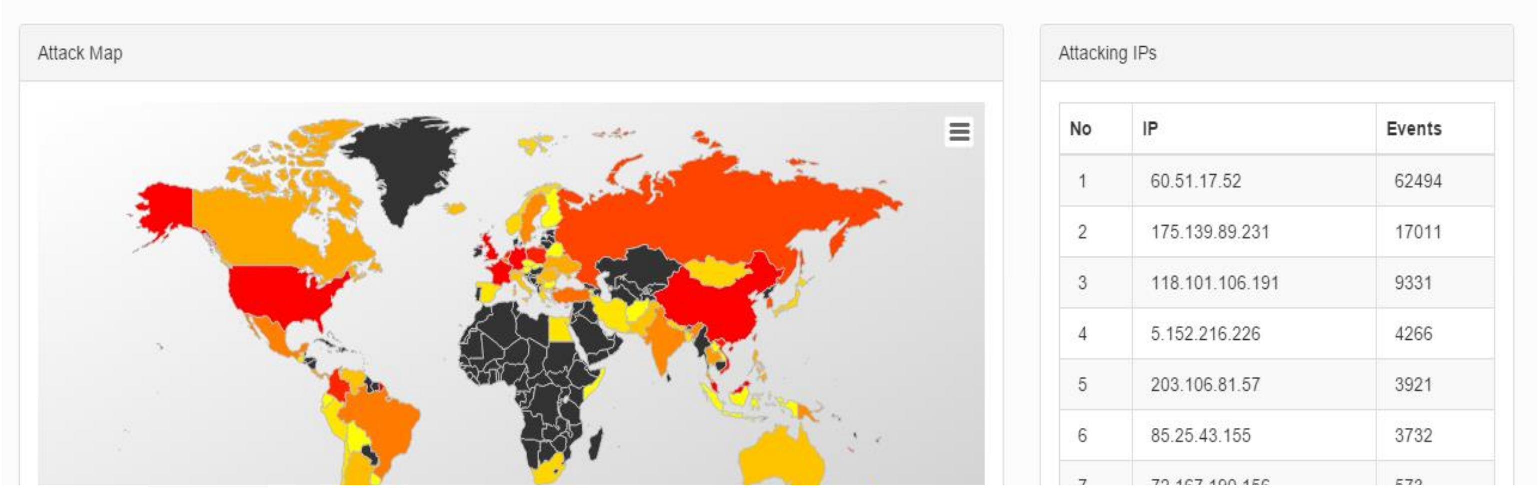
Based on ITU Academy standards

Training courses and certification programs

The Honeypot Research Network (HORNET)

Cyber Threat Intelligence – HORNET





Attacking IPs

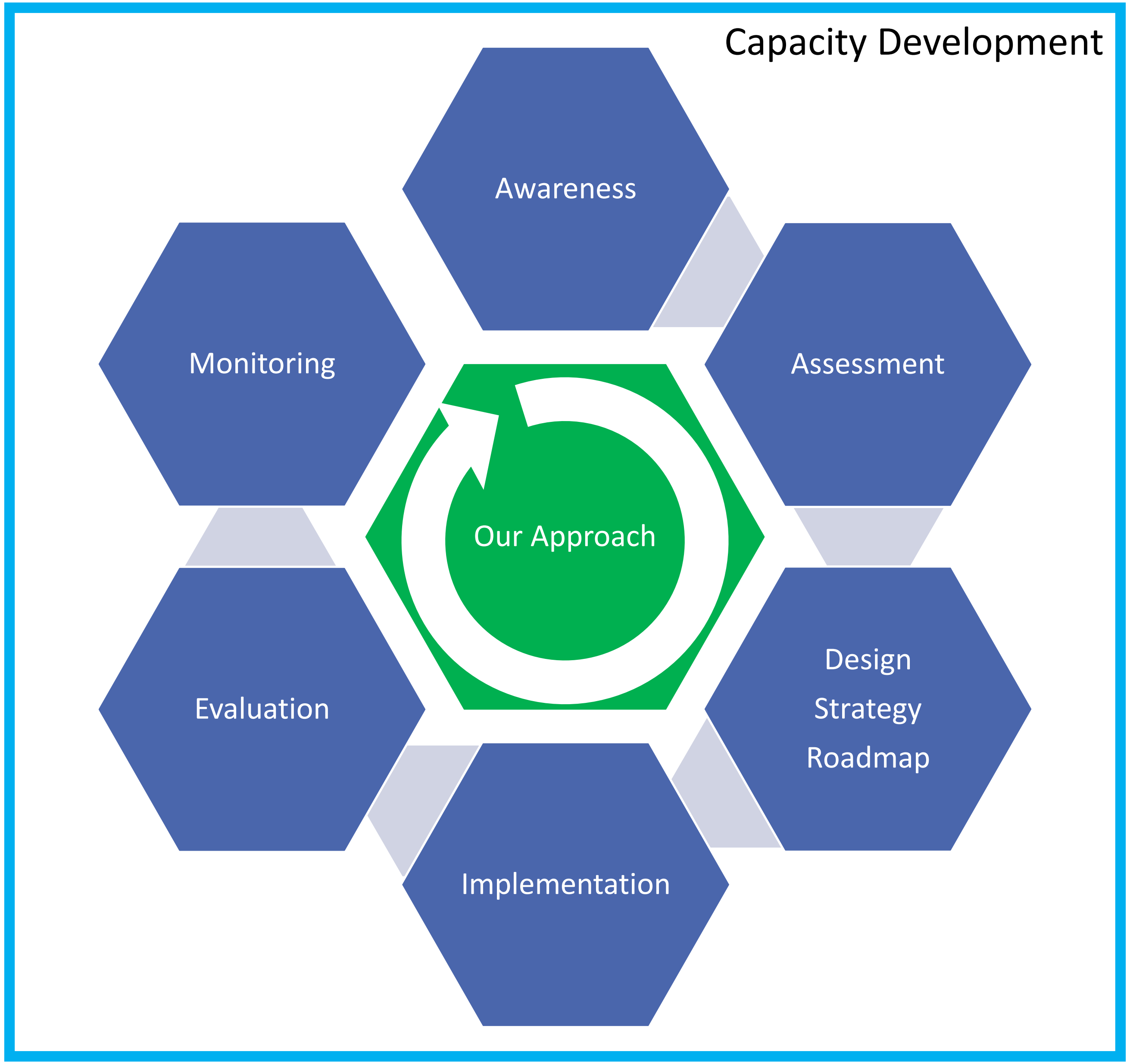
No	IP	Events
1	60.51.17.52	62494
2	175.139.89.231	17011
3	118.101.106.191	9331
4	5.152.216.226	4266
5	203.106.81.57	3921
6	85.25.43.155	3732
7	73.167.190.156	573

Dashboard

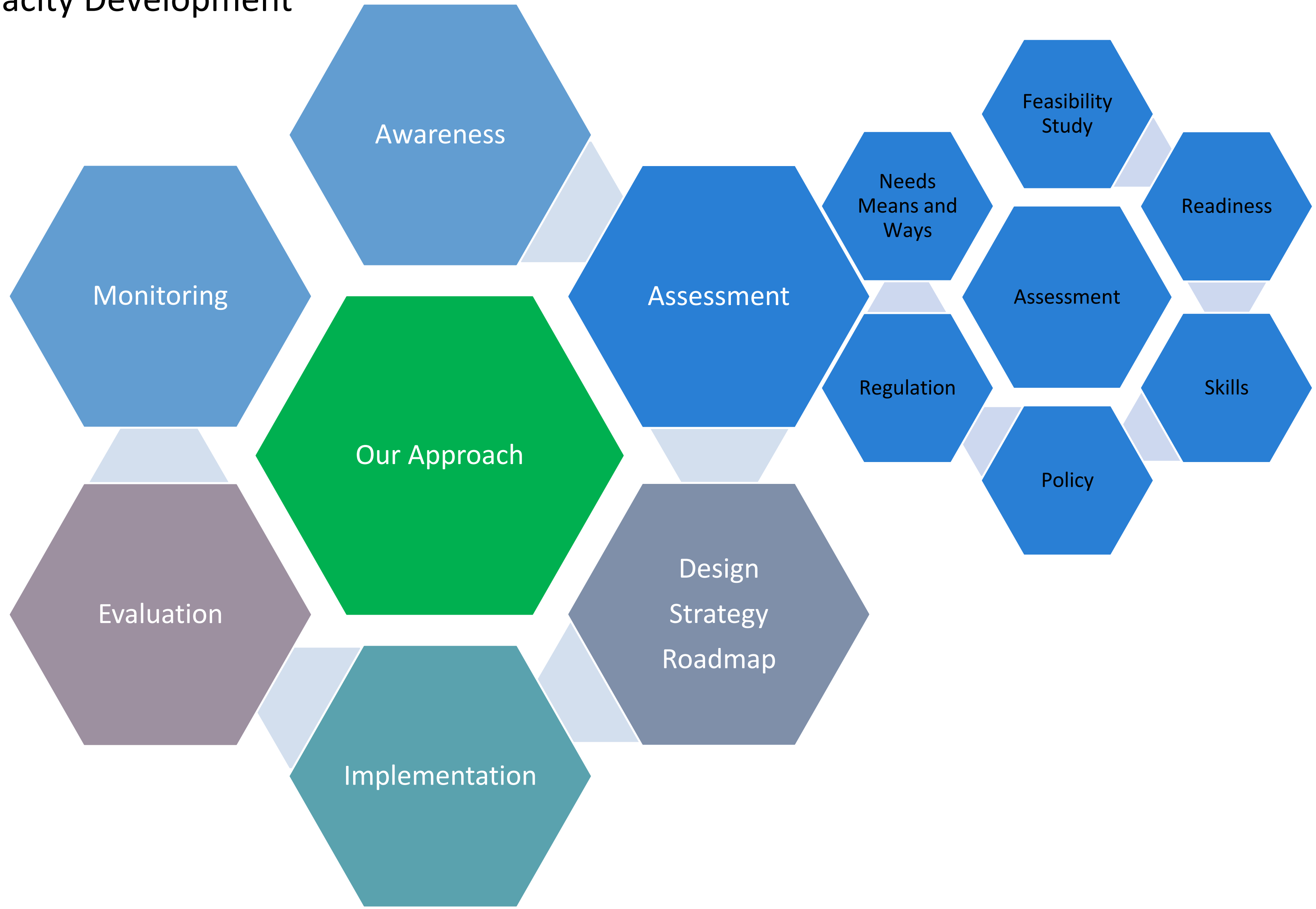
The main functions of the HORNET platform are:

- Enable countries to detect, recognize, and prevent attacks that target their cyberspace.
- Help the countries to strengthen the security monitoring of their cyberspace.
- Facilitate communication and improve collaboration between national CIRTs
- Play the role of a data sharing platform between National CIRTs

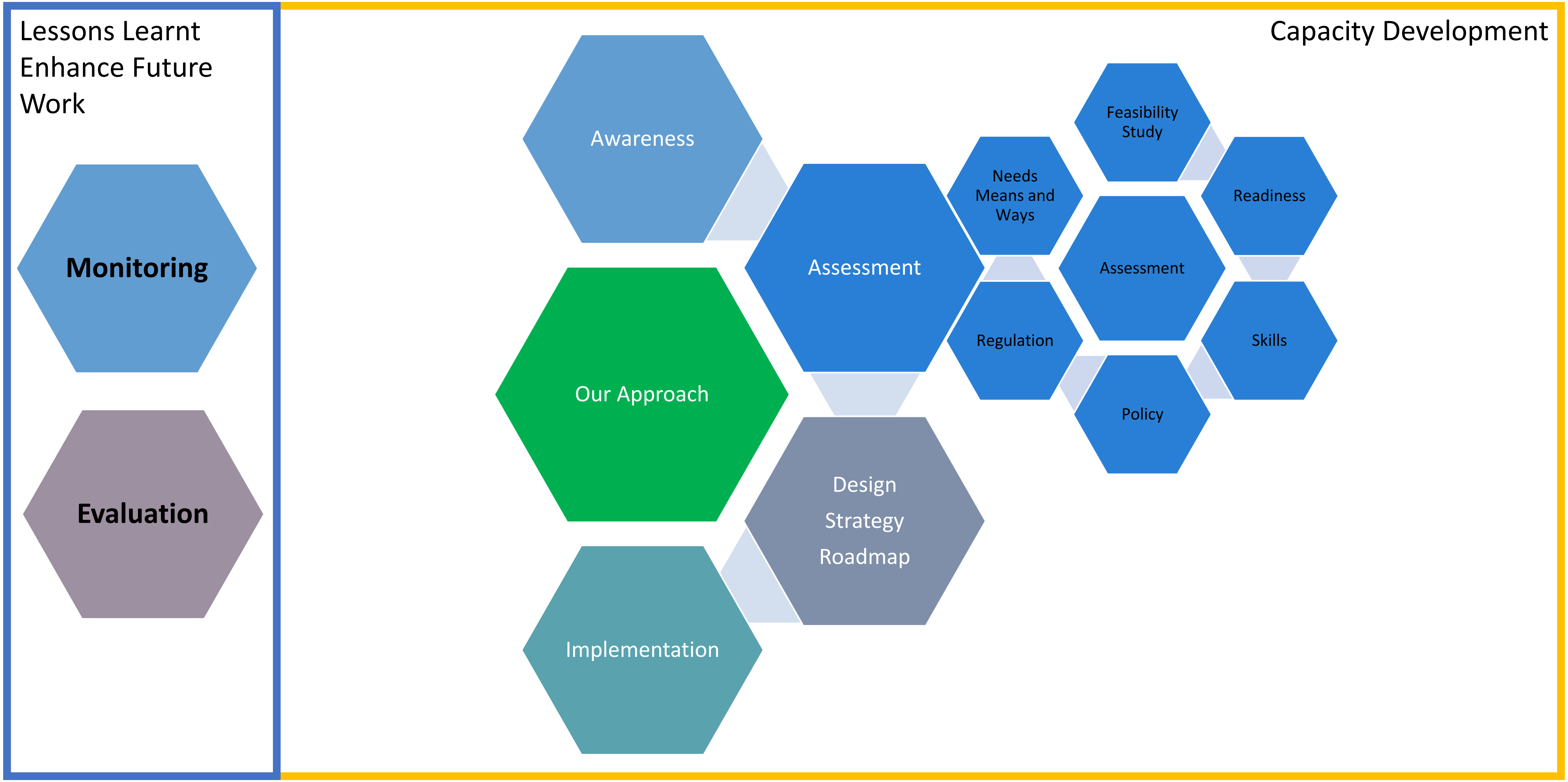
Our Approach


Capacity Development
Awareness
Assessment
Design
Strategy
Roadmap
Implementation
Evaluation
Monitoring
Our Approach

Capacity Development



Monitoring and Evaluation ➔ Enhancement



Lessons Learnt
Enhance Future
Work

Monitoring

Evaluation

Capacity Development

Awareness

Our Approach

Assessment

Design
Strategy
Roadmap

Implementation

Needs
Means and
Ways

Regulation

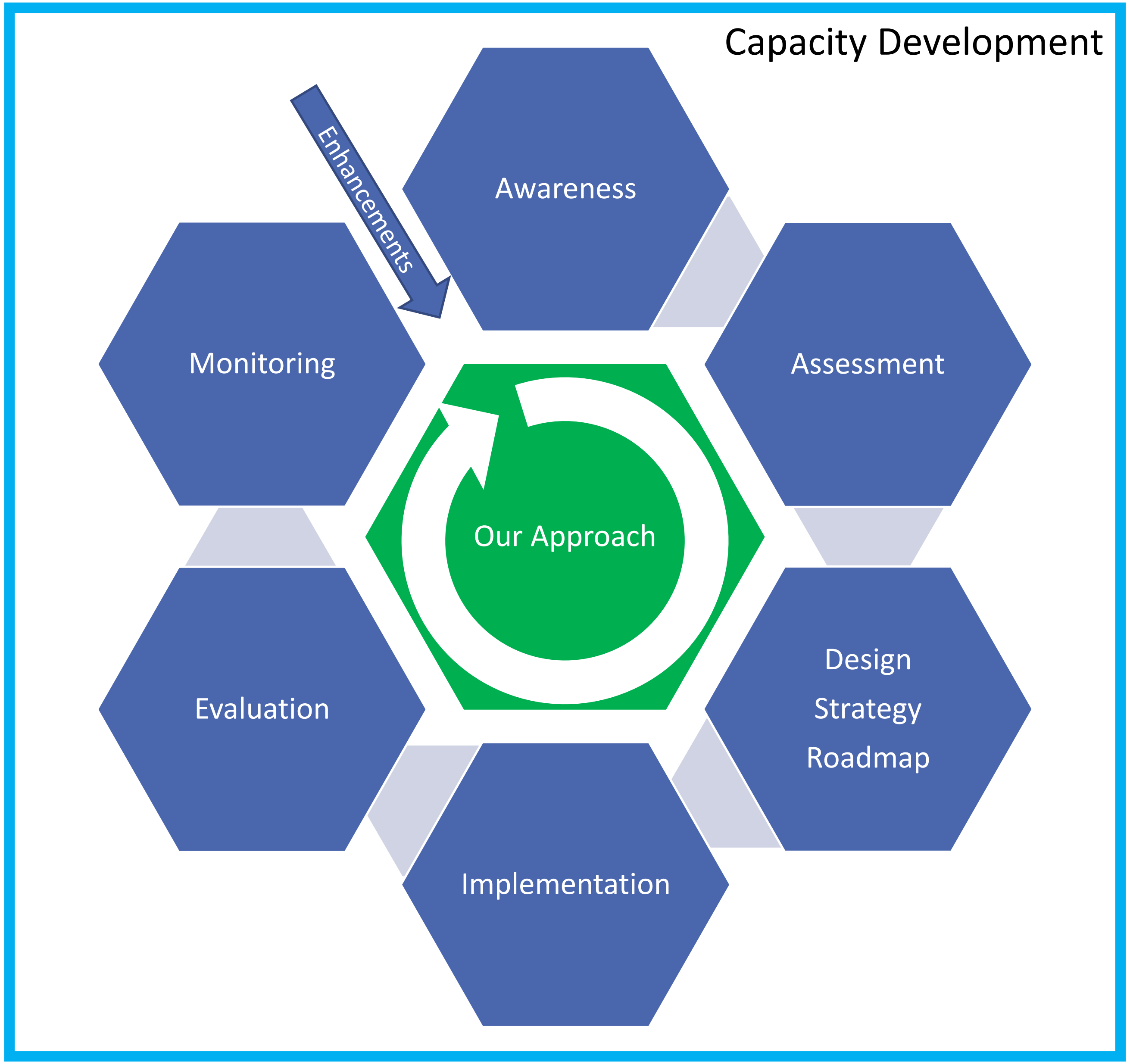
Feasibility
Study

Assessment

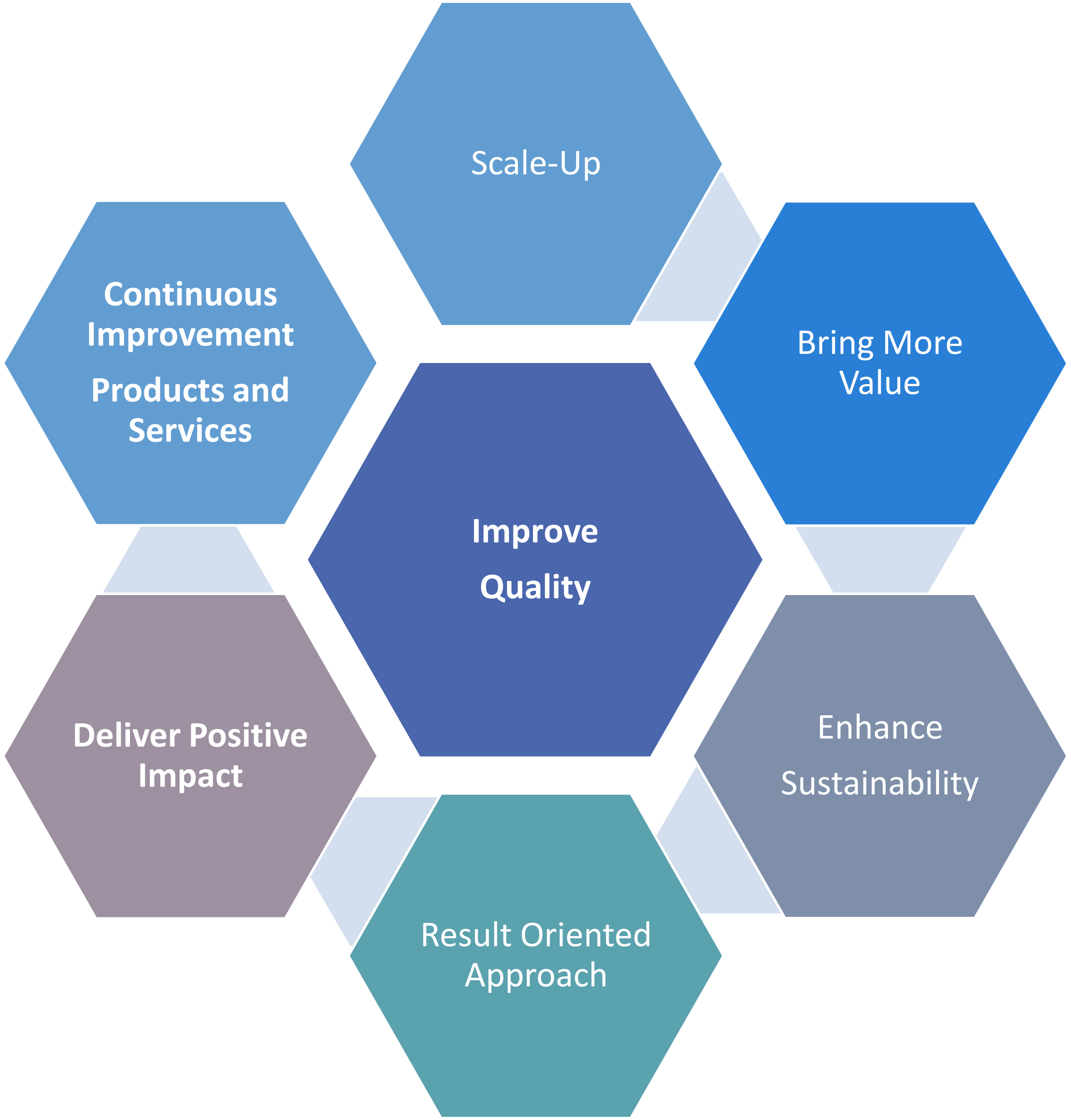
Policy

Readiness

Skills


Capacity Development
Enhancements
Awareness
Assessment
Design
Strategy
Roadmap
Implementation
Evaluation
Monitoring
Our Approach

Enhancements in our processes → Improve Quality



Improve Quality

Scale-Up

Bring More Value

Enhance Sustainability

Result Oriented Approach

Deliver Positive Impact

Continuous Improvement Products and Services

Who we work with?

- Member States
- Partner Organizations
- Private Sector Members
- Academia Sector Members
- Independent Experts

SOME OF THE ORGANIZATIONS WE WORK WITH ➔

ITU

FIRST
Improving Security Together

enisa
European Network and Information Security Agency

European Commission

NRD Cyber Security

unicri
United Nations Interregional Crime and Justice Research Institute

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

osce

guardtime

MERIDIAN
INTERNATIONAL CENTER

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

Regional Cooperation Council

Global Cyber Security Capacity Centre

POTOMAC INSTITUTE FOR POLICY STUDIES

ECS
EUROPEAN CYBER SECURITY ORGANISATION

issa

energypact
foundation

LONDON ACTION PLAN
INTERNATIONAL CYBERSECURITY ENFORCEMENT NETWORK

INDIANA UNIVERSITY

WORLD BANK GROUP

RCC

Deloitte.

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

GFCE
Global Forum on Cyber Expertise

CEDEAO
ECOWAS

DCAF
DCAF
a centre for security, development and the rule of law

CTO
COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Symantec

UNDESA

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERPOL

UNITED NATIONS
UNCTAD

GLOBAL CYBER ALLIANCE

Internet Society™

The Commonwealth

Bitdefender

Microsoft

KASPERSKY lab

UNODC
United Nations Office on Drugs and Crime

Thank you for your attention

Farid Nakhli,
Programme Officer
ITU Regional Office for CIS
farid.nakhli@itu.int