ITU Regional Workshop on "Strengthening Capacities in Internet Governance in the Arab region

Rouda AlAmir Ali
ITU

Manama, Bahrain
1-3 October 2019

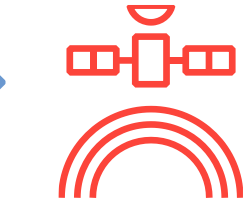
ITU at a glance

Meet us

What we do

‘Committed to Connecting the World’

3 Sectors



ITU Radiocommunication

Coordinating radio-frequency spectrum and **assigning** orbital slots for satellites

ITU Standardization

Establishing global standards

ITU Development

Bridging the digital divide

193 **+700** **+150**

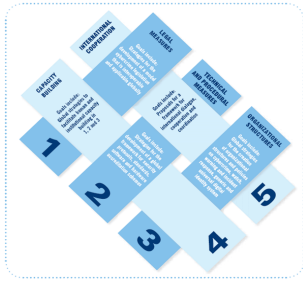
MEMBER STATES | INDUSTRY & INTERNATIONAL ORGANIZATIONS | ACADEMIA MEMBERS

MEMBERSHIP

ITU Mandate on Cybersecurity

2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - "**Building Confidence and Security in the use of ICTs**"

world summit on the information society
Geneva 2003 - Tunis 2005



2007
Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
GCA is a **framework for international cooperation in cybersecurity**

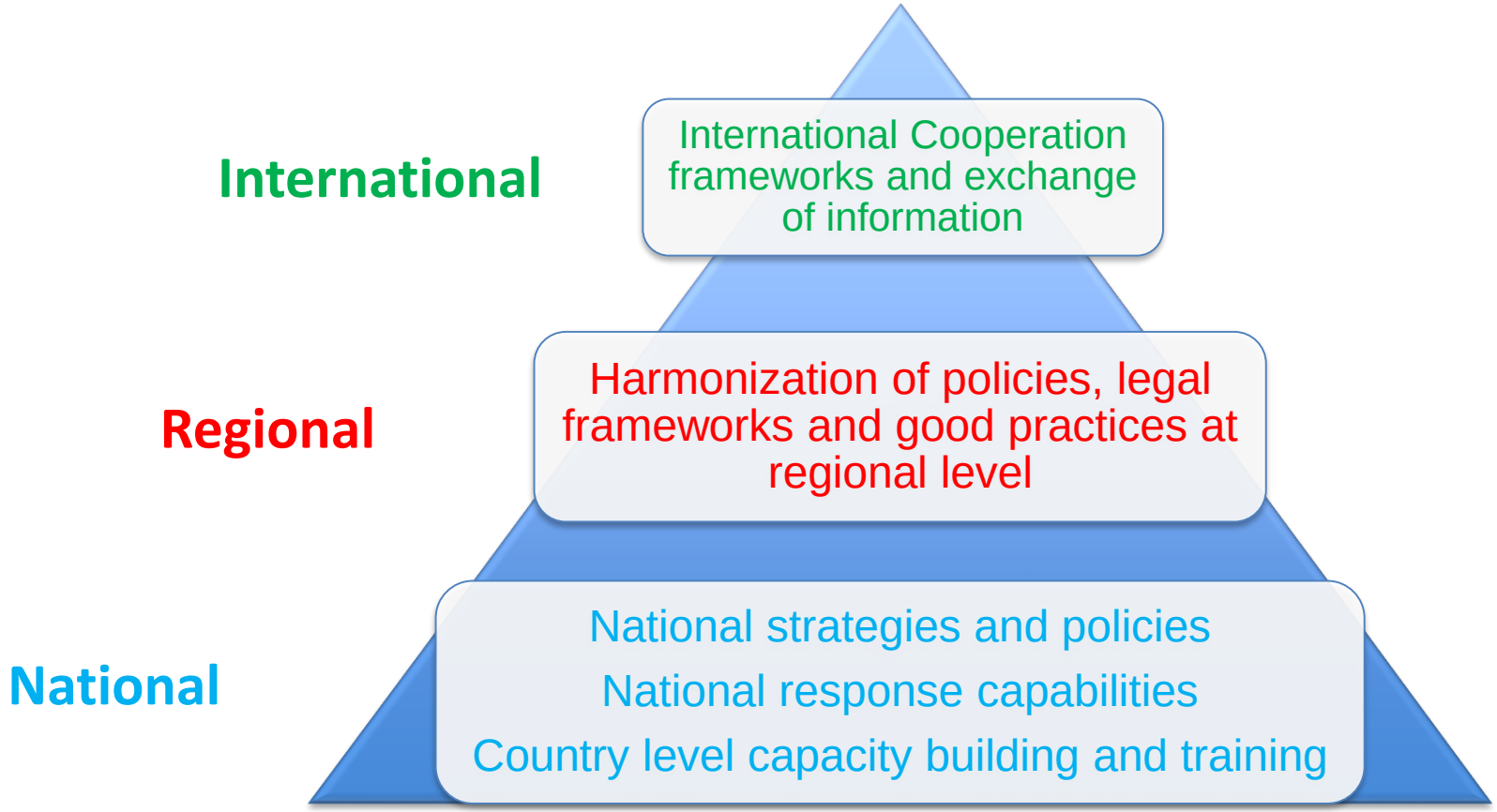
2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

GCA GLOBAL CYBERSECURITY AGENDA

Building confidence and security in the use of ICTs is widely present in **PP and Conferences**' resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

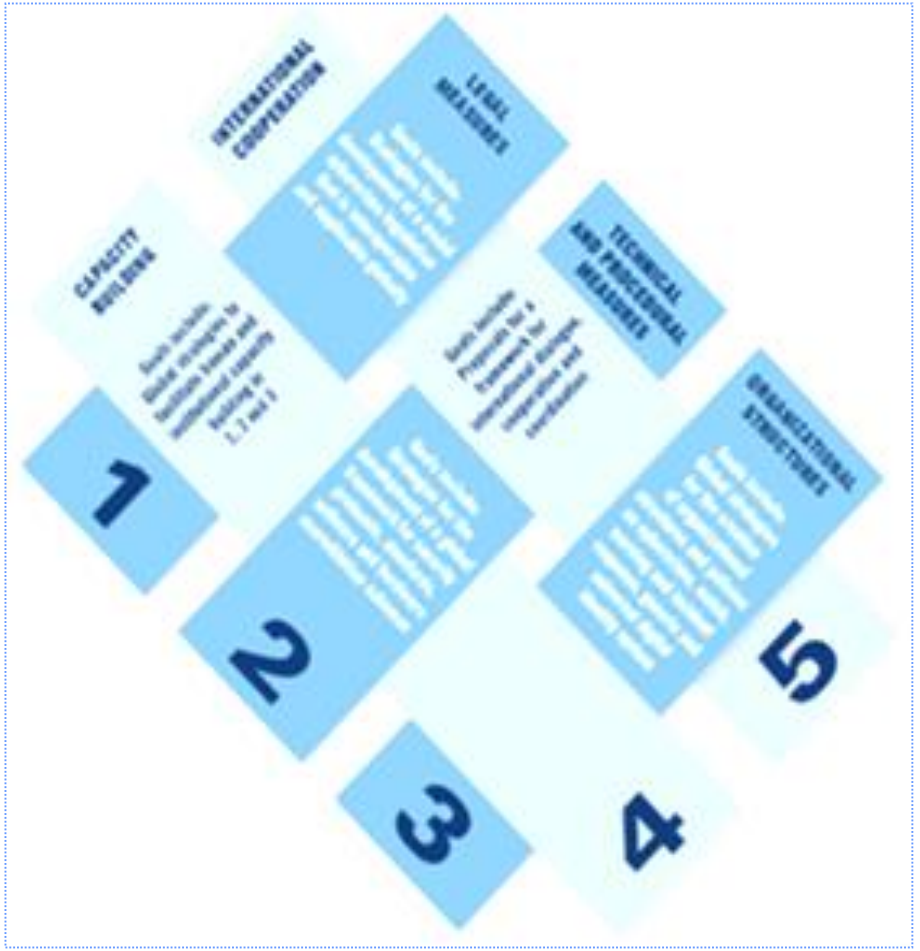
Coordinated Response

Need for a multi-level response to the cybersecurity challenges



Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
  1. Legal Measures
  2. Technical and Procedural Measures
  3. Organizational Structure
  4. Capacity Building
  5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.



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

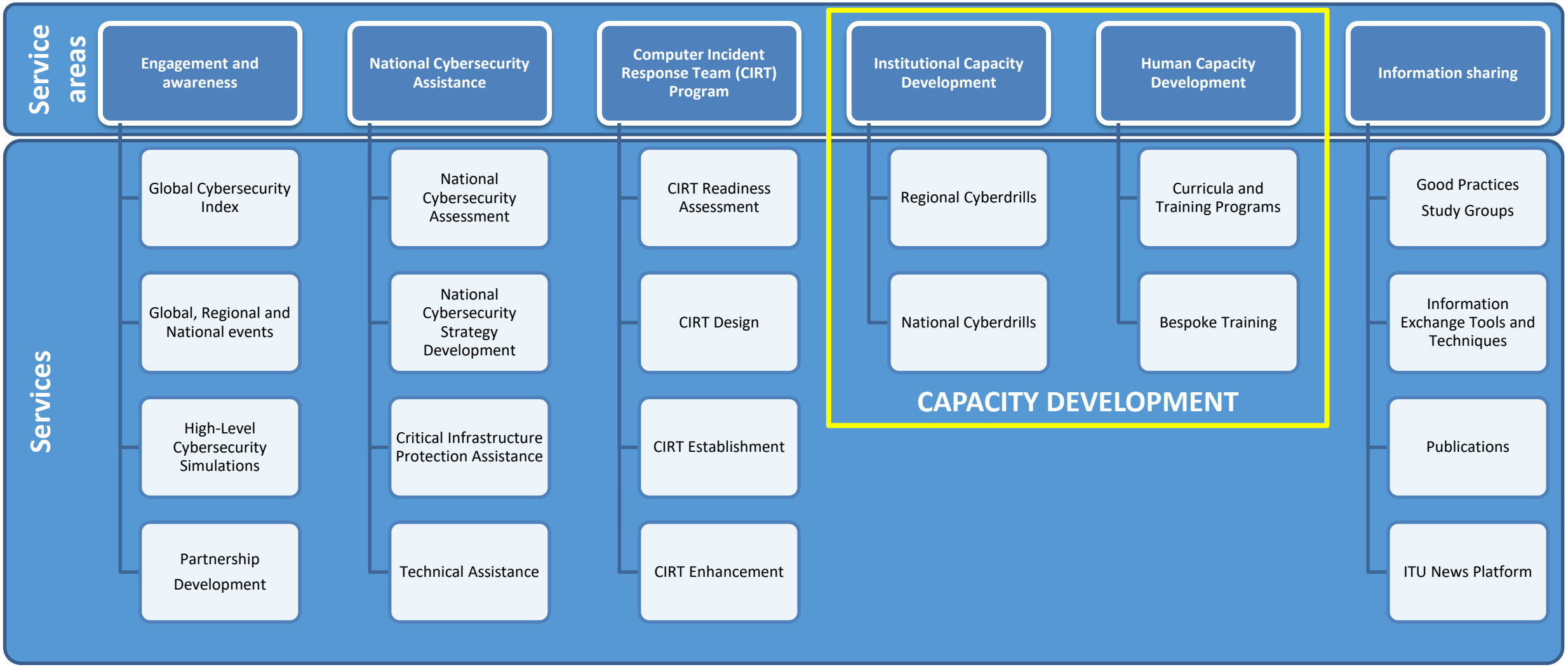
Information Sharing

Capacity Development

Partnership Development

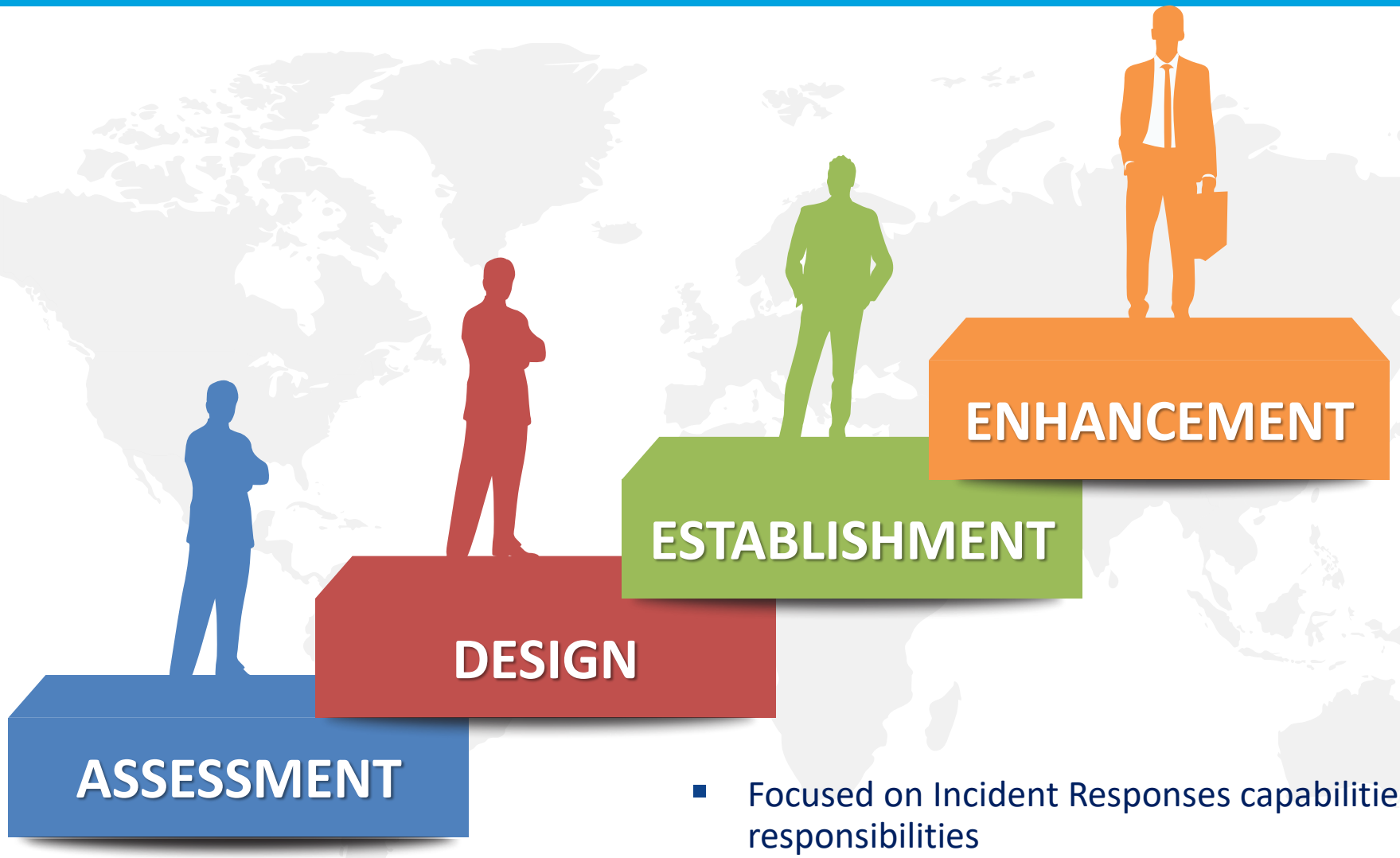
Product Development

Cybersecurity Services Catalogue



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

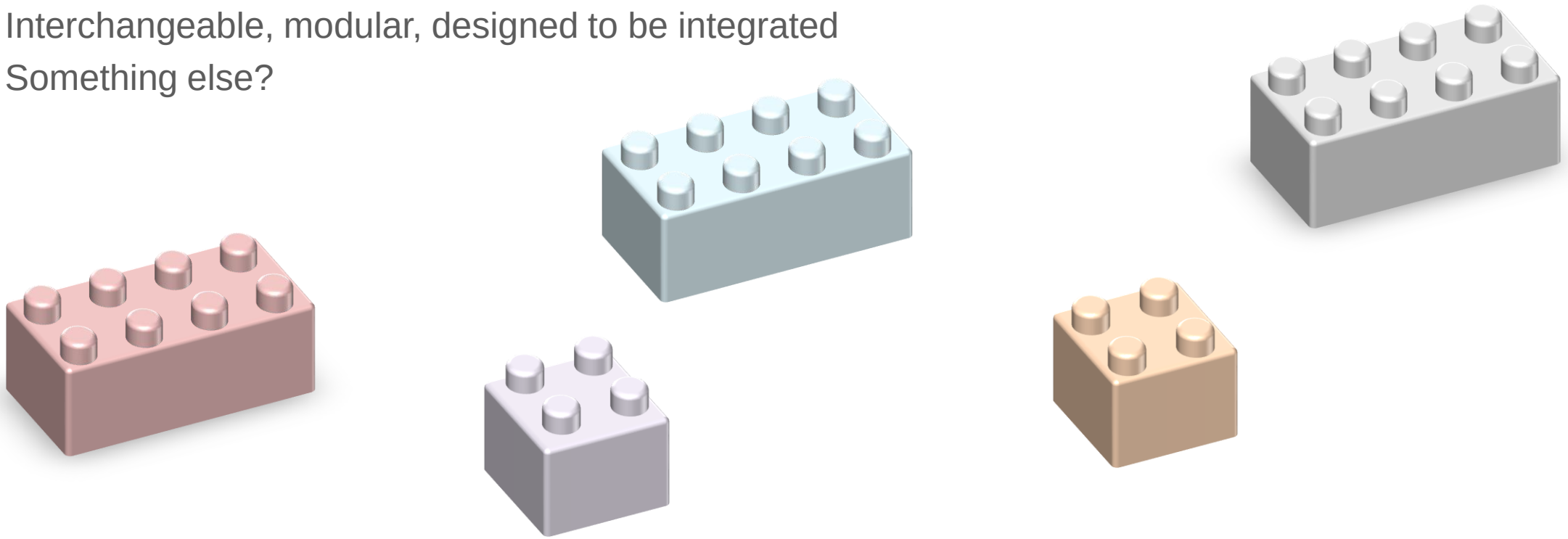
Typical enhanced services that a National CIRT may provide to its constituents:

- 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

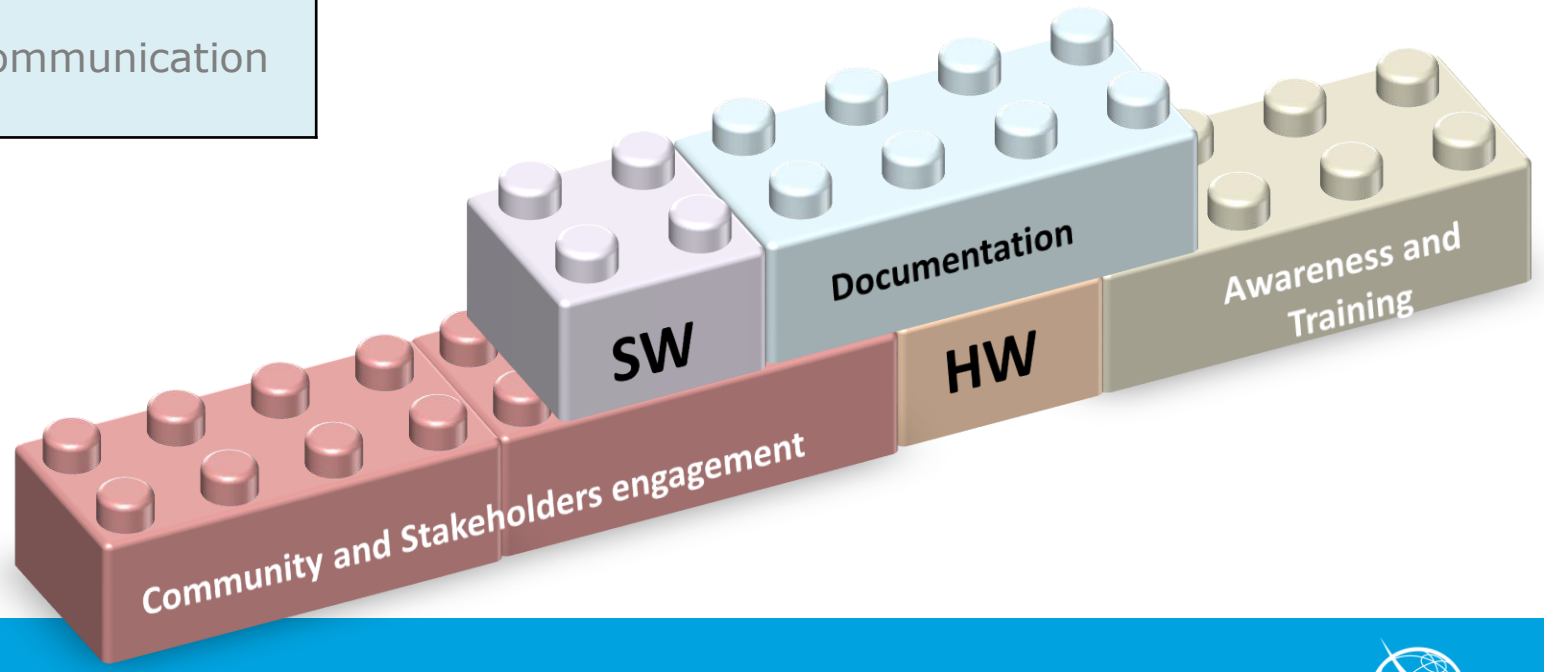
Notion of building blocks

- 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?

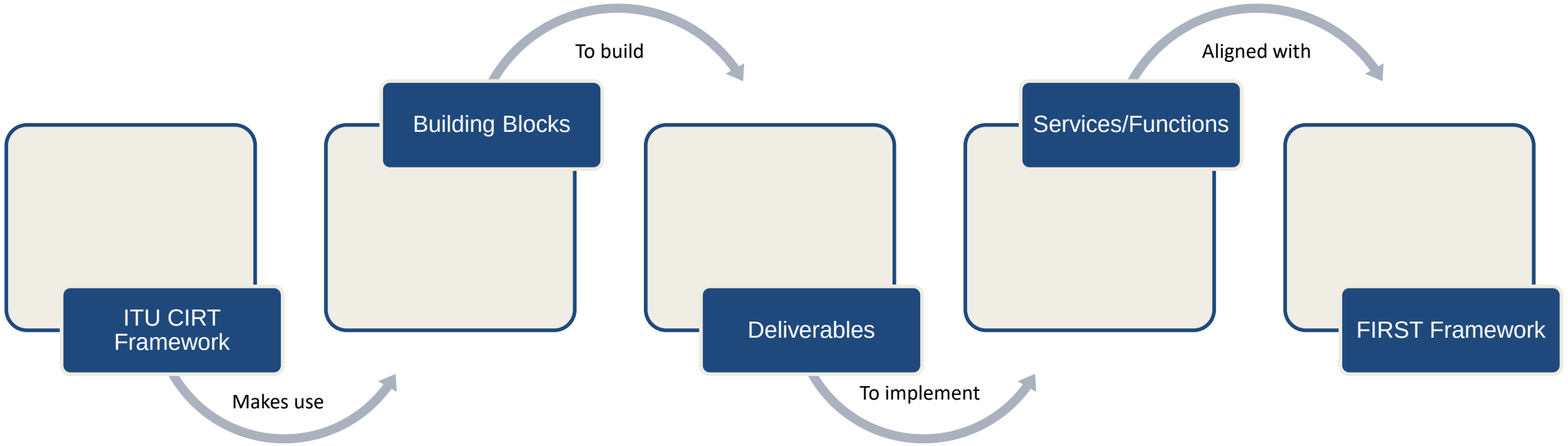


Typology of Building Blocks

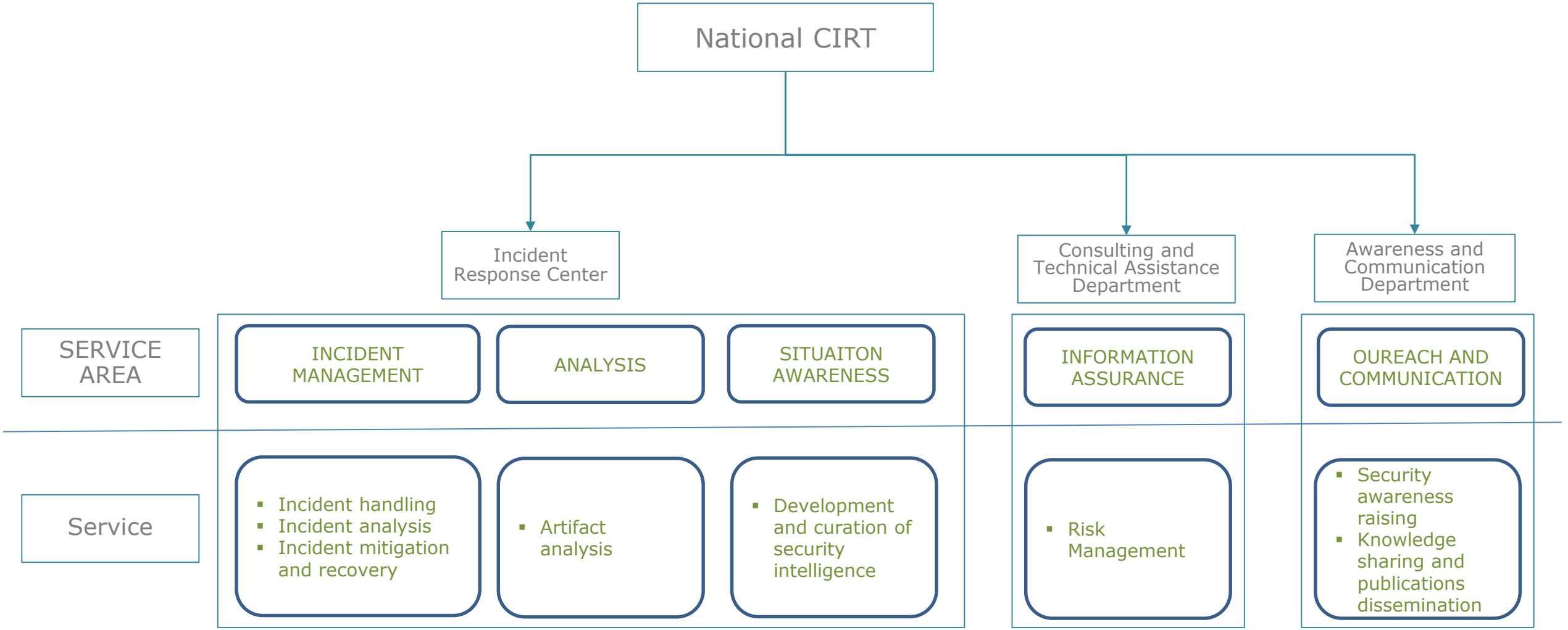
HW	▪ Appliances ▪ Network devices ▪ Desktops, laptops ▪ Cables
SW	▪ RTIR ▪ Tools for malware analysis ▪ Office automation tools
Documentation	▪ Policies (Internal security policy, data and incident classification, org charts, job profiles) ▪ Templates, manuals, communication material
Awareness and training	▪ Presentations ▪ Books ▪ Training lab ▪ Manuals ▪ Communication material
Community and stakeholders engagement	▪ FIRST Membership ▪ Outreach plan ▪ Announcement plan



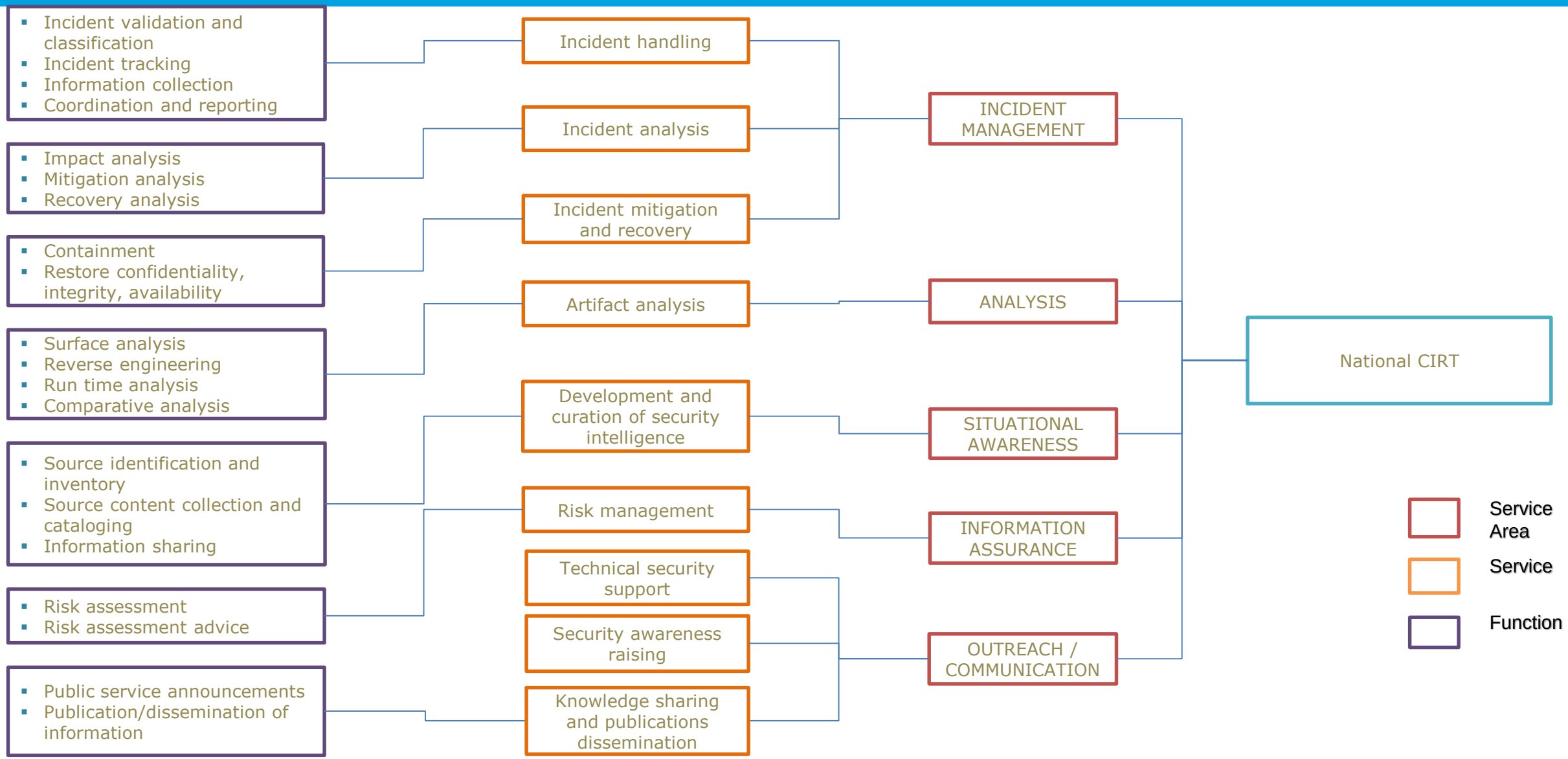
ITU CIRT Framework applied



The Basic Services Offered by a National CIRT

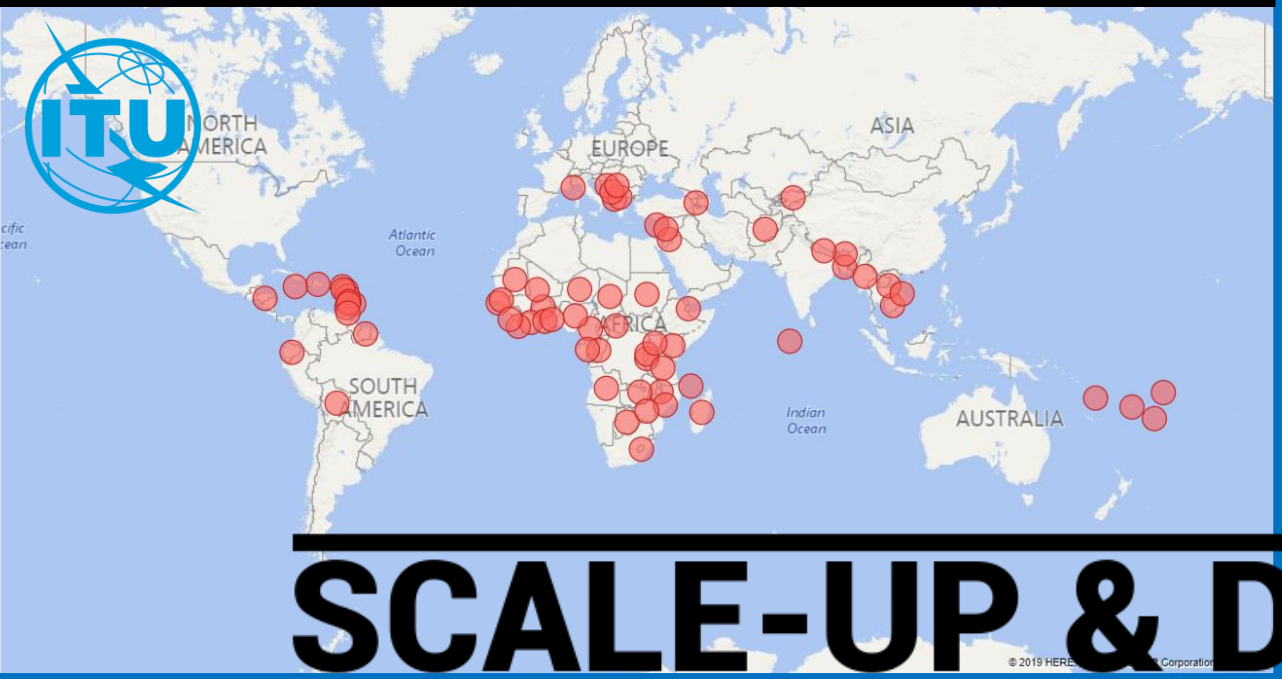


CIRT Services (FIRST)



ITU CIRT Framework Activities

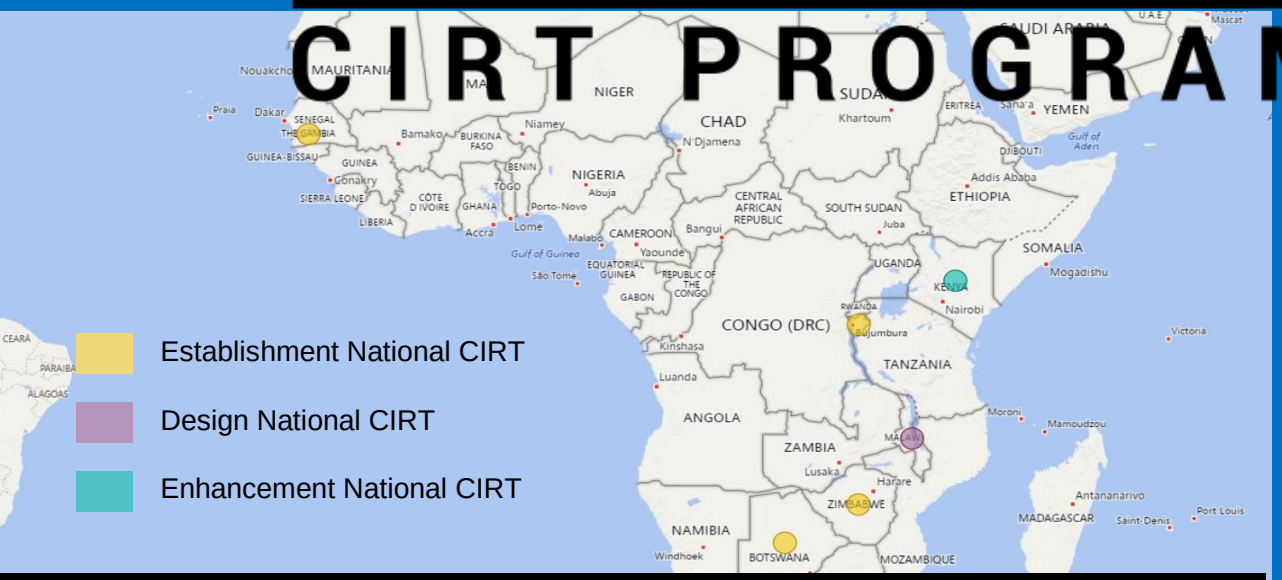
75 CIRT READINESS ASSESSMENTS



13 CIRT ESTABLISHMENT + 1 ENHANCEMENT

SCALE-UP & DELIVER MORE

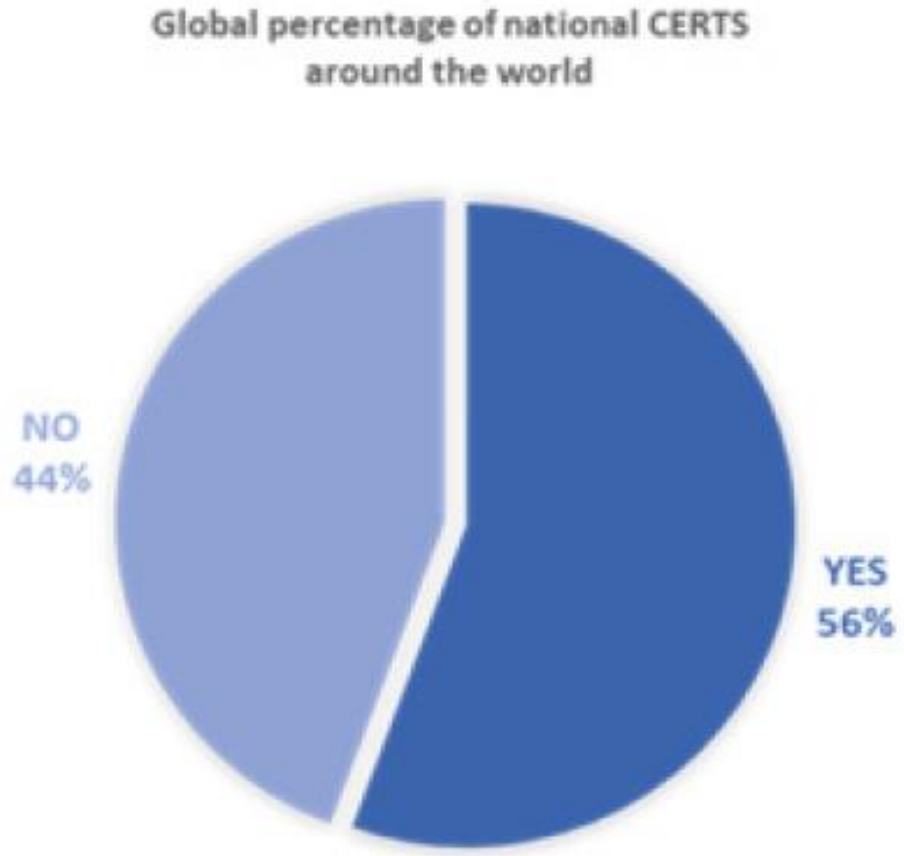
CIRT PROGRAMME EXAMPLE

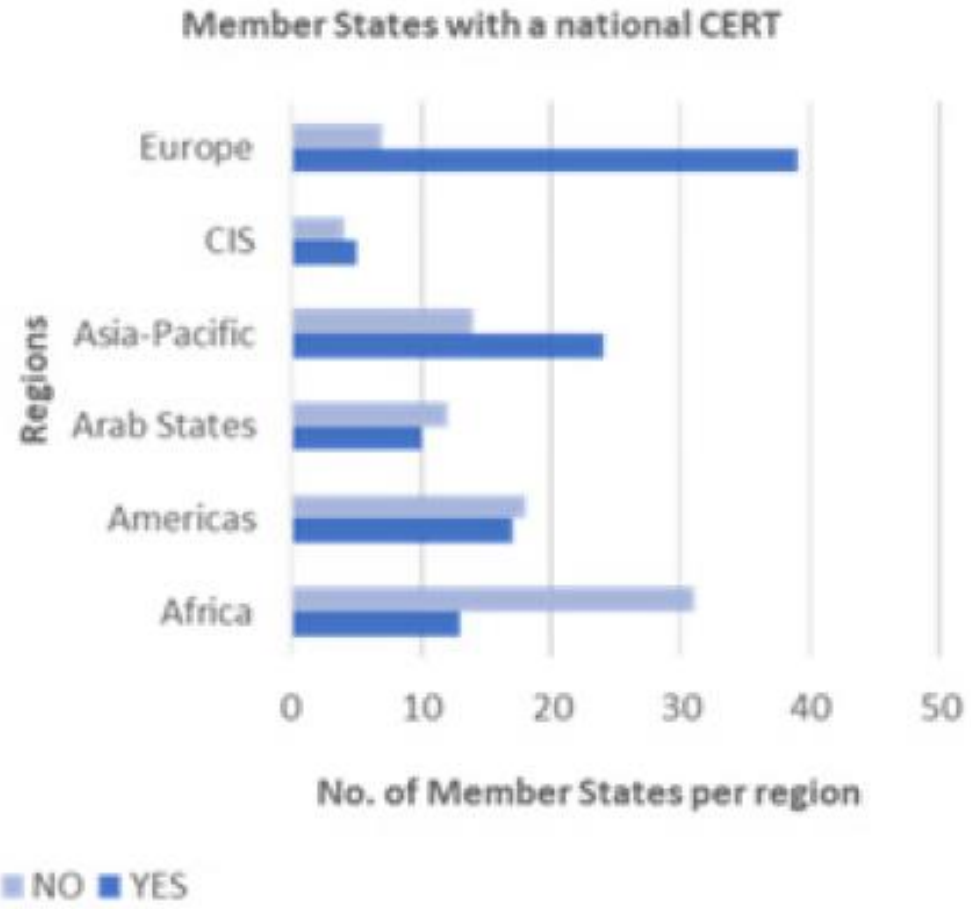


CIRT ESTBLISHMENT IN 2019

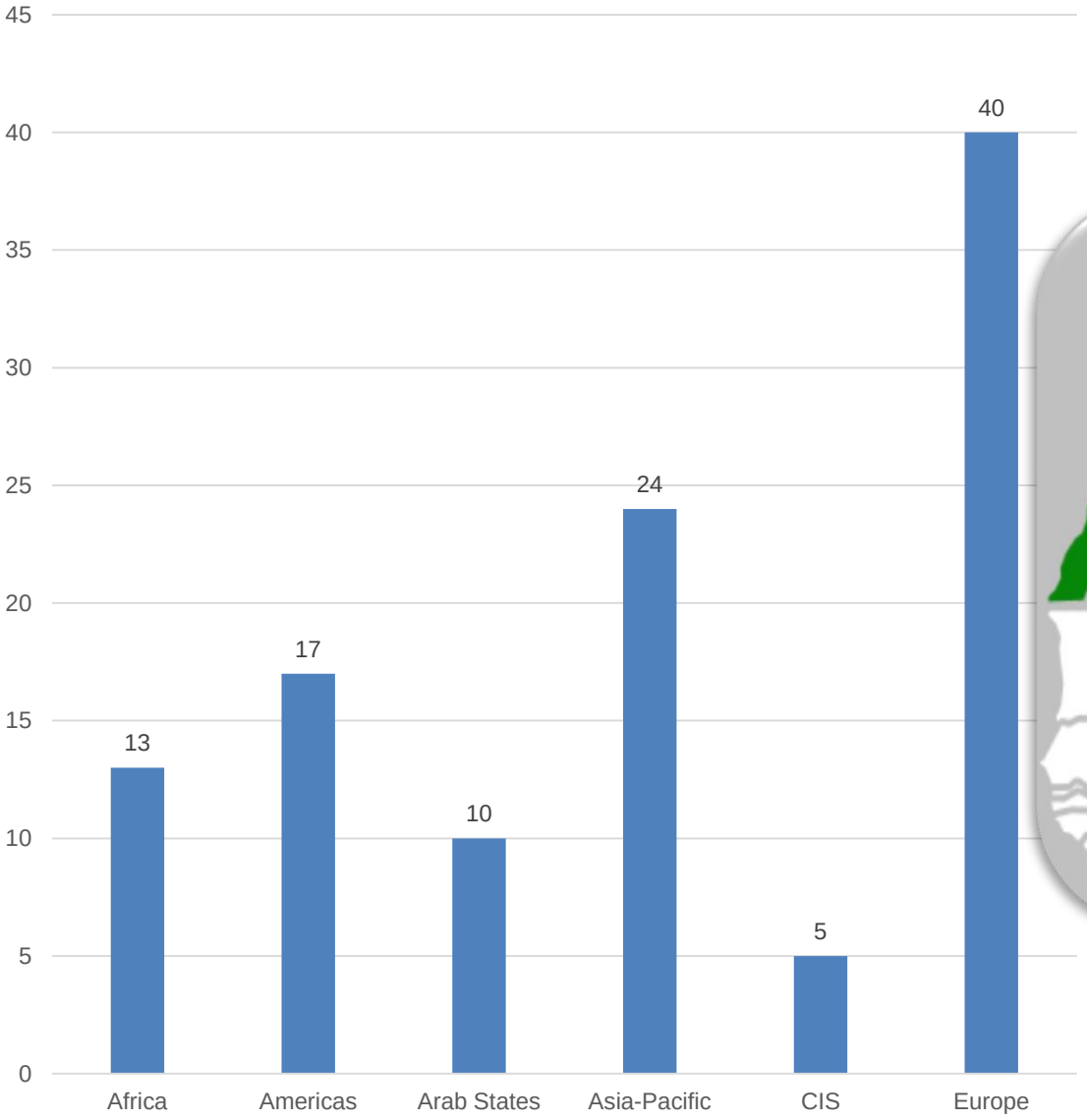
CIRT ESTABLISHMENT– INTERESTS

National CERT/CIRT/CSIRT globally and per region





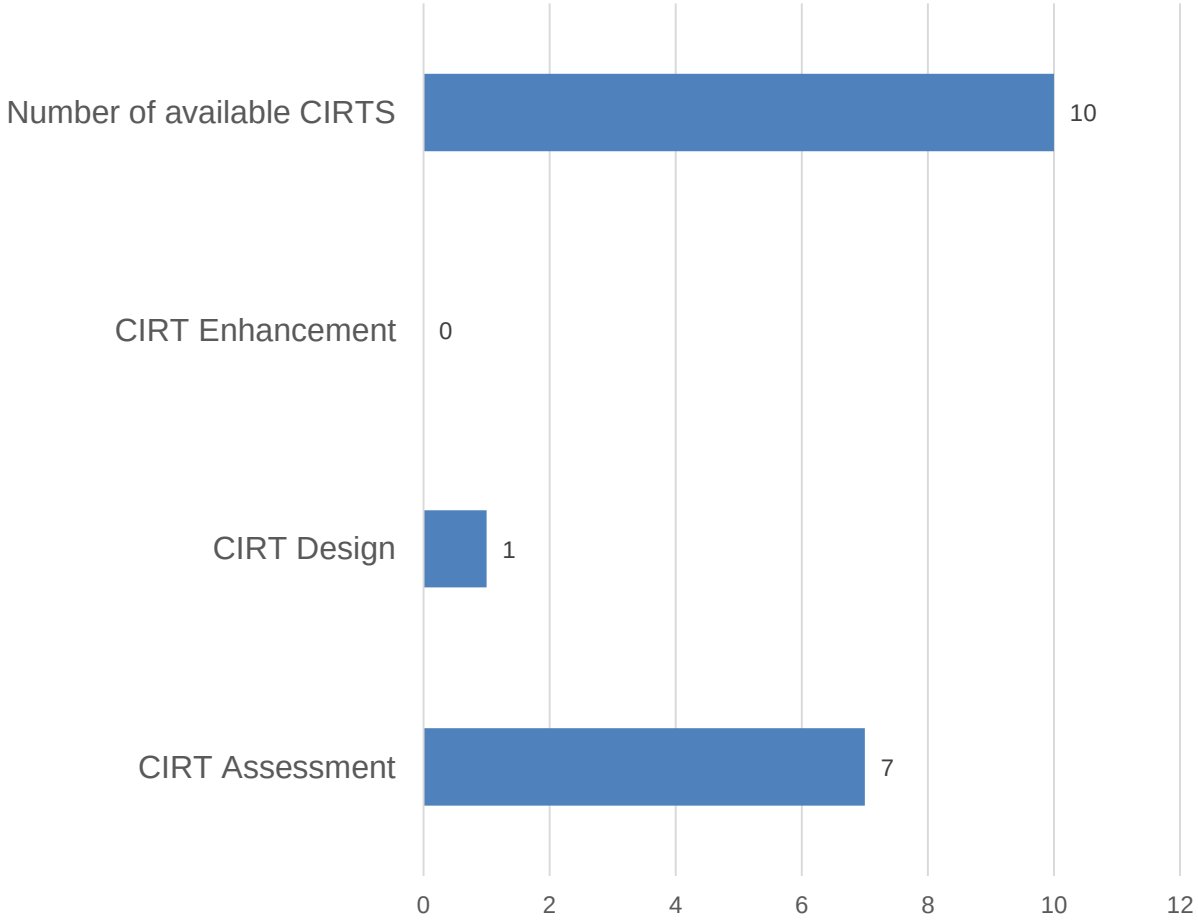
Number of CIRT activities around the world



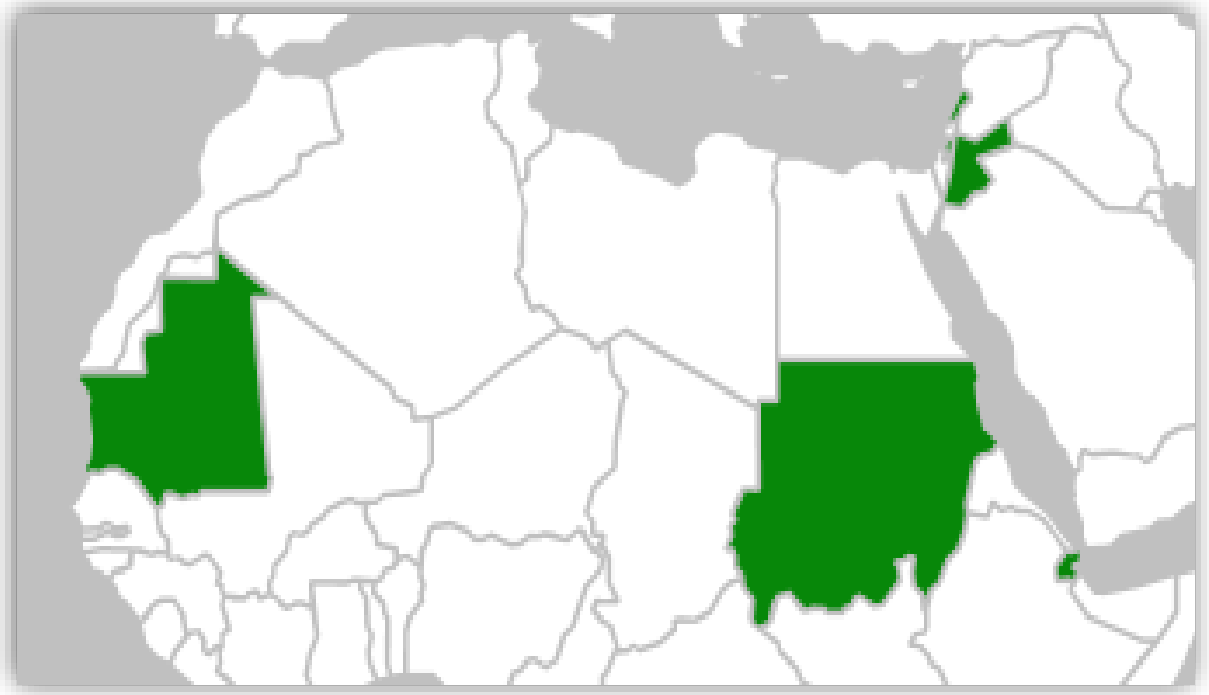
CIRTs in Arab States:

Egypt, Libya, Morocco, Oman, Qatar, Saudi Arabia, Sudan, Syrian Arab Republic, Tunisia, United Arab Emirates

Good Practices: An analysis of the Arab States CIRT establishment



7 CIRT assessment done by ITU in Arab States :
Comoros, Djibouti, Jordan, Lebanon, Mauritania, Palestine, Sudan



ITU : I Thank U