Deployment of a National CIRT

Pablo Palacios

Programme Officer

Cybersecurity Focal Point AMS

International Telecommunication Union

21 November 2022

Several Services

Facilitating a trusted cyberspace for All

- CIRT Implementation
- National Cybersecurity Strategy
- SIM 3 Assessment
- Cyberdrills
- CIRT Enhancement
- Support 6 Months after implementation
- CMM Maturity Model Assessment
- Global Cybersecurity Index
- International Cooperation
- Aligned with FIRST
- Hornet
- Capacity Building

Cybersecurity - ITU's Solution

Assessing

Benchmarking

Key metrics

Assessment exercises

Strategy principles and good practices

National readiness to establish national CIRT capabilities

Improving

Improving capacity

Least Developed & Developing Countries

Cooperation and coordination

Regional

International

National

Developing

Development national strategies

Address cybersecurity threats

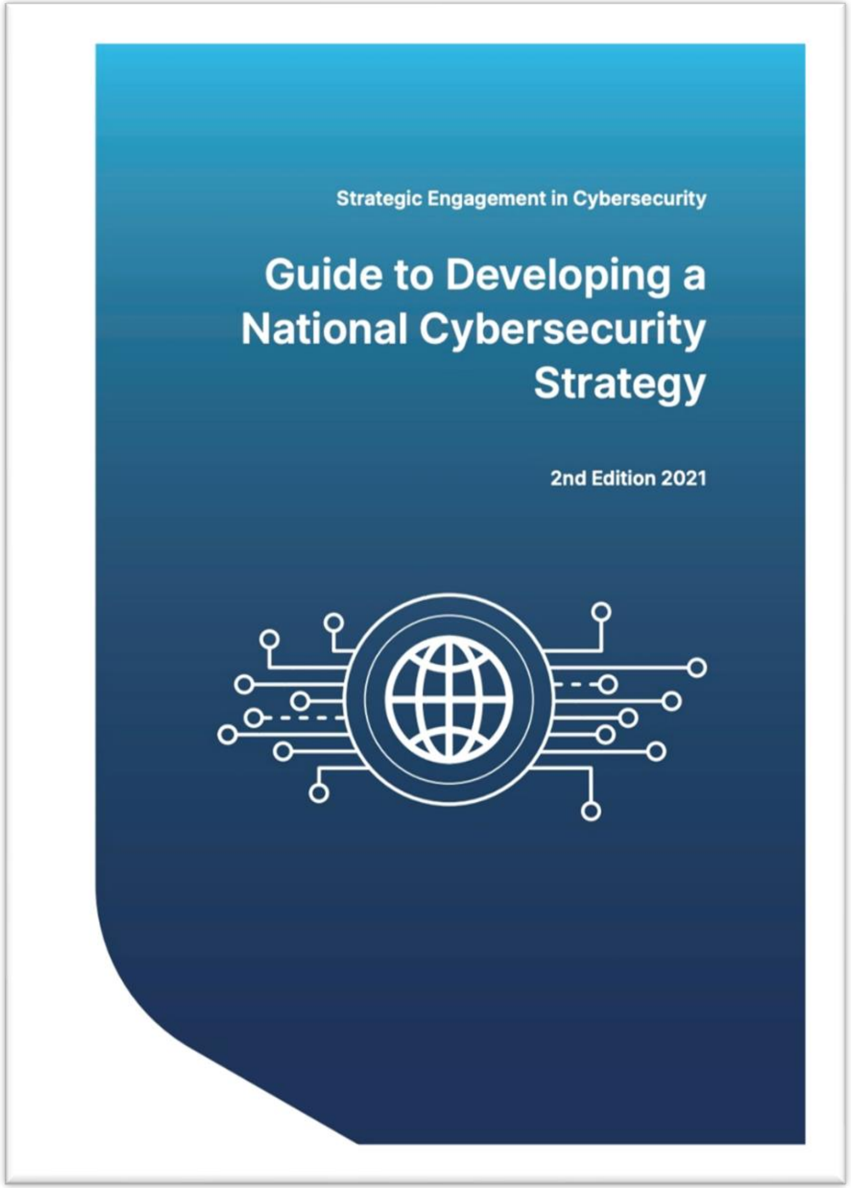
Practical

Hand-on trainings

Incident response

Establishment National CIRTs

National Cybersecurity Strategy (NCS)



Strategic Engagement in Cybersecurity

Guide to Developing a National Cybersecurity Strategy

2nd Edition 2021

NCS Activities

Development of NCS

Address risks

Supporting Member States

Transfer Knowledge

Formative resources

Facilitating Dialogue

NCS Assistance

Assessment of cybersecurity risks and landscape

Facilitate NCS development

Facilitate implementation

Trainings

Formative activities

Human capacity development

Technical assistance

NCS Framework

Guide to developing NCS

NCS Lifecycle

Overarching principles

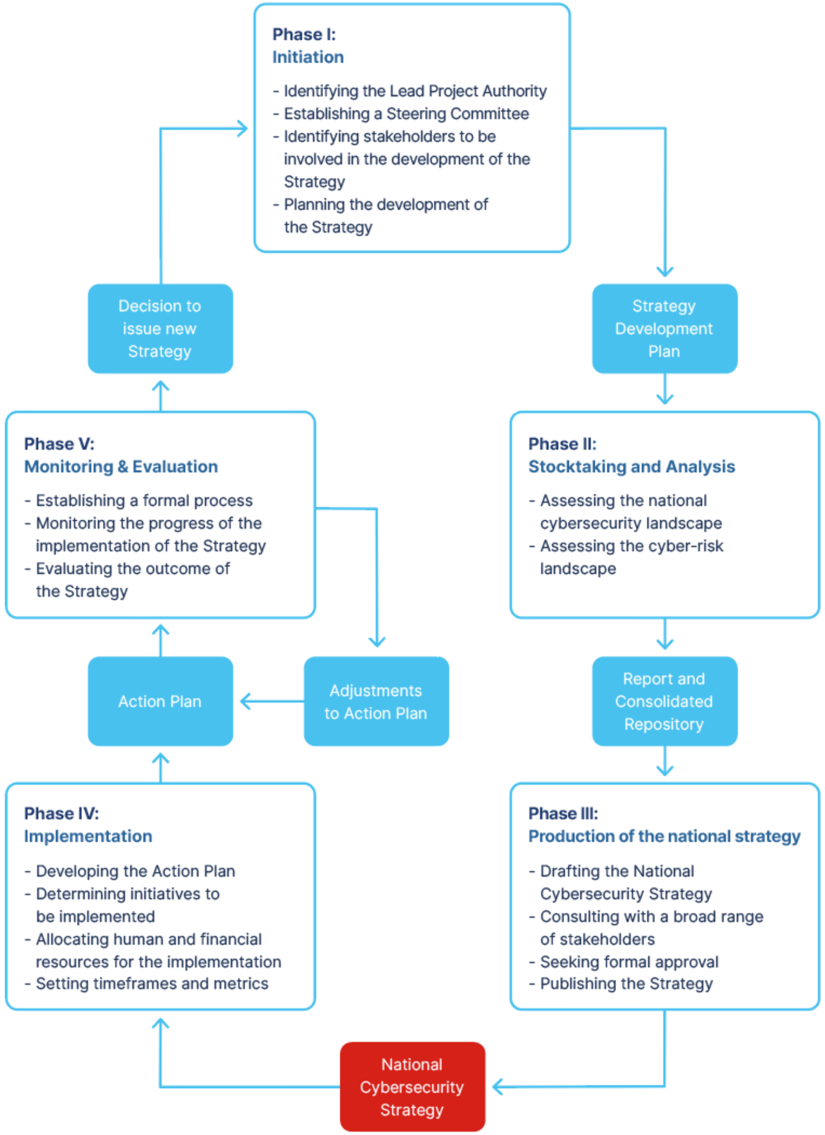
Best Practices

https://academy.itu.int/

Lifecycle, principles and good-practices on national cybersecurity strategy development and implementation

National cybersecurity strategy

Figure 1 - Lifecycle of a National Cybersecurity Strategy



Phase I:
Initiation

- Identifying the Lead Project Authority
- Establishing a Steering Committee
- Identifying stakeholders to be involved in the development of the Strategy
- Planning the development of the Strategy

Strategy Development Plan

Phase II:
Stocktaking and Analysis

- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape

Report and Consolidated Repository

Phase III:
Production of the national strategy

- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy

National Cybersecurity Strategy

Phase IV:
Implementation

- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics

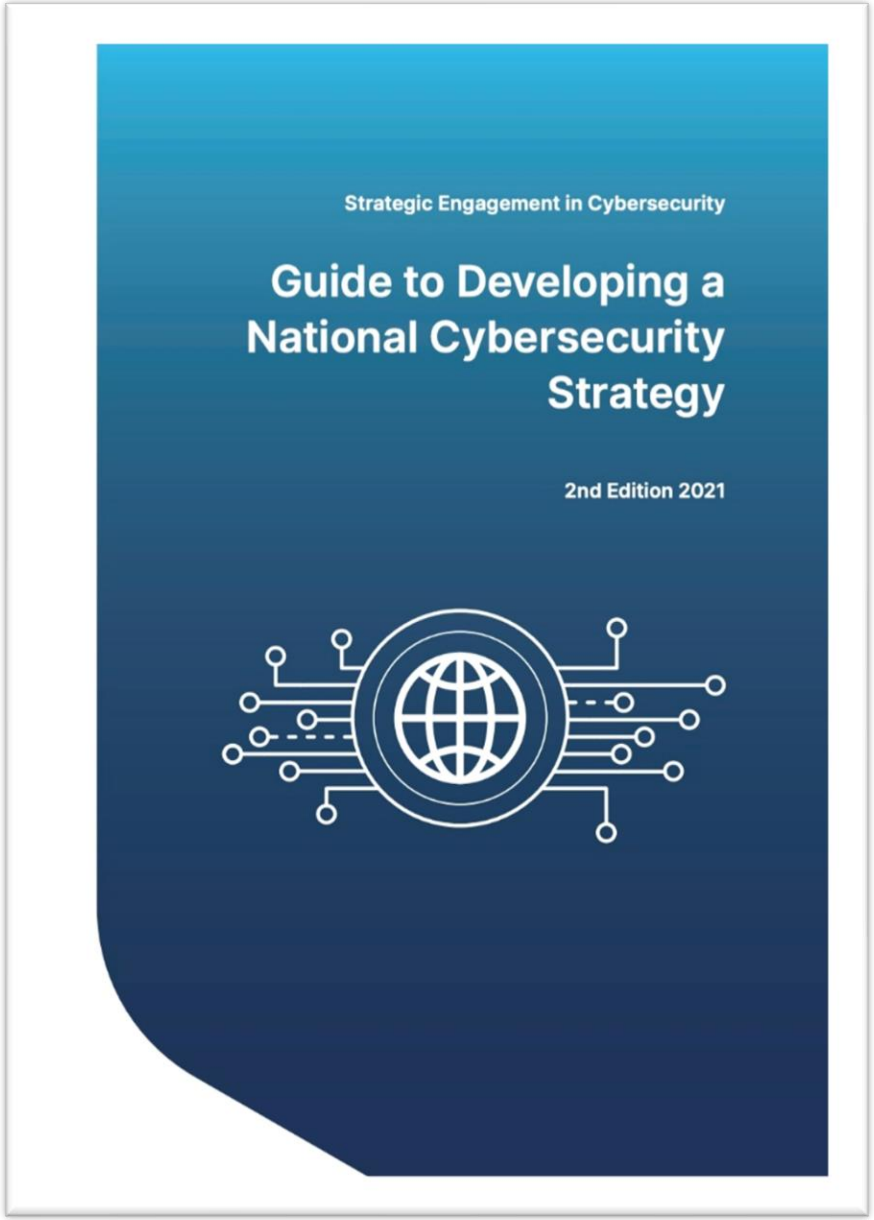
Action Plan

Adjustments to Action Plan

Phase V:
Monitoring & Evaluation

- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy

Decision to issue new Strategy



Strategic Engagement in Cybersecurity

Guide to Developing a National Cybersecurity Strategy

2nd Edition 2021

National, Regional and Global CyberDrills

CyberDrill Objectives

As a **platform for cooperation**, information sharing, and discussions on current cybersecurity issues, and

Provide hands-on exercises for national Cyber Incident Response Teams CIRTs/CERTs/CSIRTs.

32 **Exercises were conducted**

140+ **Countries participated in ITU CyberDrills**

10 Cyberdrills in: Uruguay, Colombia, Ecuador, Peru, Argentina, Suriname, Honduras
Next in 2023?

CIRT implementation

ITU CIRT Framework application in projects are geared:

To enable a National CIRT (or sectorial).

Serve as a trusted and central coordination point of contact for cybersecurity.

Identifying, defending, responding to, and managing cyber threats.

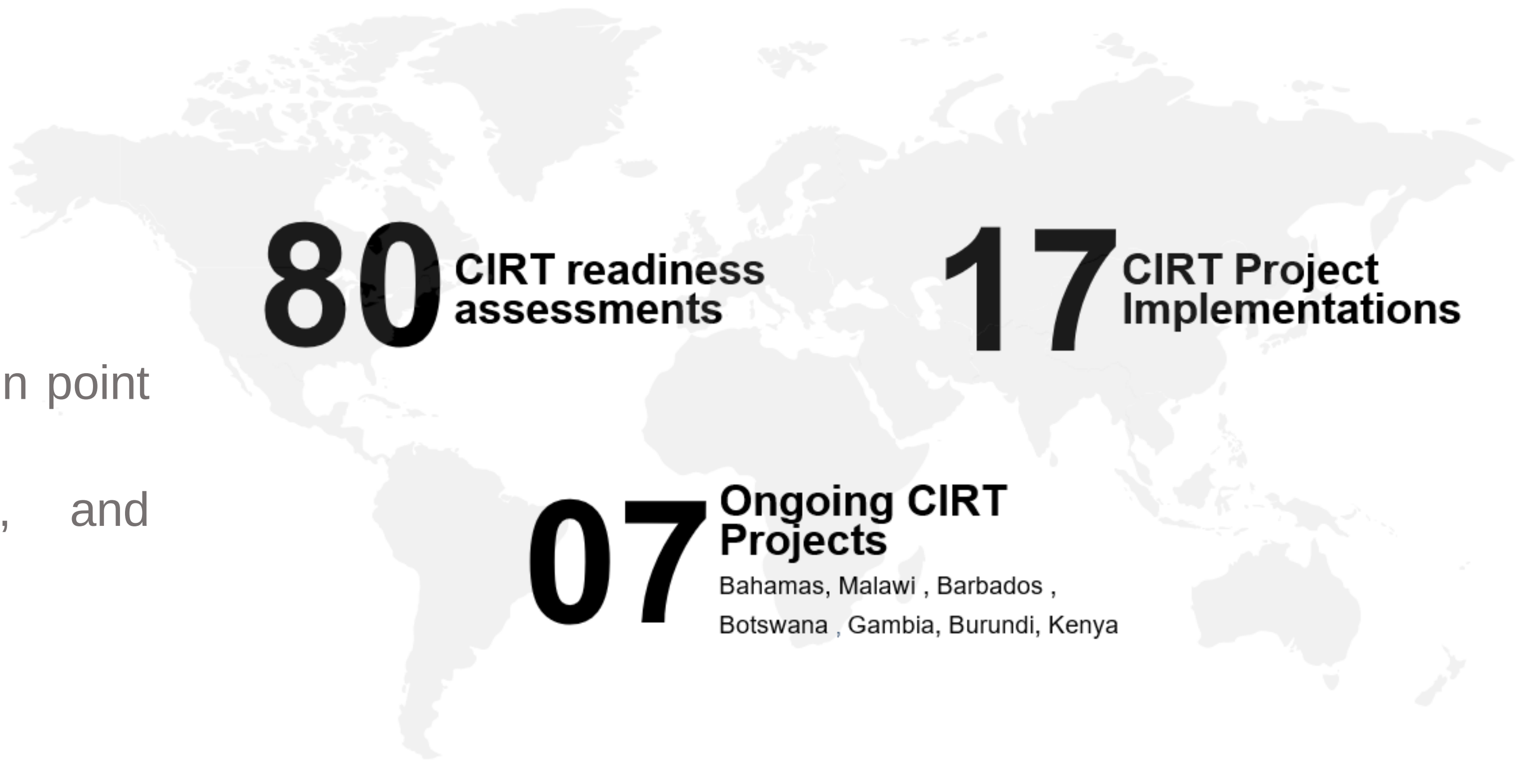
Basic set of services:

Incident Handling

Incident Analysis

Outreach/Communication

Enhanced services: Situation Awareness, Digital Forensics and other services.



80 CIRT readiness assessments

17 CIRT Project Implementations

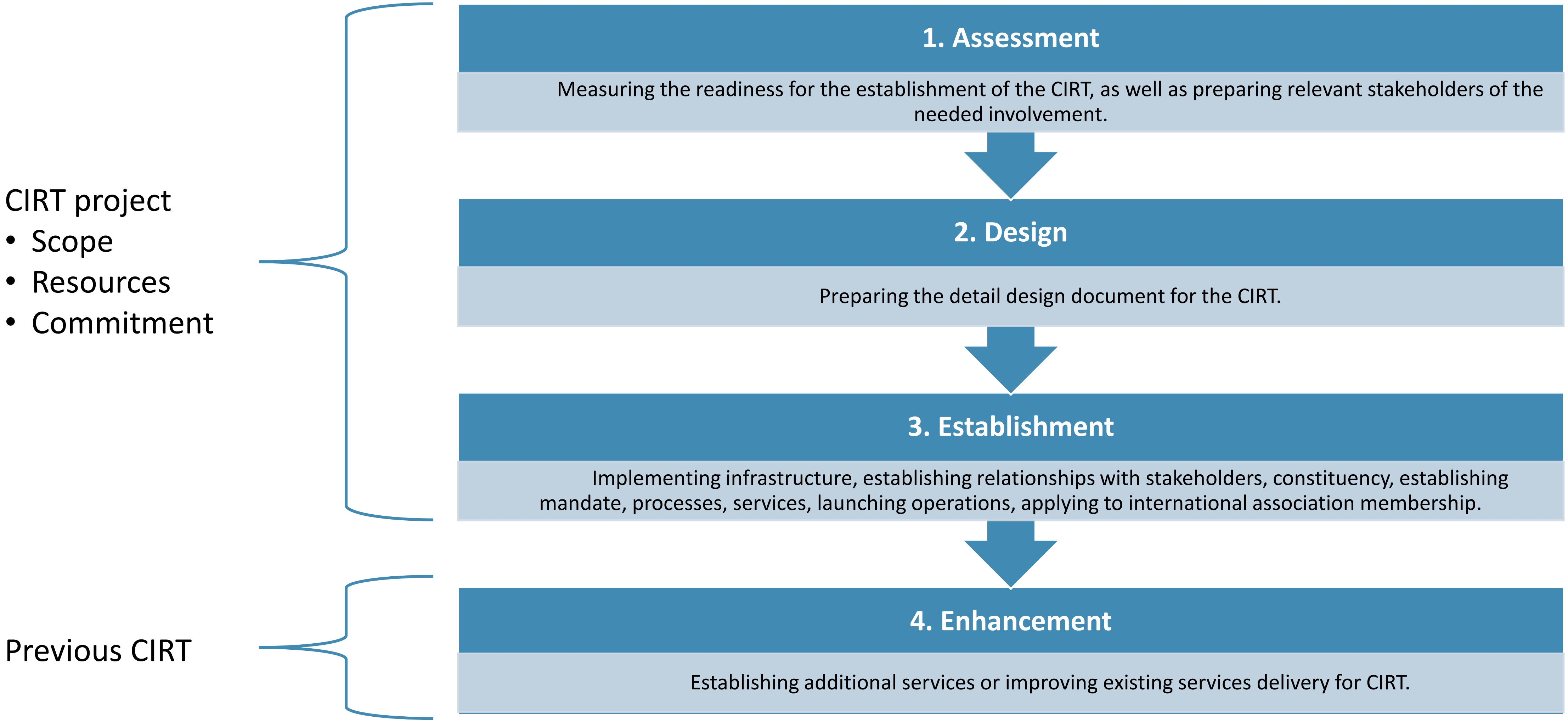
07 Ongoing CIRT Projects

Bahamas, Malawi , Barbados , Botswana , Gambia, Burundi, Kenya

Barbados, Bahamas, Trinidad and Tobago, Jamaica

Cybersecurity Activities: Guyana, Suriname, Ecuador, Paraguay…

Framework Structure and Phases



CIRT project

- Scope
- Resources
- Commitment

Previous CIRT

1. Assessment

Measuring the readiness for the establishment of the CIRT, as well as preparing relevant stakeholders of the needed involvement.

2. Design

Preparing the detail design document for the CIRT.

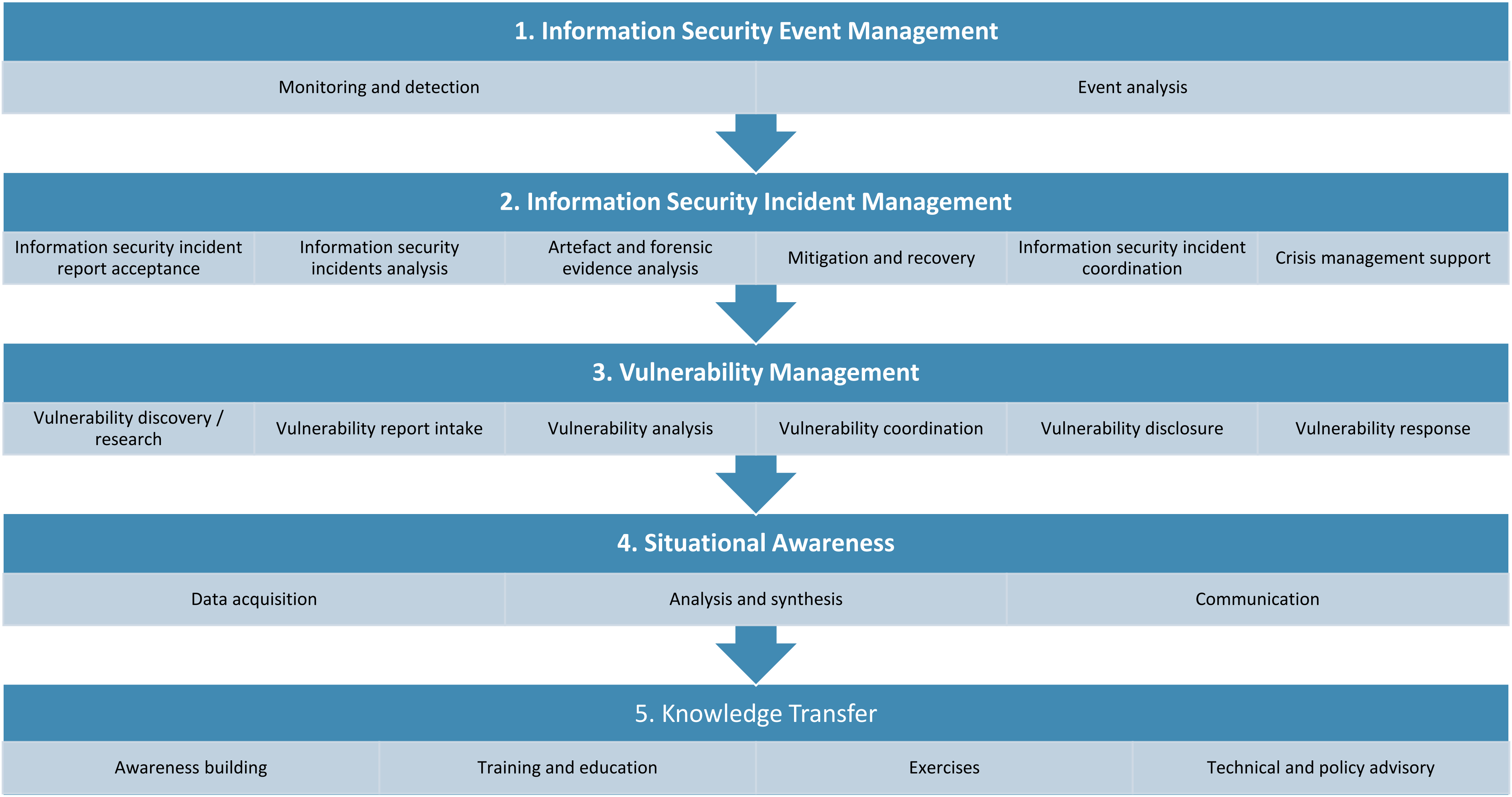
3. Establishment

Implementing infrastructure, establishing relationships with stakeholders, constituency, establishing mandate, processes, services, launching operations, applying to international association membership.

4. Enhancement

Establishing additional services or improving existing services delivery for CIRT.

Primary Services



1. Information Security Event Management

- Monitoring and detection
- Event analysis

2. Information Security Incident Management

- Information security incident report acceptance
- Information security incidents analysis
- Artefact and forensic evidence analysis
- Mitigation and recovery
- Information security incident coordination
- Crisis management support

3. Vulnerability Management

- Vulnerability discovery / research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

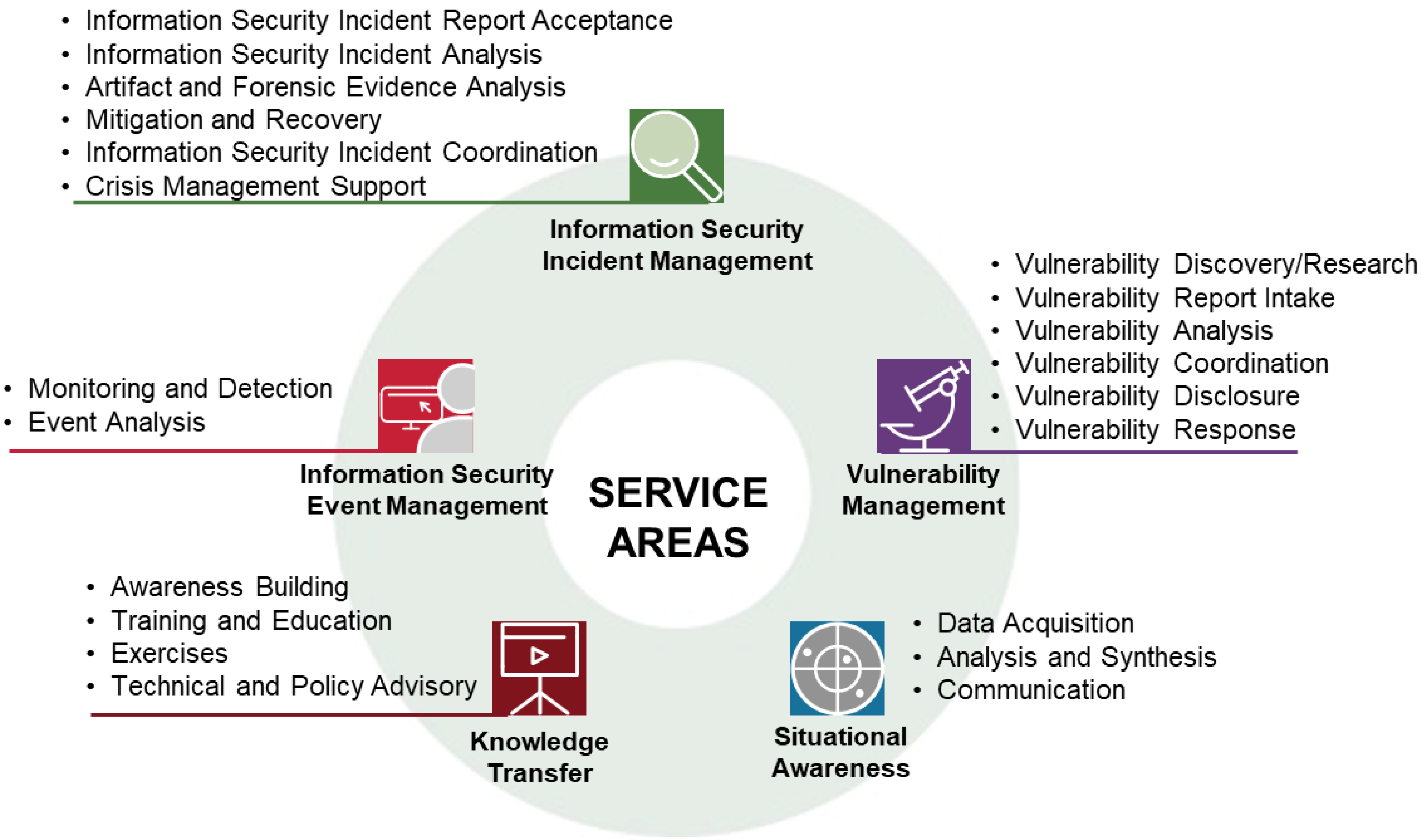
4. Situational Awareness

- Data acquisition
- Analysis and synthesis
- Communication

5. Knowledge Transfer

- Awareness building
- Training and education
- Exercises
- Technical and policy advisory

CIRT Services



- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

Information Security Incident Management

- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

Vulnerability Management

- Monitoring and Detection
- Event Analysis

Information Security Event Management

SERVICE AREAS

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

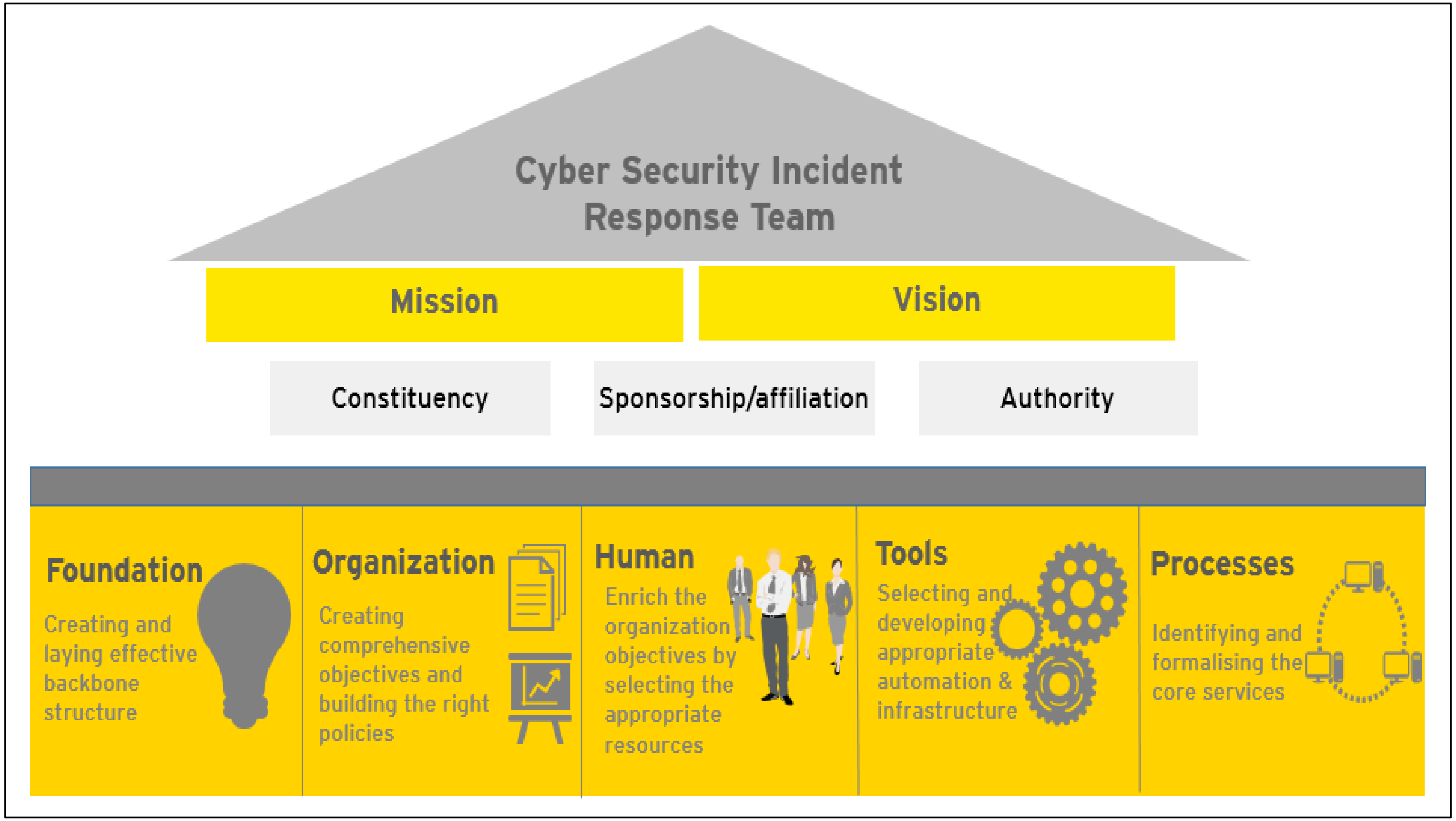
Knowledge Transfer

- Data Acquisition
- Analysis and Synthesis
- Communication

Situational Awareness

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Objective of National CIRT



Cyber Security Incident Response Team

Mission

Vision

Constituency

Sponsorship/affiliation

Authority

Foundation

Creating and laying effective backbone structure

Organization

Creating comprehensive objectives and building the right policies

Human

Enrich the organization objectives by selecting the appropriate resources

Tools

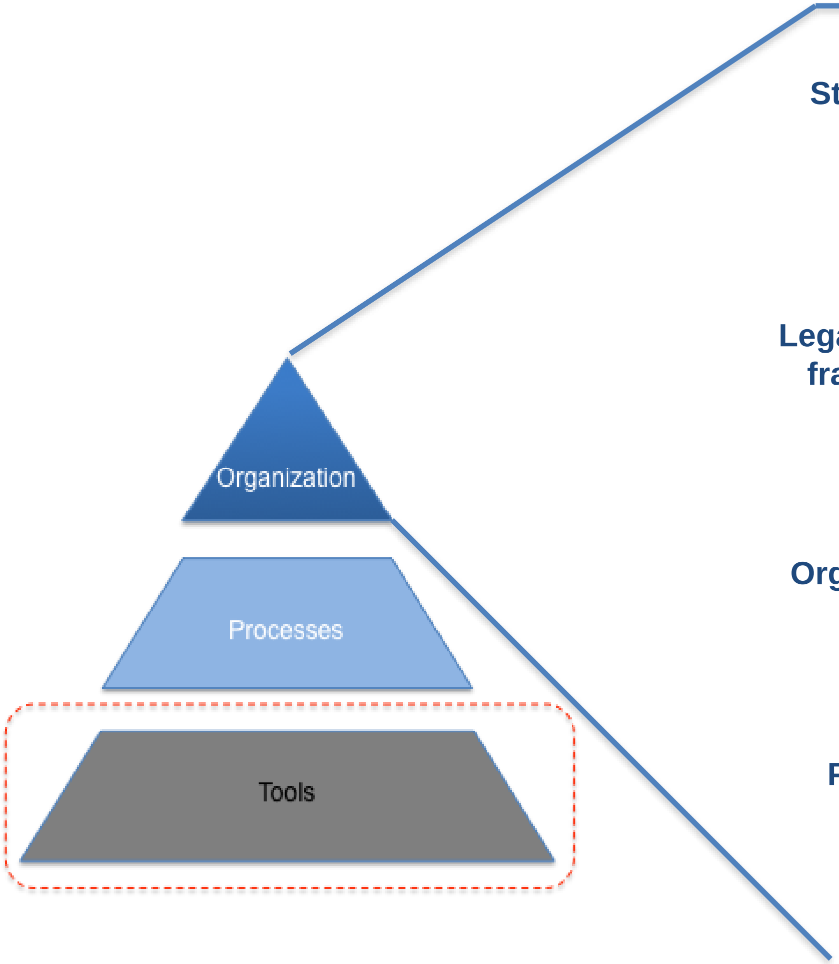
Selecting and developing appropriate automation & infrastructure

Processes

Identifying and formalising the core services

CIRT Model

Organization main aspects



Strategies

- Mission, vision, goals, objectives, constraints
- Participation strategy (members and other National Stakeholders) and minimum capability's level
- Risk Management strategies
- Trust Model
- …

Legal & admin framework

- Legal entity
- Funding Model
- Non disclosure agreements (NDAs)
- Mutual Aid and Assistance Agreement
- …

Organization model

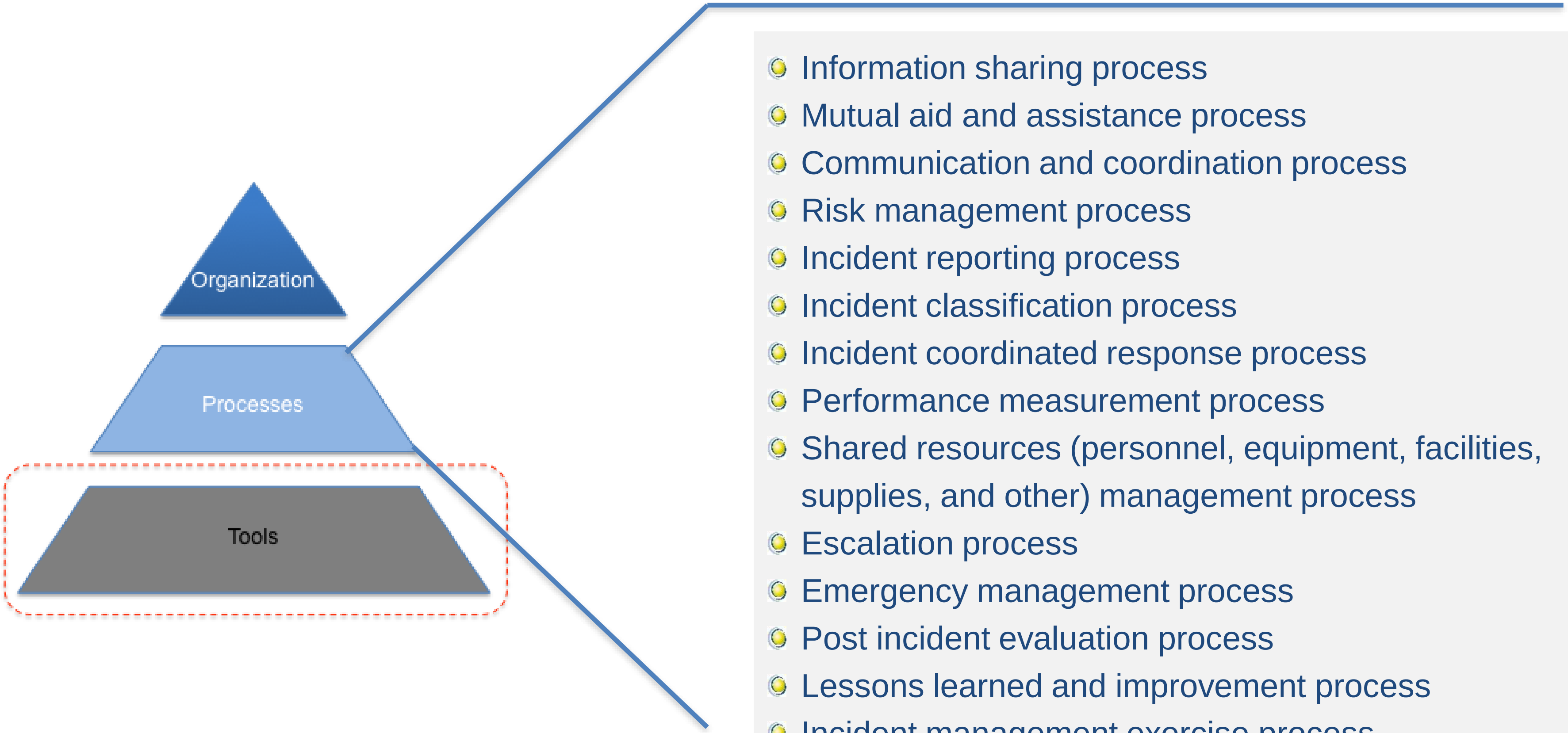
- Organizational model and structure
- Reporting structure, authority
- Roles and responsibilities
- Staff

Policies

- Information sharing policy
- Incident classification and communication policy
- Trust communication policy
- Resource management policies
- Incident handling guidelines
- Risk management policy
- Interoperability policy
- …

CIRT Model

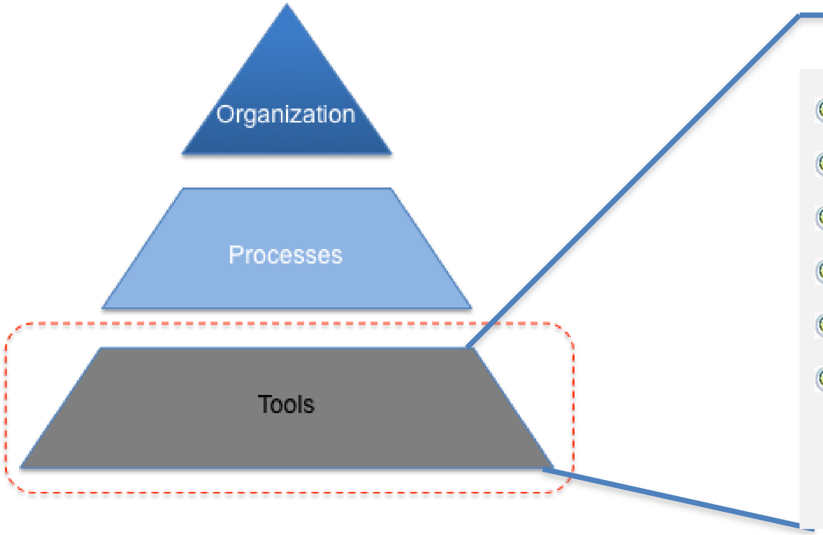
Processes main aspects



- Information sharing process
- Mutual aid and assistance process
- Communication and coordination process
- Risk management process
- Incident reporting process
- Incident classification process
- Incident coordinated response process
- Performance measurement process
- Shared resources (personnel, equipment, facilities, supplies, and other) management process
- Escalation process
- Emergency management process
- Post incident evaluation process
- Lessons learned and improvement process
- Incident management exercise process

CIRT Model

Tools main aspects



- Information sharing platform
- Technological instruments to support trust
- Early warning system
- Instruments for secure communications
- Incident forensics tools
- Other tools

GCI Key aspects of state-level

The GCI is designed to

- ✓ Drive awareness global cybersecurity
- ✓ Share best practices
- ✓ Drive continuous cybersecurity improvement
- ✓ Build capacity in ITU Members

Key Statistics

First released: **2015**

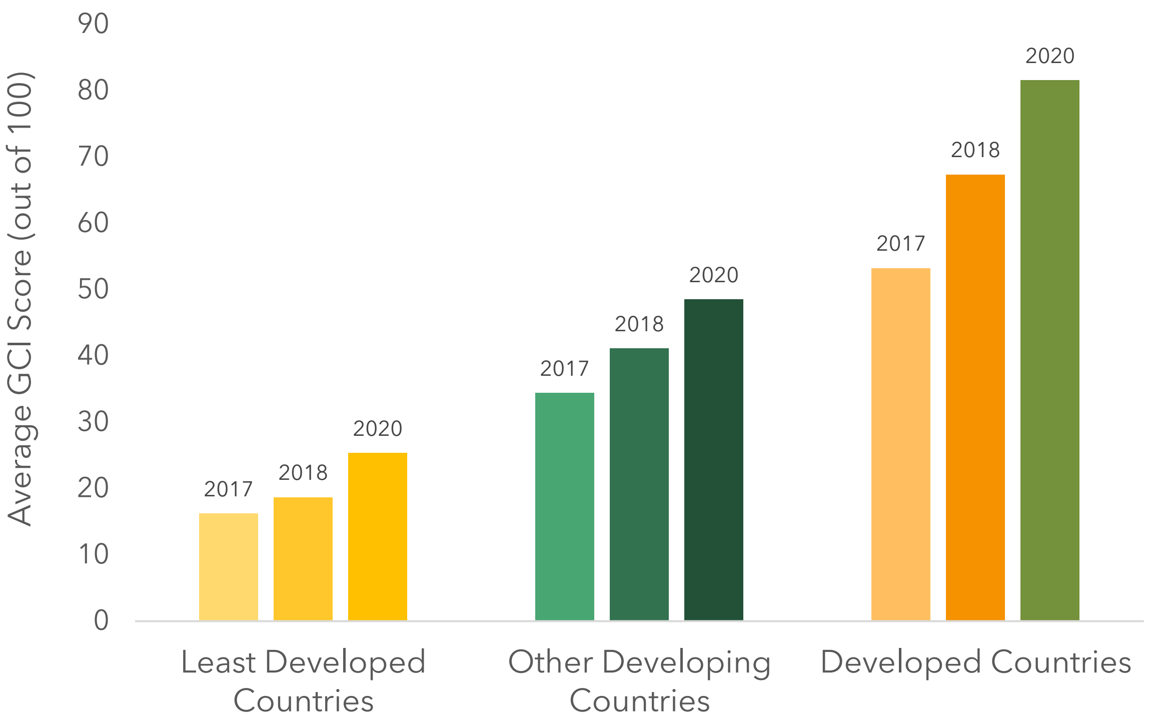
Member States Participating: **169 (of 194)**

Mentions in scholarly articles: >**1 300***

Current questionnaire: **82 questions**

GCI 2020 Report Available at:
https://www.itu.int/hub/publication/d-str-gci-01-2021/

ITU Global Cybersecurity Index (2017-2020)



GCI: Member States, academia, and Private Sector

Preparation & Survey Distribution

Meetings of Study Group

Questionnaire distributed to Member States

Data Collection & Weightage Determination

Member States submit completed Questionnaires

Weightage Expert Group meets, members submit weightage recommendations

Data Quality Check & Analysis

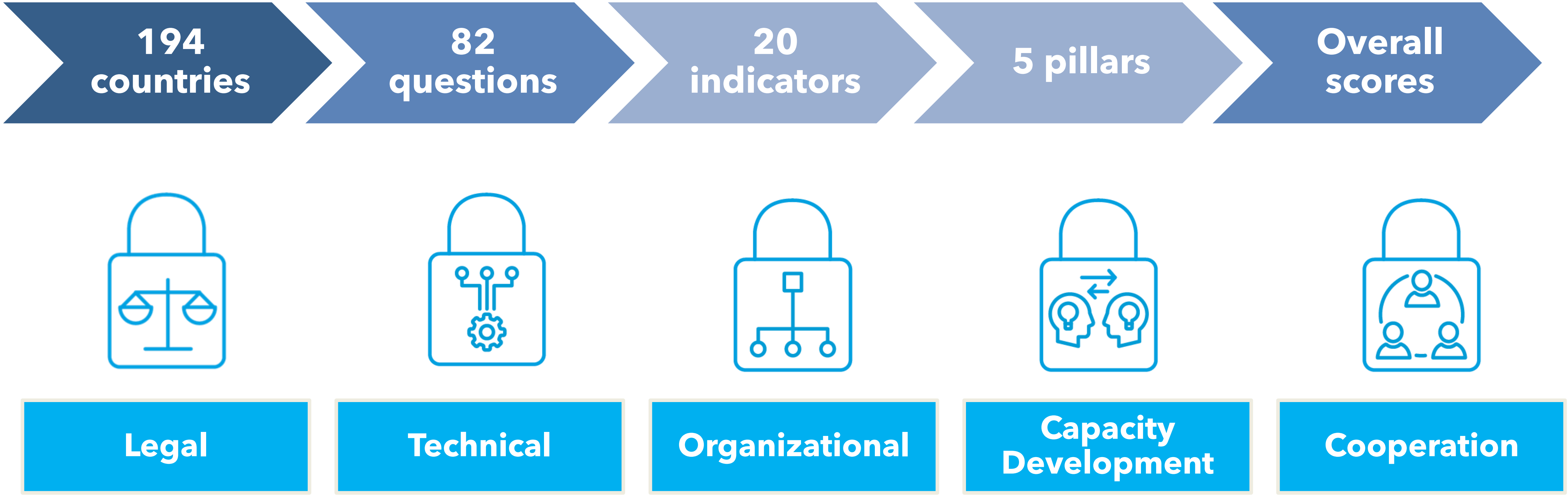
Questionnaire submissions are cross-checked

Member States are invited respond to any inconsistencies

Questionnaires are scored and weighted

Report Publication

GCI: Five pillars



194 countries

82 questions

20 indicators

5 pillars

Overall scores

Legal

Technical

Organizational

Capacity Development

Cooperation

Legal Measures

Are there legal institutions and effective frameworks dealing with cybersecurity and cybercrime?

- **Cybercrime Substantive Law** – Categories of public and private law, including the law of contracts, real property, torts, wills, and criminal law that essentially creates, defines, and regulates rights and behaviors.

- **Cybersecurity Regulations** – A rule-based and meant to carry out a specific piece of legislation.

Technical Measures

Are there of technical institutions and frameworks dealing with cybersecurity endorsed or created by the Member State

- **National/Government CERT/CIRT/CSRIT** -known as CIRT/CSIRT/CERT are concrete organizational entities that are assigned the responsibility for coordinating and supporting the response to computer security events or incidents at a national level
- **Sectoral CERT/CIRT/CSRIT** - Responds to computer security or cybersecurity incidents which affect a specific sector.
- **Child Online Protection (COP)** – The existence of a national agency dedicated to COP, the availability of a helpline to report issues associated with children online
- **National framework for cybersecurity standard implementation** -These standards include, but are not limited, to those developed by the following agencies: ISO, ITU, NIST etc.

Organizational Measures

Are there institutions and strategies organizing cybersecurity development at the national level?

- **National Cybersecurity Strategy** - A National Cybersecurity Strategy (NCS) defines the maintenance of resilient and reliable national critical information infrastructures including the security and the safety of citizens.
- **Responsible Agency** - A responsible agency for implementing the national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils, or cross disciplinary centers.
- **Cybersecurity Metrics** - The existence of any officially recognized national or sector specific benchmarking exercises or referential used to measure cybersecurity development, risk-assessment strategies, cybersecurity audits.

Capacity Development Measures

Intrinsic to the first three measures (legal, technical, and organizational). It helps understand the technology, the risks, and the implications can help to develop better legislation, better policies and strategies, and better organization as to the various roles and responsibilities.

- **Public Cybersecurity Awareness Campaigns** – Includes campaigns to reach as many citizens as possible
- **Training for Cybersecurity Professionals** - The existence of sector-specific professional training programs for raising awareness for the general public
- **National Education Programs and Academic Curriculums** - Education courses and programs to train the younger generation in cybersecurity-related skills and professions in schools, colleges, universities, and other learning institutes
- **Cybersecurity Research and Development Programs** - The investment into national cybersecurity research and development programs at institutions that could be private, public, academic, non-governmental, or international
- **National Cybersecurity Industry** - Environment supporting cybersecurity development incentivizes the growth of cyber security-related enterprises in the private sector
- **Incentive Mechanisms** - Efforts by the government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans etc.

Cooperation Measures

Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application

- **Bilateral Agreements** - Refers to any officially recognized national or sector-specific partnerships for sharing cybersecurity information or assets across borders by the government with one other foreign government and regional entity
- **Multilateral Agreements** - Refers to any officially recognized national or sector-specific program for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations
- **Participation in International Mechanisms (forums)** - May include ratification of international agreements regarding cybersecurity, such as African Union Convention on Cyber Security and Personal Data Protection, Budapest Convention on Cybercrime and others.
- **Public-Private partnerships**- Refers to ventures between the public and private sector
- **Inter-agency Partnerships** – Refers to any official partnerships between the various government agencies within the Member State (does not refer to international partnerships)

THANK YOU