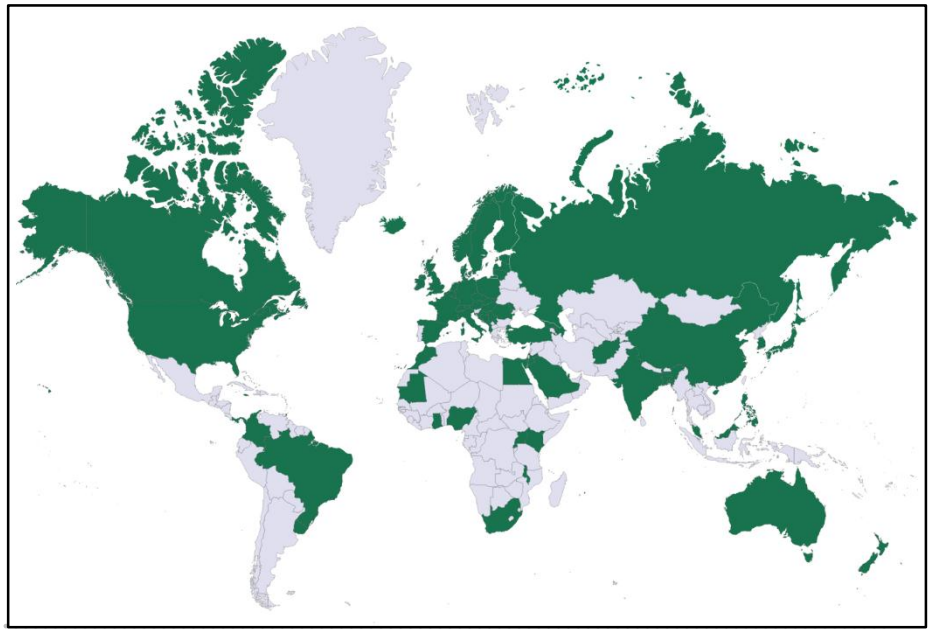
# Upcoming "Guide on Being Strategic about Cybersecurity"

BDT Efforts to Assist Member States
in Producing a
National Cybersecurity Strategy

# National Cybersecurity Strategies

**Developing a Reference Guide to help Member States produce a National Cybersecurity Strategy**

- Only 72 out of the ITU's 193 Member States have a National Cybersecurity Strategy
- New guide developed under open consultation and multi-stakeholder approach, and will replace ITU's previous National Cybersecurity Strategy Guide



# Overview of the NCS Guide

- Overarching Principles for an NCS
  - Cross-cutting, fundamental aspects applicable to the NCS development process and the NCS content
- Strategic Areas and Good Practices
  - The key elements to be considered for inclusion in an NCS
- Process to develop an NCS
  - Captures the key actions of the NCS elaboration and review cycle
- Supporting reference materials
  - Points to relevant literature

# Overarching Principles

- Comprehensiveness and Inclusiveness
- Human Rights and Fundamental Values
- Socio-Economic Prosperity
- Multi-Stakeholder Approach
- Vision
- Allocation of Roles and Responsibilities
- Intra-Governmental Coordination
- Risk Management
- Coherent use of National Cybersecurity Policies and Standards

# Strategic Areas and Good Practice

- Strategic Areas are logical groupings that put a set of related aspects together
  - Helps break down and structure the analysis work
- Good Practice identifies the elements that should be considered for inclusion in an NCS.
  - No mandatory elements; each Country free to choose which to include, and to adapt them to its specific needs.

# Strategic Area 1: Governance

Covers the Good Practice for steering the development of a NCS and its implementation plan, outlining organizational and positional authorities (determination of responsibilities) within the government and multi-stakeholder cooperation mechanisms. It also includes allocation of human and financial resources, and describes the NCS review cycle.

# Strategic Area 2: Risk-Managed Resilience

Covers the Good Practice regarding ensuring ICT systems and information are well protected according to a risk-managed approach and are able to withstand cyber-attacks. Overall, this strategic area helps governments focus on the development of regulations, standards, and policies that form the national cybersecurity framework.

# Strategic Area 3: Preparedness and Incident Response

Covers the Good Practice for the detection of cyber attacks, and the response to cyber incidents of national interest in a coherent manner, with continuous improvement of response capabilities and coordination.

# Strategic Area 4: Critical Infrastructure

Covers the Good Practice for the identification and protection of critical digital assets and infrastructures, covering the traditional critical services such as water, telecommunications, transportation, energy, finance, etc.)

# Strategic Area 5: Capability Development and Awareness

Covers the Good Practice for the advancement of national cybersecurity capabilities through national procurement of capabilities, as well as Research and Development (R&D). Also covers the Good Practice for the development of programs to increase cybersecurity awareness, education and skills development, and the development of a specialized workforce.

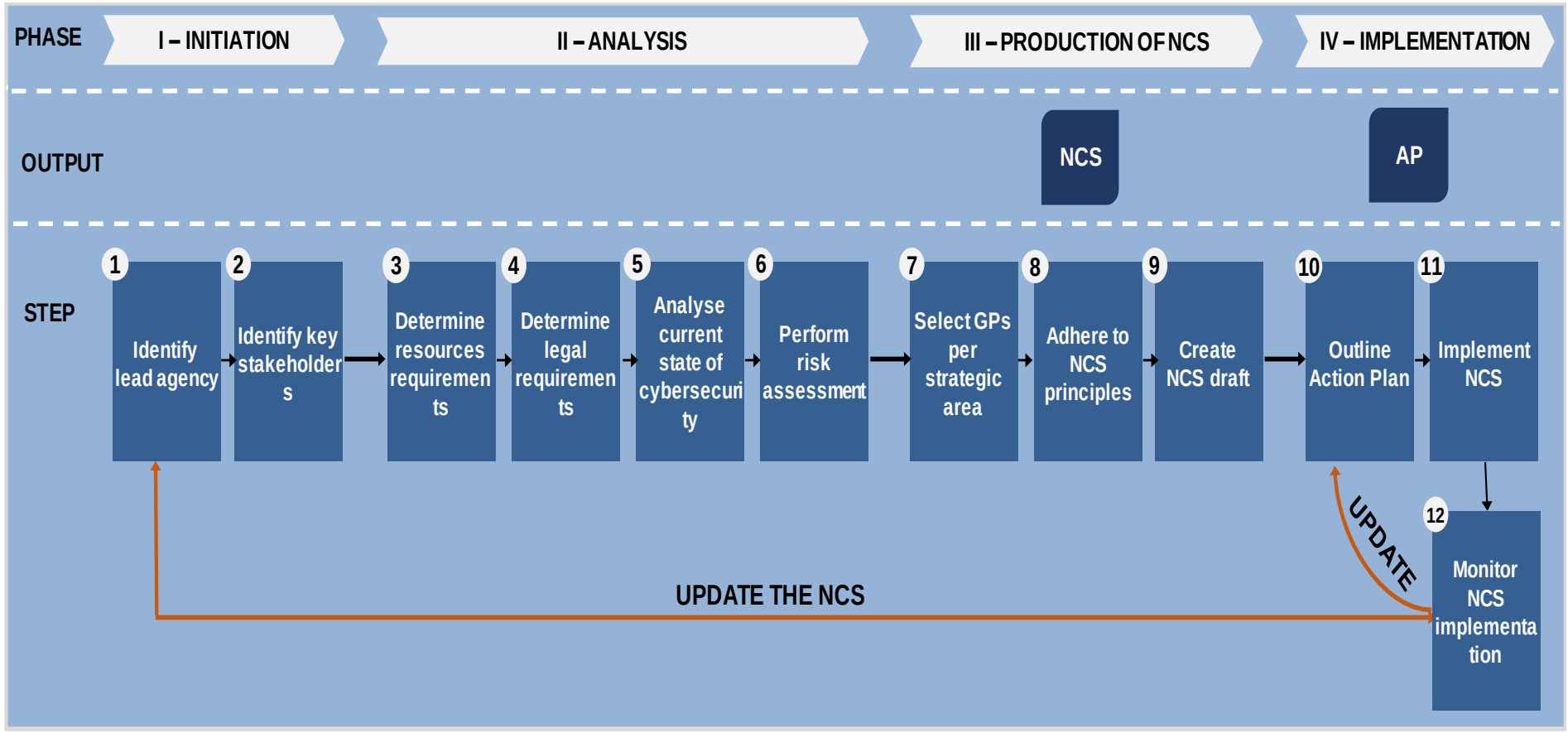
# Strategic Area 6: Criminal Justice

Covers the Good Practice for the formalization of a legal framework defining illegal cyber activities and establishing the agencies that will enforce the legal framework (e.g. police, prosecutors, judges).

# Strategic Area 7: International Collaboration

Covers the Good practice for outreach, partnership, and information sharing activities among nations and governments in order to give governments  the ability to leverage existing capabilities and knowledge.

# Process for the Development of an NCS



# Thank You

cybersecurity@itu.int