

Global Policy Dialog and Briefing: Cybersecurity Strategy Design and Implementation



*Hagai Mei Zahav
Giacomo Assenza*



06/04/2021



Agenda

- ❖ Guide to Developing a National Cybersecurity Strategy 2nd edition
- ❖ Contributors
- ❖ Framework for Supporting National Cybersecurity Strategy
- ❖ The Lifecycle of National Cybersecurity Strategy
- ❖ Phase 1: Initiation and Relevant Stakeholders
- ❖ Phase 2: Stocktaking and Analysis
- ❖ Stocktaking and Analysis – Available Cyber Diagnostics
- ❖ Phase 3: Production of NCS
- ❖ Phase 4: Implementation
- ❖ Production, Implementation and Action Plan Report – Menu of Options
- ❖ Phase 5: Monitoring and Evaluation
- ❖ “How to” – Supporting Mechanism
- ❖ Wrap Up



Guide to Developing a National Cybersecurity Strategy 2nd Edition



The guide is one of the most comprehensive overviews of what constitute successful cybersecurity strategies. It will assist national leaders and policy-makers in thinking strategically about cybersecurity, preparedness and resilience at the national level.

Evolving landscape

The complex nature of cyberspace calls for continuous improvements to NCSs:

- Evolving cybersecurity landscape
- Increased dependency on ICTs
- Rapidly growing cyber risks.

Collaborative effort

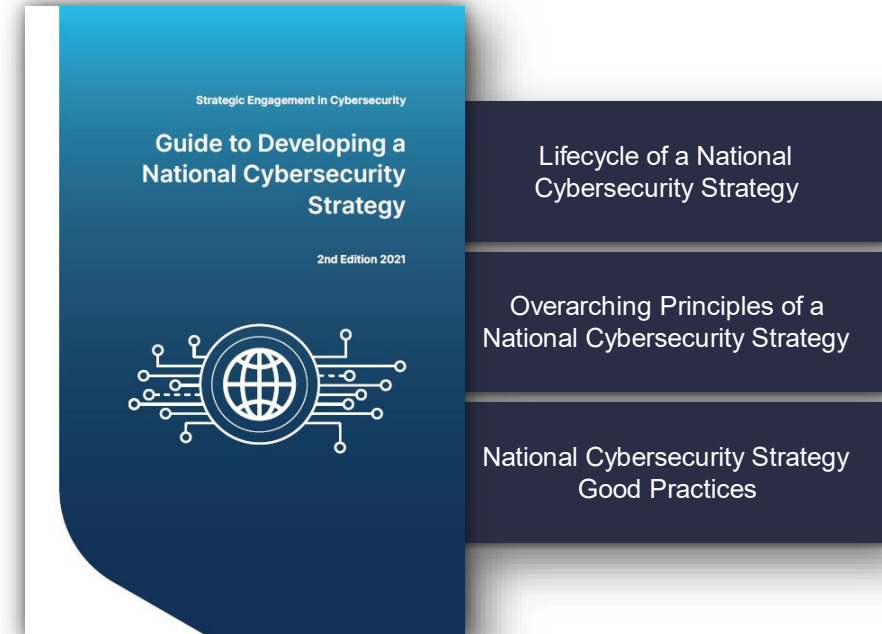
The Guide is the result of a multistakeholder cooperation effort. It merges the expertise of 19 partners from:

- Public and private sectors
- International organisations and NGOs
- Civil society
- Academia

NCS Methodology

It provides reference framework to support countries' ongoing efforts to embrace digitalisation within a comprehensive NCS:

- Lifecycle of a strategy
- 9 Overarching principles
- 37 Best Practices



Contributors



Framework for supporting National Cyber Security Lifecycle

Three categories of resources on cybersecurity

OPERATIONS

Mainstreaming cybersecurity activities into projects, through;

- Expanding available resources to project teams
- Designing cyber protected operations
- Enhancing client's cyber resilience

KNOWLEDGE

Information driven approach to ensure a better pool of knowledge, present available cyber public goods, extend expertise and support data driven decision making:

- Global Baseline Report
- Economics of Cybersecurity
- Menu of Options
- Diagnostic Framework

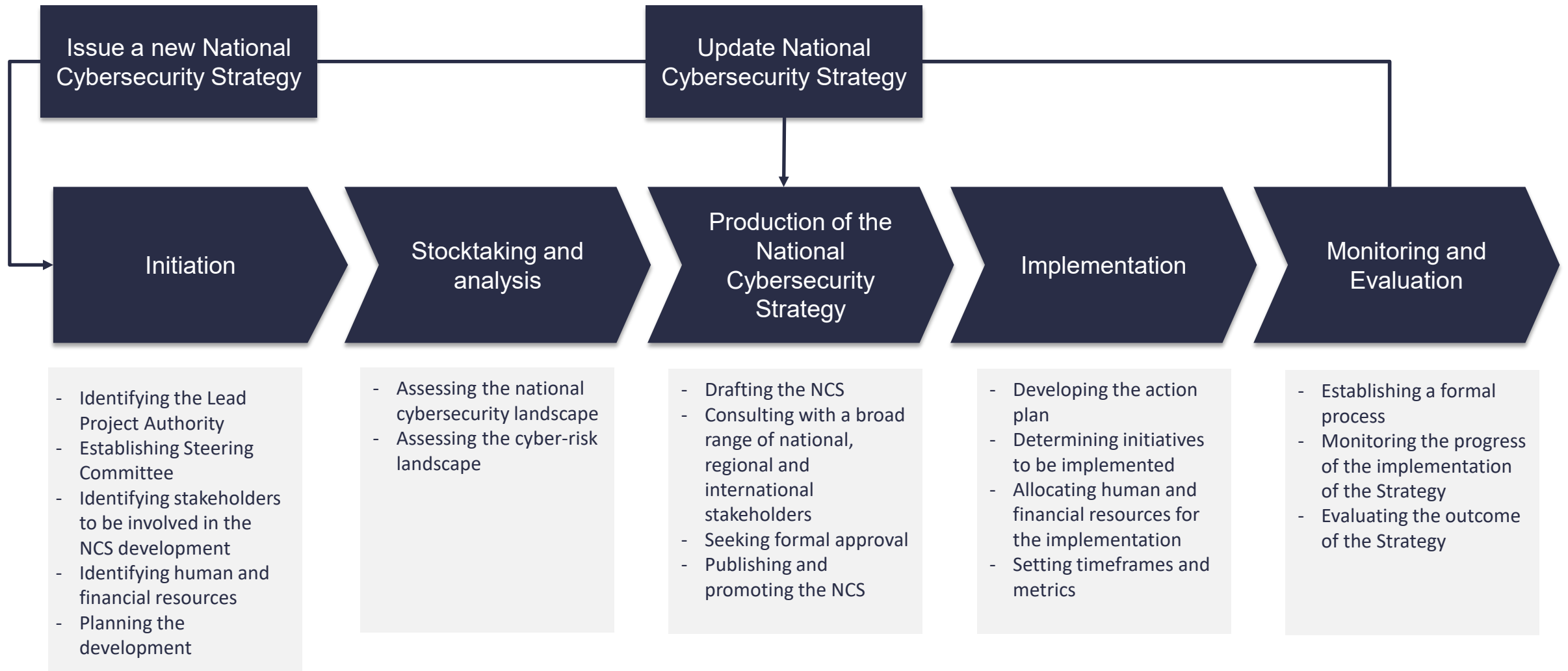
PARTNERSHIPS

Developing strong partnership, fostering awareness, sharing knowledge and expertise and mobilizing resources to support clients on cyber for development:

- Global Conference on Cyber Capacity Building
- Cybersecurity Multi Donor Trust Fund

Guide to Developing a National Cybersecurity Strategy: Collaborating through strong **PARTNERSHIP, to develop **KNOWLEDGE** resource for National Cybersecurity Strategy, for the design and implementation of cyber activities in **OPERATIONS****

The Lifecycle of a National Cybersecurity Strategy



Phase 1: Initiation



Lead Project Authority



Plan the work



Identify the stakeholders



Coordinate the effort



Monitor status updates



Facilitate communication



Be accountable for the process



NCS Development Plan



Major steps and activities



Resource requirements



Key stakeholders



Form of the strategy



Timeline

Relevant Stakeholders



- ▶ Ensure the buy-in of relevant actors
- ▶ Consider needs, knowledge and expertise
- ▶ Facilitate cooperation towards achieving the objectives of the Strategy

Governmental Bodies

Critical Infrastructure operators

Academia

Law Enforcement

International Organizations

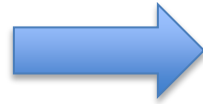
Non-governmental organizations

ICT Companies


Judiciary


Phase 2: Stocktaking and Analysis


Assessing the national cybersecurity landscape




	Documents	Services	Resources	Initiatives
Legal	✓	✗	○	→
Technical	✗	✓	✗	→
Organizational	✗	✗	✓	→
Capacity	✓	✓	✓	→
Cooperative	✗	○	✓	→
...	→	→	→	→

 Identify assets and dependencies

 Identify threats

 Identify vulnerabilities

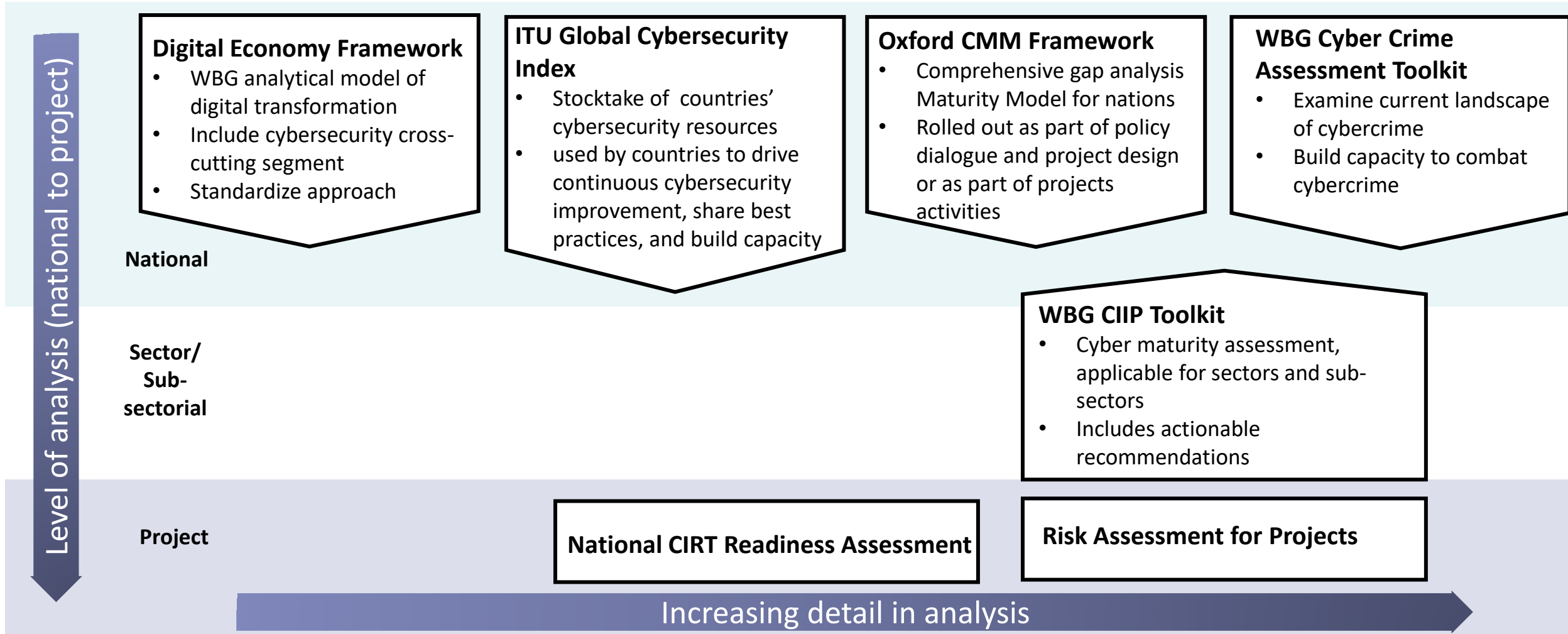
Estimate likelihood and impact of risks 



Assessing the cyber-risk landscape

Stocktaking and Analysis – Available Cyber Diagnostics

Maturity, risk, and compliance assessments at the national, sectorial, sub-sector and project levels



Phase 3: Production of NCS

Drafting



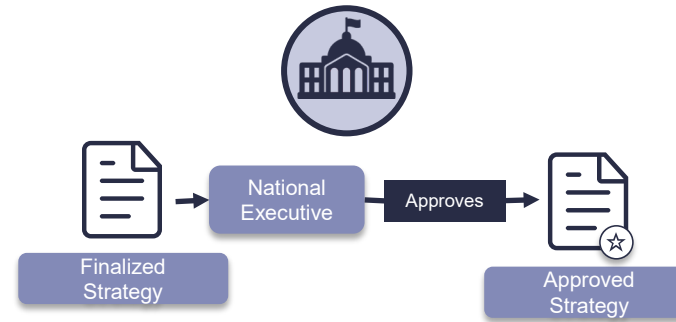
- Overall cybersecurity direction
- Areas of intervention
- Objectives and impacts
- General courses of actions.

Consulting with stakeholders



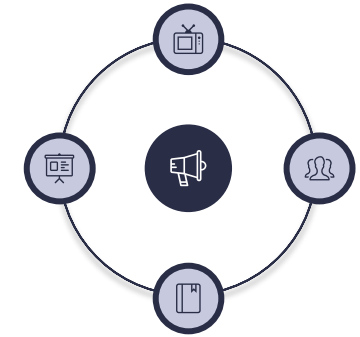
- Working groups
- Public consultation
- National Surveys
- Validation workshop
- Peer review

Formal Approval



- Strategy formally adopted by the Executive
- Adoption process depends on how the NCS is defined in the legislative framework

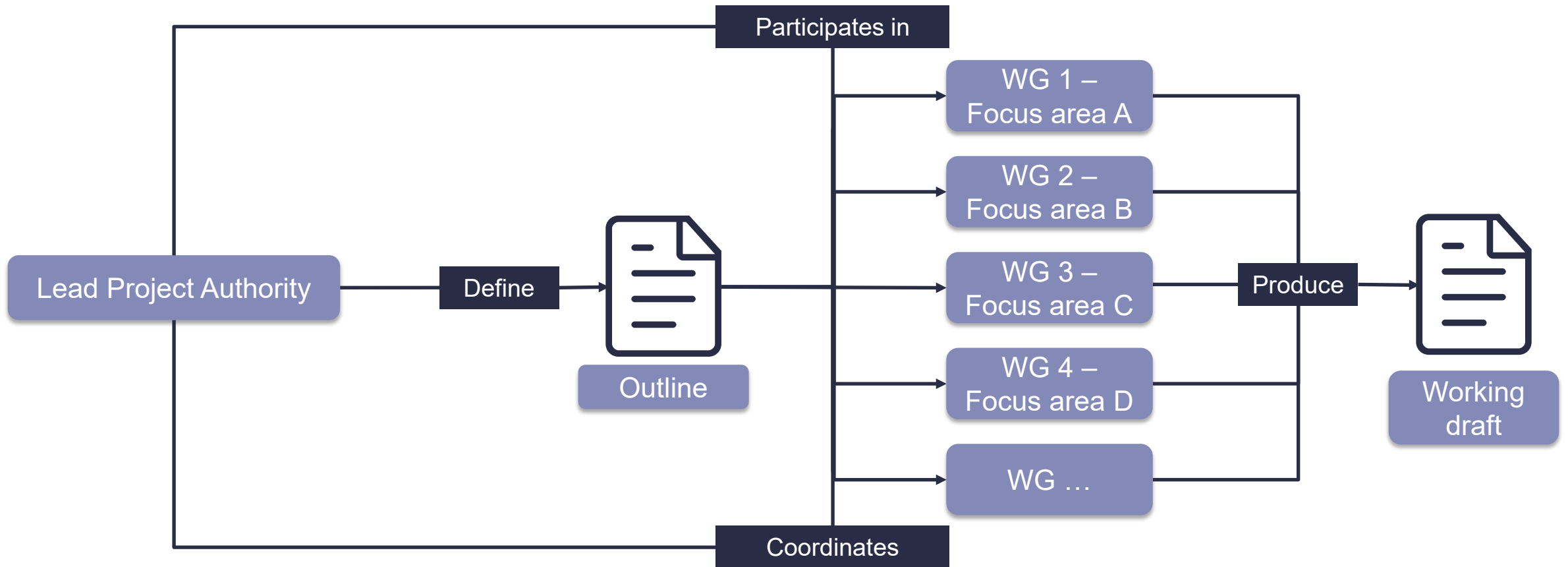
Publishing and promoting



- The NCS should be a public document
- internal and external promotion activities

Phase 3: Production of NCS

Example of drafting process



Phase 4: Implementation

Determining initiatives to be implemented

- The NCS defines the objectives to realise across the focus areas identified.
- The **AP identifies the specific initiatives** within each focus area that will help meet those objectives

Identify initiatives' owners

- The AP identifies **government entities as owners** for each of the initiatives.
- These entities are **responsible and accountable for the implementation** of the initiative assigned to them

Allocating human and financial resources

- The initiatives should be supported by **adequate resources** (human, expertise, funding)
- The initiatives should **prioritised** based on their criticality to ensure that **limited resources** are appropriately **leveraged**

Setting the timeframe

- Having a clear timeframe for each initiative contributes to build a comprehensive plan at the national level
- This also supports in identifying dependencies across different initiatives



Action Plan (AP):
a structured approach to implementation

Production, Implementation & Action Plan Support – Menu of Options

Production Phase: Support for Developing Countries with designing NCS, defining action/ implementation plan and advising on a framework for National Cybersecurity Strategy lifecycle (M&E). Workshops on the different components of NCS are available throughout the process.

Implementation Phase: Support to the operationalization and implementation of various components of the NCS.

The Seven NCS Guide Focus Areas

I. Governance

- Cybersecurity Institutional Structure
- Compliance / Audit Framework for Cyber
- Guidelines for CIIP
- Action Plan Cybersecurity Agency

II. Risk management in national cybersecurity

- Cyber Risk Assessments for Public Sector, Private Sector and Civil Sector
- Simulations and Drills

III. Preparedness and resilience

- Strengthening of national CERTs/CSIRTs/SOCs
- Tools, platforms, equipment, applications for threat intelligence, prevention, monitoring, response, recovery

IV. Capability and capacity building and awareness raising

- Training for various audiences: officials at technical levels; end users of gov systems; judges and prosecutors; budget deciders
- Establishment of a Cybersecurity Academy as part of an existing institute of higher learning
- Public awareness campaigns

V. Critical infrastructure services and essential services

- Establishment or capacity building for priority sectoral CERTs, CSIRTs or SOCs - government, banking, communications, energy
- Cybersecurity technical architecture

VI. Legislation and regulation

- Cybersecurity Cybercrime Legislation & Regulation
- Accession to Budapest Convention
- Critical Infrastructure Legislation
- Legislative reviews & assessments

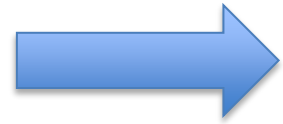
VII. International cooperation

- Exchanges with CERTs/SOCs/CSIRTs
- Study Tours
- Peer-to-peer exchanges
- Information sharing platforms and systems

Phase 5: Monitoring and Evaluation

Monitoring the progress of the implementation

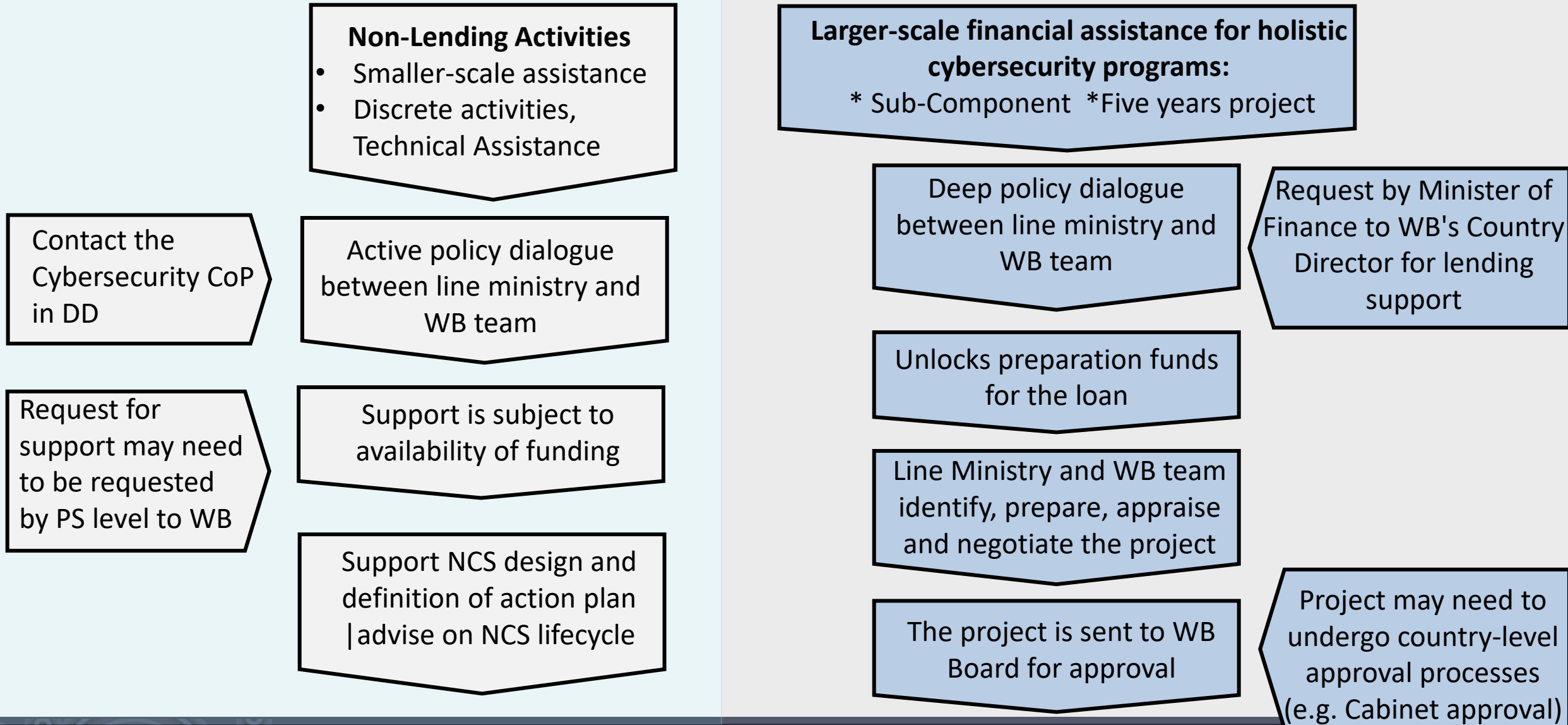
Evaluating the outcomes of the Strategy



S.M.A.R.R.T.

-  Specific
-  Measurable
-  Achievable
-  Relevant
-  Responsible
-  Time-related

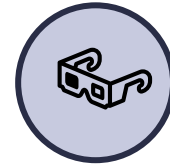
“How To” – Supporting Mechanism



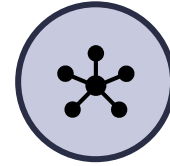
Wrap-up

National Cybersecurity Strategy (NCS) is more than a document, it includes two levels:

- **Strategy level:** what a country wants to do, what interests to pursue
- **Action plan:** how to orchestrate resources to protect national interests in cyberspace



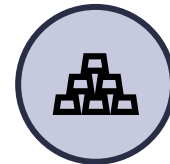
Informed decision making



Stakeholders involvement



Governance



Human/economic resources



International cooperation

“Cybersecurity is essential to ensuring effective and inclusive digital transformation. To reap the benefits and manage the challenges of digitalization, countries need to frame the proliferation of ICT-enabled infrastructure within a comprehensive National Cybersecurity Strategy”

Ms. Doreen Bogdan-Martin, Director of the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU)

Wrap-up

To learn more or get in touch:



itu.int/cyb



cybersecurity@itu.int



THE WORLD BANK
IBRD • IDA



<https://www.worldbank.org/en/topic/digitaldevelopment>



cybersecuritycop@worldbank.org

Cybersecurity CoP Leads:

Anat Lewin

Hagai Mei Zahav