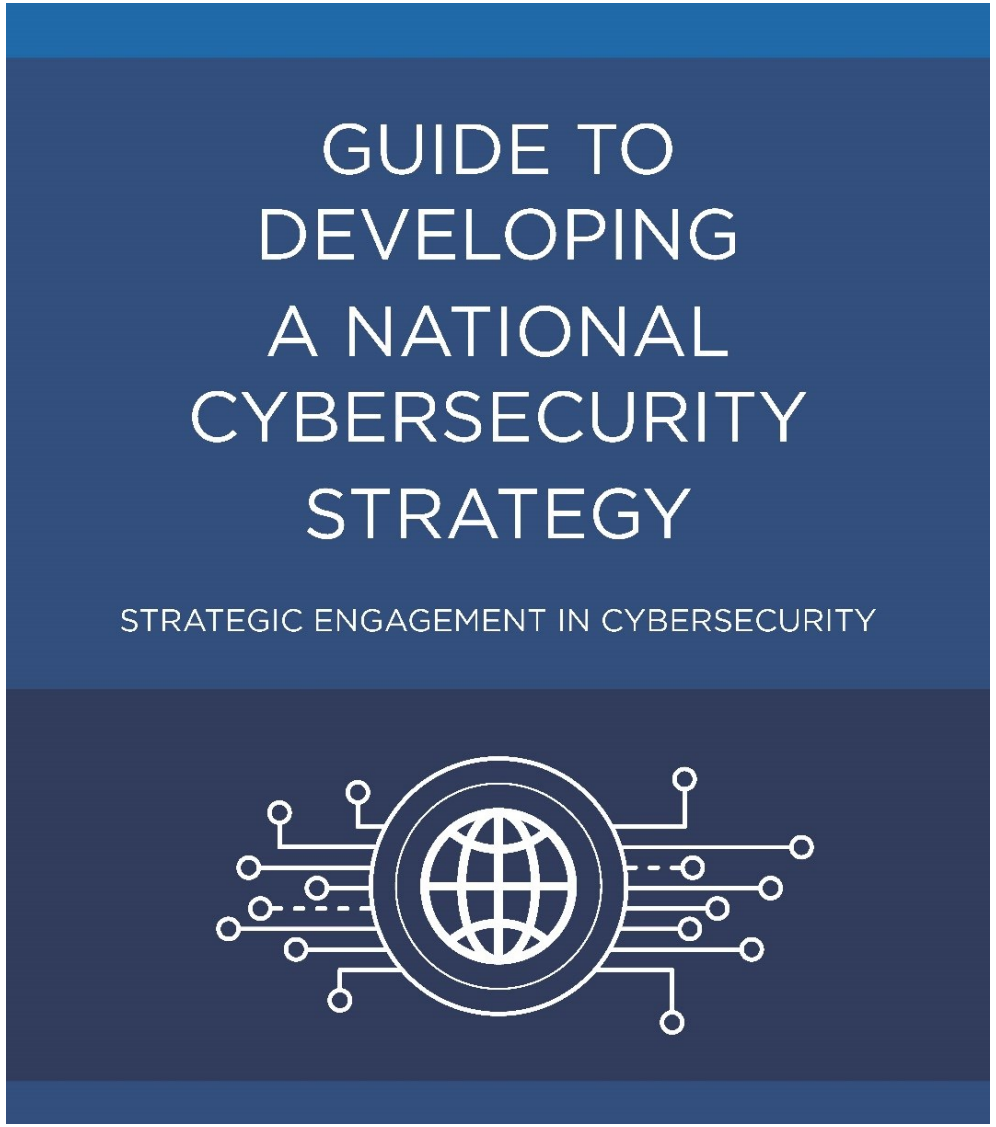



The Commonwealth Cybercrime Initiative

CCDCOE

CTO

Global Cyber Security Capacity Centre

Deloitte.

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

ITU

Microsoft

POTOMAC INSTITUTE FOR POLICY STUDIES

UNITED NATIONS
UNCTAD

RAND
CORPORATION

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

# Purpose

Guides national leaders and policy-makers in the development of a National Cybersecurity Strategy

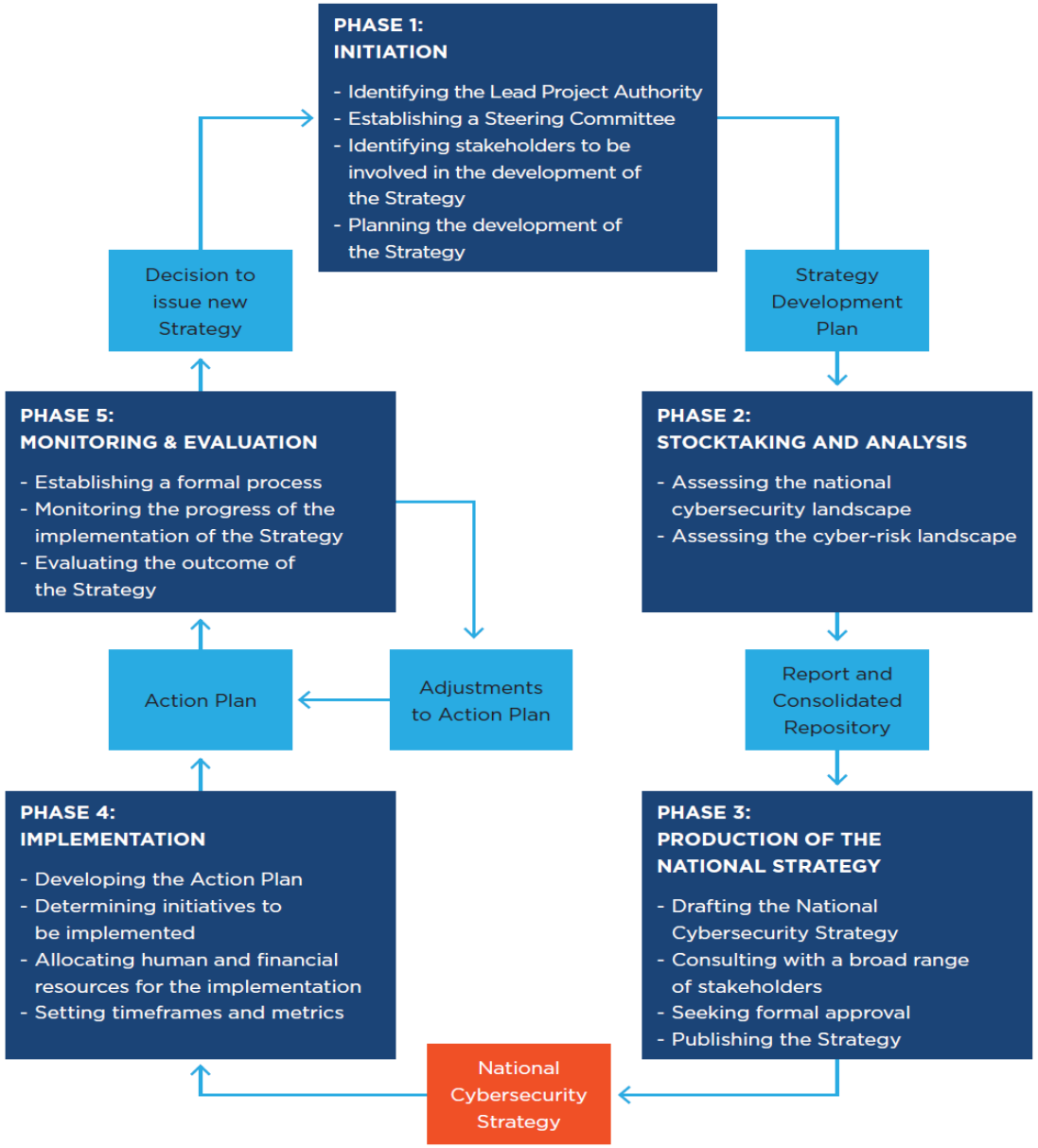
A unique resource. A framework agreed on by organisations with demonstrated and diverse experience in the topic and builds on their prior work in this space

# Scope

Focuses on protecting civilian aspects of cyberspace. Does not cover aspects related to developing offensive and defensive capabilities

Provides indications on "**what**" should be included in a National Cybersecurity Strategy, as well as on "**how**" to build, implement and review it

# Lifecycle of a National Cybersecurity Strategy




Five phases

1. Initiation
2. Stocktaking and analysis
3. Production of a national strategy
4. Implementation
5. Monitoring and evaluation

# Overarching principles

- Vision
- Comprehensive approach and tailored priorities
- Inclusiveness
- Economic and social prosperity
- Fundamental human rights

- Risk management and resilience
- Appropriate set of policy Instruments
- Clear leadership, roles and resource allocation
- Trust environment

# NCS Good Practice – Focus Areas

Focus Areas 1 - Governance

Focus Area 2 - Risk management in national cybersecurity

Focus Area 3 - Preparedness and resilience

Focus Area 4 - Critical infrastructure services and essential services

Focus Area 5 - Capability and capacity building and awareness raising

Focus Area 6 - Legislation and regulation

Focus Area 7 - International cooperation

# Reference material

Stocktaking of existing guides and best practices was conducted

List of references organized by

- National Cybersecurity Strategy Lifecycle
- Overarching principles
- National Cybersecurity Strategy Good Practice