ITU/BDT Cyber Security Programme
Global Cybersecurity Index (GCI)

Guidelines for Member States

Version 0.9

04 September 2019

TABLE OF CONTENTS

About this Document

This document is a guide created to engage Member States and other countries to follow the GCI process and to ensure transparency and accountability. The guideline is divided into four sections, following each phase taken to arrive to the final production of the GCI report. These are briefly explained below;

1. Preparation: This phase consists of activities such as review of the questions and questionnaire structure to MS; identification/review of the GCI Focal Points in Member States; detailed scheduling of all key milestones including publication date, and assignment of resources required, as well as preparation of a standard Operational Procedure (S.O.P) to guide validators, report and presentation templates for the final results.
2. Survey: This phase consists of the following activities: Publication of the updated reference model; opening of the questionnaire to the GCI Focal Points; support to the GCI Focal Points to facilitate responses and monitoring of progress to ensure timely completion of the lime survey and primary data collection.
3. Verification and validation: This phase consists of the following activities: closure of the questionnaire; individual country validation, ensuring all responses have the evidence required to support the answer provided and discussion with GCI Focal Points to ensure accuracy of responses.
4. Drafting of the report and publication: This phase consists of the following activities: drafting of the report, design and BDT editorial processes; handling of the press releases and blogs and Member States inquiries.

The document also includes a summarised timeframe to ensure that Member States submit data and other materials that is required of them within the scheduled timeframe to allow timely delivery of the report for publication.

BACKGROUND

The Global Cybersecurity Index (GCI) is a composite index that combines evolving numbers of indicators into one benchmark to measure the commitment of countries to cybersecurity. Through questions developed on the five pillars (legal, technical, organizational, capacity development, and cooperation) to assess the commitment, the index uses data collected from an online survey and a secondary research process to ensure quality of the data.

ITU Plenipotentiary Conference Resolution 130 (Rev. Dubai 2018) invites Member States “to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors”.

In order to foster a global culture of cybersecurity and its integration at the core of information and communication technologies, the GCI is aiming towards minimizing the visible gap in the level of cybersecurity engagement between different regions around the world.

The GCI is being used as a reference by the ITU Member States and other countries to improve their commitment in cybersecurity. Several countries are in fact implementing measures that are reflected in their score and ranking as well as using the GCI as a benchmark to track the improvement process. Different universities and researchers have taken to using the GCI indicators as references to conduct researches in cybersecurity related studies.

A first iteration of the GCI was published in 2014 with 105 countries that responded, a second iteration saw a response of 134, and 155 countries for third iteration.

The GCI aims at leaving no country behind regarding its cybersecurity development, using the following objectives to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- progress in cybersecurity commitment of all countries from a global perspective;
- progress in cybersecurity commitment from a regional perspective;
- the cybersecurity commitment divide (i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives).

The GCI process has benefited from the contributions of several partners, including Australia Strategic Policy Institute, FIRST (Forum for Incident Response and Security Team), Grenoble University, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet and Security Agency, NTRA Egypt, Red Team Cyber, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica, UNODC, and the World Bank.

With an elevated interest shown in the GCI, the upcoming version four (GCIv4) is being elaborated in consultation with the Member States (ITU-D Study Group 2 – Question 3), in order to improve the process and questionnaire to be administered. The questionnaire and any relevant GCI related documentation will be submitted by the BDT Secretariat to the Q3 Rapporteur Group meeting in October 2019, to be revised and agreed by the meeting before starting the launch of the survey. In March 2020 during the SG2 meeting, BDT will update Q3 with the status and will initiate the analysis of the data, engaging a group of experts formed through an open consultation process with Member States, Sector Members and BDT partners.

To this end, the GCI team has created this simple guide to help Member States in understanding the GCI process.

1 PREPARATION

This phase revolves around the initiating/development stage of the GCI and it consists of specific activities. The GCI team within CYB Division have a brainstorming session with a thorough planning on how to implement each new iteration of GCI every year before the initial start of the project. These activities include tasks such as the following;

- Prior to the start of the GCI activities, a team of 3 individuals with previous experience with GCI are to be selected to work on the GCI project (especially recommended for a later stage).
- The cybersecurity team at ITU conducts primary revision on the existing questionnaire by composing, documenting and identifying all issues and challenges that were faced in all the previous versions of GCI before structuring the new version. In each iteration, the questionnaire is restructured in order to avoid redundancy and reduce time required to provide responses and validation.
- Following the modification of the questionnaire structure and indicators, every year the reference model is revised.
- A formal letter (from the Director) is also prepared. This is the formal invitation that is sent out to all administrations with a copy to the missions and the ITU regional offices. This letter is to request each country to appoint a focal point who will be responsible throughout the GCI process and to indicate if

this will be the same individual for the next 3 years or more in order to create a permanent list of focal points.

- The questionnaire, consisting of its one page guide on how to answer the questions, and a revised reference model agreed upon by all stakeholders, are to be ready for publication. Also, the prepared invitation letter with annexes of this principle guideline and a timeline designed specifically for Member States, will be uploaded on the BTD-GCI website. This is to allow Member States to familiarize themselves with the objectives, background, methodology and the framework of GCI.
- This phase will be followed by the data collection phase (between October 2019 and March 2020).

Upon official invitation

- Member States should appoint one focal point to be the direct contact during all the phases of GCI before the deadline indicated to them. The contact details of the appointed focal point should be formally provided to ITU's GCI team as early as possible.
- The focal point must be able to coordinate with all relevant governmental and non-governmental entities and gather the necessary information to answer accurately to the GCI questionnaire, as there is a possibility that different bodies are responsible for the different sections of the GCI questionnaire.

2 CONDUCTING THE GCI SURVEY/DATA COLLECTION

- The focal point will receive information regarding the survey by email from GCI team as soon as the on-line survey has been prepared.
- The questionnaire will be presented in English with a translation into the other 5 UN languages available.
- Once the questionnaire is opened to Member States and other countries, the focal point must carefully follow the survey's guidelines in order to properly answer each question. Not following the guideline might lead to loss of points/scores.
- Stages, deadlines and tasks will be clearly defined for each person who is involved in carrying out the survey. The focal point must share the guidelines to those assisting in filling the questionnaire. Deadlines must be strictly respected. During the opening survey, the GCI team will remain available to assist the focal point. The lime survey will be closed in March 2020 after the Study Group 2 rapporteur meeting to allow time for validation and preparation of the report.
- Completed submissions of the survey must be submitted by the focal point before the official closing to allow the GCI team to validate their answers. Reminders will be sent to focal points related to the final deadline of the questionnaire.
- The online survey may remain open to allow Member States to complement answers with additional information that will be considered for the next iteration.

Primary data collection

Data collection for Member States that have not responded to the official email of the Director can start as the survey is still ongoing. This is a sole responsibility of the GCI team. Vigorous research will be conducted corresponding to each question of the GCI and results will be pre-filled in the validation template. Data will be collected through publicly available information and the ITU repository.

Weightage Distribution with GCI experts

The weightage development will be conducted through an open approach of establishment of an expert group that will be discussed during the Q3 meeting in October 2019.

In parallel with the ongoing rapporteur meeting in March 2020 (ITU-D Study Group 2 – Question 3), and just before the closure of the online survey, a session regarding the distribution of weightage will be organized of the expert group that was formed through an open consultation process with Member States. Sector Members will be guided on how to fill and assign points to each question of the GCI. For each question, the experts must agree that the question measures some aspect of commitment. This meeting will not only focus on weightage assignment but also take into consideration proposals to improve the GCI publication.

3 VALIDATION AND VERIFICATION OF ANSWERS

- Once the survey has closed, the GCI team will verify answers provided by focal points and immediately send back the validated responses to the focal points for approval.
- Focal points are given the possibility to amend/make changes to their answers and either give an approval or disagree with the GCI team validation by providing new relevant proof corresponding to each question.
- Please take note that the approval must be given within two weeks. Should no feedback from focal points be received after two weeks, the GCI team will use data validated on their side.
- Final approval by focal points, on behalf of Member States, will then be taken into consideration for scoring and report writing.
- During the process of scoring, no further new information from the focal points are accepted.

4 DRAFTING THE REPORT

- Using the existing report template, modification to the already published reference model to be constituted with the findings and analysis of validation and scores.
- The GCI team will compile a draft report releasing results and ranking of each Member State without disclosing their information/data collected.
- The report is submitted to the BDT Editor for proof reading and designing of the publication in a reader friendly manner.
- The final step of the launch will be done just after the analysis phase and will be submitted to the Q3 meeting in October 2020 for revision and approval for publication. And the cycle for the next iteration will restart again.

ANNEX A: TIMEFRAME

Phases	Timeline	Activity	Start Date	End Date
Phase 1: Preparation	**7 months**		**01.04.19**	**13.10.19**
Preparing for the GCI v4		Documenting feedbacks Internal Planning and establishment of a timeframe Modification of the questionnaire Review of the reference model Review of expert group Survey preparation (Lime Survey Platform) And all the documents/material necessary for the proper implementation of the GCI.	01.04.19	11.10.19
Upon receiving official invitation	**4 weeks**		**14.10.19**	**11.11.19**
Upon receiving the invitation letter	2 weeks	Member States are expected to confirm their participation, appoint primary and secondary focal points that will be responsible to facilitate the process within respective country.	14.10.19	28.10.19
Focal point to be confirm to the ITU	2 weeks	Member States to inform ITU of the Focal point chosen to answer the questionnaire	28.10.19	11.11.19
Phase 2: Survey	**4 1/2 months**		**11.11.19**	**31.03.20**
Online survey	4 1/2 month	On the survey platform Questionnaire will be presented in English and translations of the questionnaire in the other 5 UN languages will be available on BDTs GCI Website (to be shared)	11.11.19	31.03.20

FAQ	4 ½ months	During the opening survey, the GCI team will be available for questions	11.11.19	31.03.20
Last reminder	1 month	Reminder will be received by MS related to the final deadline of the questionnaire	03.02.20	28.02.20
Definitive closure	**31.03.20**	Closure of GCI questionnaire. No more changes will be allowed for the present year. However, the platform will stay available to add information that will be considered for the next iteration.	**31.03.20**	**31.03.20**
Primary data collection	**2 months**	ITU GCI team will collect data on behalf of countries that will not respond to take part in the survey. Data will be collected through publicly available information and the ITU repository	**03.02.20**	**31.03.20**
Weightage consultation with experts	**1 day workshop**	Experts will be provided TOR to facilitate the weightage distribution. The points will be awarded in accordance to the relevancy of each question to each individual expert	**Date to be confirmed through the study group**	**Date to be confirmed through the study group**
Phase 3: Validation	**6 months**		**02.12.19**	**29.05.20**
Verification		After the closure of the questionnaire, data will be reviewed by analysts and sent back for correction to Member States. This process may starts as soon as focal points submit in responses. This could be as early as two weeks from the time of the start of the survey	02.12.19	29.05.20
Corrections and validation		Member State to review the ITU corrections, complete any missing information, including additional proof, and send back to GCI team with a confirmation of a complete validation.	31.03.20	12.06.20
Score calculation		Calculating scores to Member States after the final confirmation of validation	12.06.20	13.07.20
Phase 4: Drafting of the Report	**4 months**		**12.06.20**	**21.10.20**

		Data analysis and report drafting	12.06.20	13.07.20
		The design phase plus BDT Editor, reviews etc.	13.07.20	20.10.20
		Publication of the report	**21.10.20**	**21.10.20**

GLOBAL CYBERSECURITY INDEX V4 2019/2020

Questions in this questionnaire have been elaborated and reviewed by the ITU-D Rapporteur Study Group meeting for Question 3/2 : Securing information and communication networks: Best practices for developing a culture of cybersecurity. The meeting was used as a channel to seek Memberships approval for launching the GCIv4 - 2019/2020. The questionnaire is composed of five sections, where questions in all sections expect yes/no responses accompanied by ticking the boxes placed before each element where applicable. The questionnaire should be completed online. Each respondent will be provided (via an official email from ITU) a unique URL for his/her safekeeping. If a focal point chooses a team to respond to the questionnaire, he/she may share the same login to provide in their responses.

The online questionnaire enables the respondents to upload relevant documents (and URLs) for each question as supporting information. Information being provided by respondents to this questionnaire is not expected to be of confidential nature.

LEGAL MEASURES

1. Cybercrime substantive law

EXP: *Substantive law refers to all 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.*

1.1 Do you have substantive law on illegal online behaviour?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.1.1 Do you have substantive laws on illegal access on devices, computer systems and data? ***EXP: Access*** *- the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components, and functions (NICCS);* ***Computer system*** *or* ***system*** *- any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (COE - Convention on Cybercrime);* ***Computer data*** *- any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (COE - Convention on Cybercrime);* □ ***YES*** □ ***No*** Provide links/URL Provide document
1.1.2 Do you have substantive law on illegal interferences (through data input, alteration, and suppression) on devices, data and computer system? ***EXP: Computer system interference*** *- both intentional and unauthorized serious hindering of the functioning of a computer system. It may include inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.* ***Data interference*** *- either intentional and unauthorized damaging, deletion, deterioration, alteration or suppression of computer data.* □ ***YES*** □ ***No*** *Provide links/URL* *Provide document*

1.1.3 Do you have substantive laws on illegal interception on devices, computer systems and data?

EXP: Illegal interception *- both intentional and unauthorized, non-public transmission of computer data to, from or within a computer or another electronic system, made by technical means.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.1.4 Do you have substantive laws on online identity and data theft?

EXP: Online identity theft*- stealing personal information such as names, addresses, date of birth, contact information or bank account. Can occur as a result of phishing, hacking online accounts, retrieving information from social media or illegal access to databases.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.2 Do you have dispositions on computer-related forgery (piracy / copyright infringements)?

EXP: *Unauthorized input, alteration, or deletion of computer data resulting to inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, to perpetuate a fraudulent or dishonest design.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.3 Do you have substantive laws on online safety?

EXP: Online Safety - *refers to maximizing Internet safety-related to various security risks on private and personal or property associated information, as well as enhancing users' self-protection from cybercrimes.*

1.3.1 Do you have dispositions/legal measures on offences related to racist and xenophobic online materials?

EXP: *Measures to prevent different forms of online hate speech and other forms of intolerances because of race, colour, religion, descent or national or ethnic origin, sexual orientation or gender identity, disability, social status or other characteristics.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.3.2 Do you have dispositions/legal measures on online harassment and abuse against personal dignity/integrity?

EXP: Cyber harassment or bullying *- messages sent by email, direct messaging, or derogatory websites aimed to bully or otherwise harass an individual or a group of individuals via personalized attacks.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.3.3 Do you have dispositions/legal measures related to Child Online Protection?

EXP: *Laws which makes it clear that any and every crime that can be committed against a child in the real world can also be committed on the internet or any other electronic network. It is necessary to develop new laws or adopt existing ones to outlaw certain types of behaviour which can only take place on the internet, for example the remote enticement of children to perform or watch sexual acts or grooming children to meet in the real world for a sexual purpose (ITU Guidelines for policy makes on Child Online Protection).*

□ *YES*

□ *No*

Provide links/URL

Provide document

2. Is there any cybersecurity regulation related to…

EXP: *Regulation is rule based and meant to carry out a specific piece of legislation. Regulations are enforced usually by a regulatory agency formed or mandated to carry out the purpose or provisions of a legislation.*

Cybersecurity regulation designates the principles, to be abided by various stakeholders, emanating from and being part of the implementation of laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers.

2.1 Personal data/privacy protection?

EXP: *Regulations about protection personal data from unauthorized access, alteration, destruction, or use. Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences; An example of such legislation may be in the Data Protection Act.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.2 Data breach/incident notification?

EXP: *Breach notification laws or regulations are ones that require an entity that has been subject to a breach to notify the authorities, their customers and other parties about the breach, and take other steps to remediate injuries caused by the breach. These laws are enacted in response to an escalating number of breaches of consumer databases containing personally identifiable information;*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.3 Cybersecurity audit requirements?

EXP: *A security audit means a systematic and periodic evaluation of the information system's security. Typical audit may include assessment of the security of the system's physical configuration and environment, software, information handling processes, and user practices.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.4 Implementation of standards?

EXP: *Existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.;*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.5 Use of digital signatures in government services and applications (e-govt)?

EXP: *A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks; examples of such legislative documents include Electronic Commerce Act, Law on Electronic Signatures, E-Transaction Law, and other which may include regulations on the establishment of a controller of certificate authorities..*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.6 Curbing of spam?

EXP: *Please add information on any laws or regulations restricting SPAMMING activities.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.7 Identifying and protecting the national critical information infrastructures?

EXP: *Critical infrastructure constitutes basic systems crucial for safety, security, economic security, and public health of a nation. Those systems may include, but are not limited to defense systems, banking and finance, telecommunications, energy, and other. Attach any links or documents that define critical infrastructures or documents/news that confirms definitions of those.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

Please provide some of the best practices/achievements/on-going developments that your country has/is been/being involved in pertaining to the legal areas as part of cybersecurity activities? (Use the comment box for a detailed practice/s and include links for proof)

Or provide document/s including links for proof

TECHNICAL MEASURES

1. National/Government CIRT/CSIRT/CERT.

EXP: *CIRT-CSIRT-CERT: computer incident response teams, staffed concrete organizational entities that are assigned the responsibility for coordinating and supporting the response to computer security events or incidents on national or government level.*

NOTE: *Sometimes distinctions are made between Government and National CIRTs as separate/different entities – Government CIRT serves Governmental constituents, and National CIRT serves the national constituents, including the private sector and citizens. Sometimes they referred to them as the same entity.*

1.1 Is there a National/Government CIRT/CSIRT/CERT?

EXP: *Supported by a government's decision or is part of governmental or national structures.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.2 Does your National or Government CIRT/CSIRT/CERT…

1.2.1 Develop and execute cybersecurity awareness activities?

EXP: *Efforts to promote widespread publicity campaigns to reach the nation about safe cyber-behaviour online.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.2.2 Conduct regular cyber security exercises such as CyberDrills?

EXP: *A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to, or recovering from the disruption. Are the exercises organized periodically or repeatedly?*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.2.3 Provide publicly available Advisories?

EXP: *CIRT Advisories: the sharing of information with the general public on emerging cyberthreats and the recommended actions to take.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.2.4 Contribute to the issues of Child Online Protection?

EXP: *The CIRT/CSIRT/CERT provides support such as awareness creation campaigns, reporting of incidents related to children, providing educational materials on Child Online Protection and others.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.3 Are the above mentioned CIRTs (CSIRT or CERT) affiliated with FIRST?

EXP: *A Full Member or Liaison Member of the Forum of Incident Response and Security Teams. www.first.org*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.4 Are the above CIRT/s (CSIRT or CERT) affiliated with a regional CERT?

EXP: *A formal or informal relation with any other CERT within, or outside the country, as a part of any regional CERT group. Examples of regional CERTS include APCERT, AFRICACERT, EGC, OIC, and OAS.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.5 Was the maturity level of above CIRT, CSIRT or CERT services certified by the TI certification scheme under TF-CSIRT –SIM3?

Exp: *SIM3 is a basis for CIRT certification.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2. Sectoral CIRT/CSIRT/CERT

EXP: *A sectoral CIRT/CSIRT/CERT is an entity that responds to computer security or cybersecurity incidents which affect a specific sector. Sectoral CERTs are usually established for critical sectors such as healthcare, public utilities, academia, emergency services and the financial sector. The sectoral CERT provides its services to constituents from a single sector only.*

2.1 Are there sectoral CIRTs/CSIRTs/CERTs in your country?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.2. Does your sectoral CIRT/s, CSIRT/s, CERT/s:

2.2.1 Develop and execute cybersecurity awareness activities for a sector?

□ *YES*
□ *No*

Provide links/URL

Provide document

2.2.2 Actively participate in national CyberDrills?

□ *YES*
□ *No*

Provide links/URL

Provide document

2.2.3 Share sectoral related incidents within its constituency?

EXP: *sharing of information on emerging cyberthreats and the recommended actions to take.*

□ *YES*
□ *No*

Provide links/URL

Provide document

3. National framework for implementation of cybersecurity standards

EXP: *Adopted a national framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to, those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.*

3.1 Is there a framework for implementation/adoption of cybersecurity standards?

□ *YES*
□ *No*

Provide links/URL *Provide document*
3.2 Does the framework include international or other related standards? ***EXP:*** *ITU-T, ISO/IEC, NIST, ANSI/ISA and others.* □***YES*** □***No*** *Provide links/URL* *Provide document*
4. Child Online Protection ***EXP:*** *This indicator measures the existence of a national agency dedicated to Child Online Protection, the availability of a national telephone number to report issues associated with children online, any technical mechanisms and capabilities deployed to help protect children online, and any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online telephone number, email address, web forms and other, where the interested parties can report incidents or concerns related to Child Online Protection (COP).*
4. Are there any reporting mechanisms and capabilities deployed to help protect children online? ***EXP:*** *Such as hotlines, helplines etc.* □***YES*** □***No*** *Provide links/URL* *Provide document*
Please provide some of the best practices/ achievements/on-going development your country has/is been/being involved in pertaining to the technical areas as part of cybersecurity activities. (Use the comment box for a detailed practice/s and include links for proof)

Or provide document/s including links for proof

ORGANIZATIONAL MEASURES

1. National Cybersecurity Strategy

EXP: *The development of policy to promote cybersecurity as one of national top priorities. A national cybersecurity strategy should define the maintaining of resilient and reliable national critical information infrastructures including the security and the safety of citizens; protect the material and intellectual assets of citizens, organizations and the nation; respond, prevent cyber-attacks against critical infrastructures; and minimize damage and recovery time from cyber-attacks.*

1.1 Does your country have a national cybersecurity strategy/policy?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.1.1 Does it address the protection of national critical information infrastructures, including in the telecommunication sector?

EXP: *Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any from including data, voice, or video that is vital to the functioning of a critical infrastructure; so vital that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.1.2 Does it include reference to the national cybersecurity resilience?

EXP: *A national cybersecurity resiliency plan ensures that the country has the ability to resist, absorb, accommodate to and recover from the effects of any hazard (including natural or human-made) in a timely and efficient manner, including through the preservation and restoration of its essential services and functions with reliance on external service.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.1.3 Is the national cybersecurity strategy revised and updated on a continuous basis?

EXP: *The life cycle management of the strategy is defined, the strategy is updated according to national, technological, social, economic and political developments that may affect national cybersecurity situation.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.1.4 Is the cybersecurity strategy open to any form of consultation with national experts in cybersecurity?

EXP: *The strategy is open for consultation by all relevant stakeholders, including operators of critical infrastructures, ISPs, academia and others.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.2 Is there a defined action plan/roadmap for the implementation of cybersecurity governance?

EXP: *A strategic plan that defines the national cybersecurity outcomes including steps and milestones needed to implement it.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.3 Is there a national strategy for Child Online Protection?

□ *YES*

□ *No*

Provide links/URL

Provide document

2. Responsible Agency

EXP: *A responsible agency for implementing the national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils, or cross-disciplinary centres. Such a body may also be directly responsible for the national CIRT. The responsible agency may exist within the government and may have the authority to compel other agencies and national bodies to implement policies and adopt standards.*

2.1 Is there an agency responsible for cybersecurity coordination at a national level?

□ *YES*

□ *No*

Provide links/URL

Provide document

2.1.1 Does this agency oversee National Critical Information Infrastructure Protection?

□ *YES*

□ *No*

Provide links/URL

Provide document

2.2 Is there a national agency overseeing national cybersecurity capacity development?

□ *YES*

□ *No*

Provide links/URL

Provide document

2.3 Is there any agency overseeing the child online protection initiatives at the national level?

EXP: *Existence of a national agency dedicated to oversee and promote Child Online Protection*.

□ *YES*

□ *No*

Provide links/URL

Provide document

3. Cybersecurity metrics

EXP: *Existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development, risk-assessment strategies, cybersecurity audits, and other tools and activities for a rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27004, which is concerned with measurements relating to information security management.*

3.1 Are there any cybersecurity audits performed at a national level?

EXP: *A security audit is a systematic evaluation of the security of an information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Privately managed critical infrastructures may be requested by the regulatory bodies to perform security posture assessments periodically and report on findings.*

□ *YES*

□ *No*

Provide links/URL

Provide document

3.2 Are there metrics for assessing cyberspace associated risks at a national level?

EXP: *It is a process comprising risk identification, risk analysis and risk evaluation.*

□ *YES*

□ *No*

Provide links/URL

Provide document

3.3 Are there measures for assessing the level of cybersecurity development at a national level?

EXP: *It is an approach to measure the development level of cybersecurity in a nation state.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

Please provide some of the best practices/achievements/on-going development your country has/is been/being involved in pertaining to the organizational measures as part of cybersecurity activities. (Use the comment box for a detailed practice/s and include links for proof)

Or provide documents including links for proof

CAPACITY DEVELOPMENT

1. Public cybersecurity awareness campaigns

EXP: *Public awareness includes efforts to promote campaigns to reach as many citizens as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centres, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behaviour online. This includes actions such as setting up portals and websites to promote awareness, disseminating support materials and other relevant activities.*

1.1 Are there public awareness campaigns targeting specific sector such as SMEs, private sector companies, and government agencies?

□ *YES*

□ *No*

Provide links/URL

Provide document

1.2 Are there public awareness campaigns targeting civil society?

EXP: *NGOs, community-based organisations.*

□ *YES*

□ *No*

Provide links/URL

Provide document

1.3 Are there public awareness campaigns targeting citizens?

□ *YES*

□ *No*

Provide links/URL

Provide document

1.4 Are there public awareness campaigns targeting the elderly?

□ *YES*

□ *No*

Provide links/URL

Provide document

1.5 Are there public awareness campaigns targeting persons with special needs?

□ *YES*

□ *No*

Provide links/URL

Provide document

1.6 Are there public awareness campaigns involving parents, educators and children (COP related)?

□ *YES*

□ *No*

Provide links/URL

Provide document

2. Training for Cybersecurity professionals

EXP: *The existence of sector-specific professional training programs for raising awareness for the general public (i.e., national cybersecurity awareness day, week, or month), promoting cybersecurity education for the workforce of different profiles (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.*

It also includes cybersecurity training for law enforcement officers, judicial and other legal actors designate professional and technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession. This indicator also includes the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of professionals by internationally recognized cybersecurity standards. These certifications, accreditations, and standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), and other.

2.1 Does your government develop/support professional training courses in cybersecurity?

EXP: *Promoting cybersecurity courses in the workforce (technical, social sciences, etc. and promoting certifications for professionals in either the public or the private sector.*

□ *YES*

□ *No*

Provide links/URL

Provide document

2.2 Is there an accreditation program for cybersecurity professionals in your country?

EXP: *Institutes accrediting cybersecurity professionals, or any other related mechanisms.*

□ *YES*

□ ***No***

Provide links/URL

Provide document

2.3 Are there a national sector-specific educational programmes/trainings/courses for professionals in cybersecurity?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.3.1 Are there a national sector-specific educational programmes/trainings/courses for law enforcement?

EXP: *Cybersecurity formal process for educating legal actors (police officers and enforcement agents) about computer security*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.3.2 Are there a national sector-specific educational programmes/trainings/courses for judicial and other legal actors?

EXP: *Cybersecurity training or technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.3.3 Are there a national sector-specific educational programmes/trainings/courses for SMEs/private companies?

EXP: *Good practices trainings / capacity development on cybersecurity to guard their businesses, etc. by proper use of online services.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2.3.4 Are there a national sector-specific educational programmes/trainings/courses for other public sector/government officials?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

3. Does your government/organization develop or support any educational programmes or academic curricula in cybersecurity…

EXP*: Existence and the promotion of national education courses and programmes to train the younger generation in cybersecurity-related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity-related professions include, but are not limited to, cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers.*

3.1 In primary education?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

3.2 In secondary education?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

3.3 In higher education?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

4. Cybersecurity research and development programmes

EXP: *This indicator measures the investment into national cybersecurity research and development programs at institutions that could be private, public, academic, non-governmental, or international. It also considers the presence of a nationally recognized institutional body overseeing the program. Cybersecurity research programs include but are not limited to, malware analysis, cryptography research, and research into system vulnerabilities and security models and concepts. Cybersecurity development programs refer to the development of hardware or software solutions that include but are not limited to firewalls, intrusion prevention systems, honey pots, and hardware security modules. The presence of an overarching national body to increase coordination among the various institutions and the sharing of resources is required.*

4.1 Are there cybersecurity R&D activities at the national level?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

4.1.1 Are there private sector cybersecurity R&D programmes?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

4.1.2 Are there public sector cybersecurity R&D programmes?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

4.1.3 Are higher education institutions such as academia and universities engaged in R&D activities?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

5. National cybersecurity industry

EXP: *A favourable economic, political, and social environment supporting cybersecurity development incentivizes the growth of a private sector around cybersecurity. The existence of public awareness campaigns, workforce development, capacity building, and government incentives drive a market for cybersecurity products and services. The existence of a home-grown cybersecurity industry is a testament to such a favourable environment and drives the growth of cybersecurity start-ups and associated cyber-insurance markets.*

5.1 Is there a national cybersecurity industry?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

6. Are there any government incentive mechanisms in place...

EXP: *This indicator looks at any incentive efforts by the government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, including dedicated and nationally recognized institutional body overseeing cybersecurity capacity-building activities. Incentives increase the demand for cybersecurity-related services and products, which improves defences against cyber threats.*

6.1 To encourage capacity development in the field of cybersecurity?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

6.2 For the development of a cybersecurity industry?

EXP: *support to start-ups cybersecurity services in academia and other*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

Please provide some of the best practices/achievements/on-going development your country has/is been/being involved in pertaining to the capacity building measures as part of cybersecurity activities. (Use the comment box for a detailed practice/s and include links for proof)

Or provide document/s including links for proof

COOPERATIVE MEASURES

1. Bilateral agreements on cybersecurity cooperation with other countries

EXP: *Bilateral agreements (one-to-one agreements) refer 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 (i.e., the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether information sharing of threat intelligence. Capacity building refers to the sharing of professional tools, advanced envelopment of experts, and others.*

1.1 Do you have bilateral agreements on cybersecurity cooperation with other countries?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.1.1 Is information sharing part of the agreement(s)?

EXP: *Information-sharing refers to the practices around sharing on non-sensitive information.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.1.2 Is capacity building part of the agreement(s)?

EXP: *The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

1.1.3 Is mutual legal assistance part of the agreement(s)?

EXP: *Mutual assistance between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

2. Government participation in international mechanisms related to cybersecurity activities

EXP: *It may also 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.*

2.1 Does your government/organization participate in international mechanisms related to cybersecurity activities?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

3. Cybersecurity multilateral agreements

EXP: *Multilateral agreements (one to multiparty agreements) refers to any officially recognized national or sector-specific programmes for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations (i.e. the cooperation or exchange of information, expertise, technology and other resources).*

3.1 Does your government have multilateral agreements on cybersecurity cooperation?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

3.1.1 Is information sharing part of the agreement(s)?

EXP: *Information-sharing refers to the practices around sharing on non-sensitive information.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

3.1.2 Is capacity building part of the agreement(s)?

EXP: *The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

4. Partnerships with the private sector (PPPs)

EXP: *Public-private partnerships (PPP) refer to ventures between the public and private sector. This performance indicator measures the number of officially recognized national or sector-specific PPPs for sharing cybersecurity information and assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources), whether nationally or internationally.*

4.1 Does your government engage in PPPs with locally established companies?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

4.2 Does your government engage in PPPs with foreign owned companies in your country?

□ ***YES***

□ ***No***

Provide links/URL

Provide document

5. Inter-agency partnerships

EXP: *This performance indicator refers to any official partnerships between the various government agencies within the nation state (does not refer to international partnerships). This can designate partnerships for information- or asset-sharing between ministries, departments, programmes and other public sector institutions.*

5.1 Are there inter-agency partnerships/agreements among different governmental bodies in relation to cybersecurity?

EXP: *Cooperation between ministries or specialized agencies*

□ ***YES***

□ ***No***

Provide links/URL

Provide document

Please provide some of the best practices/ achievements/on-going development that your country has/is been/being involved in pertaining to the cooperation measures as part of cybersecurity activities. (Use the comment box for a detailed practice/s and include links for proof)

Or provide document/s including links for proof