Annex 1 – Terms of Reference

ITU/BDT Cyber Security Program

GCI Weightage Expert Group

Terms of Reference

August 2020

The GCI

First published in 2015, the Global Cybersecurity Index (GCI) helps countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, in turn raising the overall level of cybersecurity worldwide. Through the data collected, the GCI highlights practices that Member States can implement suitable to their national environment, promotes good practices, and fosters a global culture of cybersecurity.

The GCI scope and framework is set out in ITU Plenipotentiary Resolution 130 (Rev. Dubai, 2018), which addresses strengthening the role of ITU in building confidence and security in the use of information and communication technologies. The GCI Questionnaire, from which indicators, sub-indicators, and micro-indicators are derived is created and approved by a consultation under Study Group 2, Question 3: Securing information and communication networks: Best practices for developing a culture of cybersecurity of ITU Members.

The GCI Weightage Expert Group

The objective of the Expert Group is to determine the weightage of GCI indicators, sub-indicators, and micro-indicators and to propose changes to the GCI Questionnaire for future iterations.

Members of the GCI Expert Group are appointed to provide thorough and unbiased recommendations for distribution of points within the GCI model. Expert Group recommendations of the weight of indicators and sub indicators should reflect the importance of given indicator for the overall cybersecurity commitment of a Member State. Specific activities of the Expert Group include:

- To provide input on the computation of the main index and sub-indices, illustrated in Annex B of this document; and,
- To provide input on possible future iterations of the GCI.

In exceptional cases, and upon agreement of the majority, review questions may be recommended by the Expert Group for the next GCI iteration.

The ITU will act as secretariat for the Expert Group. The Expert Group is open to ITU Member States and Sector Members, in addition to experts that participated in the previous iterations of the GCI.

The composition of the Expert Group should reflect regional diversity, gender diversity, diversity of expertise, as well as the balance amongst different stakeholders, including governments, the private sector, and academia.

Weightage Process

The overall evaluation process follows these steps:

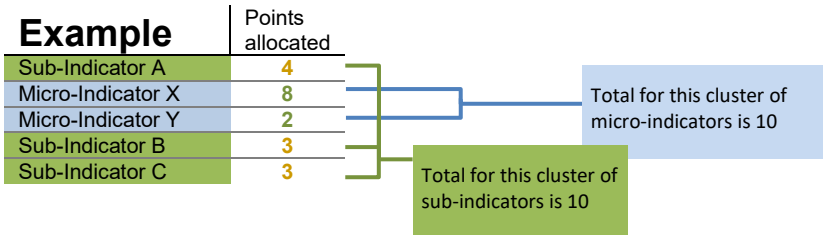
1. ITU will provide each individual Expert Group member with all relevant materials, specifically:
    a. Weightage spreadsheet with GCI questions
    b. Terms of Reference, with how-to guide and indicator explanations (this document)
2. There will be a GCI Expert Group meeting on **15 October 2020** to discuss the process, and answer questions.
3. After the initial meeting, Expert Group members will independently fill in the weightage Excel spreadsheet with their weightage recommendation for each indicator, sub-indicator, and micro-indicator, and submit to gci@itu.int by **31 October 2020.**
4. Once all recommendations have been submitted by individual Expert Group members, the weightage recommendations will be averaged and compiled into a single weightage spreadsheet.
5. The averaged weightage recommendations will be shared with the Expert Group members.

ANNEX A: HOW TO ALLOCATE WEIGHTS

You should only review weightages for pillars in which you have indicated expertise. Weightages allocated for pillars for which you have not indicated expertise will not be considered.

The GCI is built on a nested hierarchical model. Each "branch" of the model will herein be referred to as a cluster, such as a cluster of indicators, cluster of sub-indicators, and cluster of micro-indicators.

Within each cluster, you can allocate 10 points. You should allocate more points to indicators/sub-indicator/micro-indicators that are more important, based on your expertise.



How to Use the Weightage Spreadsheet

These instructions refer to the spreadsheet *GCI-Questionnaire-weightage-calculation.xlsx*.

This file is designed to be used in Microsoft Excel. Certain functions may not work in other programs.

Getting Started

1. Enter your name.
2. Check the pillars for which you are evaluating weights. These should match your indicated areas of expertise.
3. You can click on the name or icon for each pillar to navigate to the pillar for which you are giving input.

Entering Weights

4. Change the weight of an indicator, sub-indicator, or micro-indicator either by typing a number in the cell or using the scroll buttons to increase or decrease the numbers.
    a. You have 10 points to allocate across a cluster. If you over or under allocate, all cells in a cluster will turn red, like the below:

    b. The scroll arrows up and down will change the number in whole integers.
    c. To enter fractions, start the number with an =. For example, =1/3 for ⅓.
    d. If you do not want to allocate all 10 points, or wish to over-allocate, please make a note within the comments. Your weightage will be rebalanced out of 10 for when expert responses are arithmetically averaged.

5. You can leave any comments you have about the indicator, sub-indicator, or micro-indicator weighting in the Comments column.
6. You can click on the link *GCIv4 Definitions* link to better understand what is meant by any indicator.
7. The *Weight in overall GCI* section shows how much this indicator, based on your scoring, will weigh in the final GCI. You cannot edit or change these cells.

Finishing up

1. When you are finished, click “Save As” (for information on how to do this, refer to Microsoft Support instructions), appending your name to the end.
   Ex. *GCI-Questionnaire-weightage-calculations-**NAME**.xlsx*
2. Attach your spreadsheet to an email, and email it to gci@itu.int by the assigned date.

ANNEX B: DEFINITION OF PILLARS AND INDICATORS

Legal Measures

Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common legislative and regulatory basis, whether on the matter of prohibition of specified criminal conduct or minimum regulatory requirements.

The legal environment can be measured based on the existence of legal institutions and effective frameworks dealing with cybersecurity and cybercrime. It is composed of the following performance indicators:

- **Cybercrime Substantive Law**

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 and behaviors.

- **Cybersecurity Regulation**

Regulation is rule-based and meant to carry out a specific piece of legislation.

Technical Measures

Without adequate technical measures and capabilities to detect and respond to incidents, Member States and their respective entities remain vulnerable to cyber risks that can undermine the benefits stemming from the adoption of digital technologies Information. Member States therefore need to be capable of developing strategies for the establishment of accepted minimum-security criteria and accreditation schemes for software applications and systems. Technical measures can be measured based on the existence of technical institutions and frameworks dealing with cybersecurity endorsed or created by the Member State. The sub-group is composed of the following performance indicators:

- **National/Government Incidence Response Teams**

Computer incident response teams, 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 on a national level.

- **Sectoral CERT/CIRT/CSRIT Sectoral CERT/CIRT/CSRIT**

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, emergency services and the financial sector.

- **National Framework for the Implementation of Cybersecurity Standards**

Adoption of 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) is critical. 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.

- **Child Online Protection (COP)**

This Indicator measures the existence of a national agency dedicated to COP, the availability of a helpline to report issues associated with children online, and any other technical mechanisms and capabilities deployed to help protect children online.

Organizational Measures

Organizational and procedural measures are necessary for the proper implementation of any type of national initiative. A broad strategic objective needs to be set by the Member State, with a comprehensive plan in

implementation, delivery, and measurement. Structures such as national agencies need to be established in order to put the strategy into effect and evaluate the success or failure of the plan. The organizational structures can be measured based on the existence and number of institutions and strategies organizing cybersecurity development at the national level. The sub-group is composed of the following performance indicators:

- **National Cybersecurity Strategy/Policy**

The development of policy to promote cybersecurity as one of national top priorities. A national cybersecurity strategy should define the maintenance 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 Member State; respond, prevent cyber-attacks against critical infrastructures; and minimize damage and recovery time from cyber-attacks.

- **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. Such a body may also be directly responsible for the national CIRT.

- **Cybersecurity Metrics**

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.

Capacity Development Measures

Capacity building is intrinsic to the first three measures (legal, technical, and organizational). Understanding the technology, the risk and the implications can help to develop better legislation, better policies and strategies, and better organization as to the various roles and responsibilities. This area of study is most often tackled from a technological perspective; yet numerous socio-economic and political implications are applicable in this area.

A capacity building framework for promoting cybersecurity should include awareness-raising exercises and the availability of resources. The sub-group is composed of the following performance indicators:

- **Public Cybersecurity Awareness Campaigns**

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 centers, community colleges and adult education programs, schools and parent-teacher organizations to get the message across about safe cyber-behavior online.

- **Training for Cybersecurity Professionals**

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.

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 (ISC^2), and other.

- **National Education Programs and Academic Curriculums**

Establishment and the promotion of national education courses and programs 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.

- **Cybersecurity Research and Development Programs**

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.

- **National Cybersecurity Industry**

A favorable economic, political, and social environment supporting cybersecurity development incentivizes the growth of cyber security-related enterprises in the private sector. 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 favorable environment and drives the growth of cybersecurity start-ups and associated cyber-insurance markets.

- **Incentive Mechanisms**

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.

Cooperation Measures

Cybersecurity requires input from all sectors and disciplines and for this reason needs to be tackled from a multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Information sharing is difficult at best between different disciplines, and within private sector operators. It becomes increasingly so at the international level. The sub-group is composed of the following performance indicators:

- **Bilateral Agreements**

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).

- **Participation in International Mechanisms (forums)**

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.

- **Multilateral Agreements**

Multilateral agreements (one to multiparty 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 (i.e. the cooperation or exchange of information, expertise, technology and other resources).

- **Public-Private Partnerships**

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.

- **Inter-agency Partnerships**

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