ITU-D Cybersecurity Program
Global Cybersecurity Index – GCIv5
Reference Model (Methodology)

Contents

History and Background

First published in 2015, the Global Cybersecurity Index (GCI) helps countries improve their commitment to cybersecurity through identifying areas of strength and growth in cybersecurity and highlighting good practices. Through the data collected, the GCI highlights cybersecurity commitments for Member States to 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. Specifically, Member States are invited "*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*." The ultimate goal is to foster a global culture of cybersecurity and the integration of cybersecurity at the core of information and communication technologies.

The preceding editions of the Global Cybersecurity Index will follow recommendations of ITU-D Resolution 45 (Rev. Kigali, 2022) that clearly defines the work done through the Global Cybersecurity Index (GCI) and recommends BDT "to consider the results of the GCI to guide its cybersecurity-related initiatives, especially taking into account the gaps identified through the GCI process."

Previous editions include:

Edition name	GCIv1	GCIv2	GCIv3	GCI 2020 (GCIv4)
Edition number	1	2	3	4
Countries participating	105 countries	136 countries	155 countries	169 countries
Year data collected	2013-14	2016	2017-2018	2020
Year published	2015	2017	2019	2021
Notes	In partnership with ABI Research			

The GCI Questionnaire, with its respective indicators, sub-indicators, and micro-indicators, is updated between editions in consultation with ITD-D Study Group Question: *Securing information and communication networks: Best practices for developing a culture of cybersecurity of ITU Members*.

As a result of the continued interest by Member States in the GCI, ITU is compiling a fifth edition (GCIv5) in consultation with the GCI Expert Group as recommended by Resolution 45 (Rev. Kigali, 2022).

Scope

The Global Cybersecurity Index (GCI) is a composite index combining a variety of cybersecurity indicators into measures, based on the five pillars of the Global Cybersecurity Agenda (GCA). These pillars form the five pillars of GCI. The main objectives of GCI are to measure:

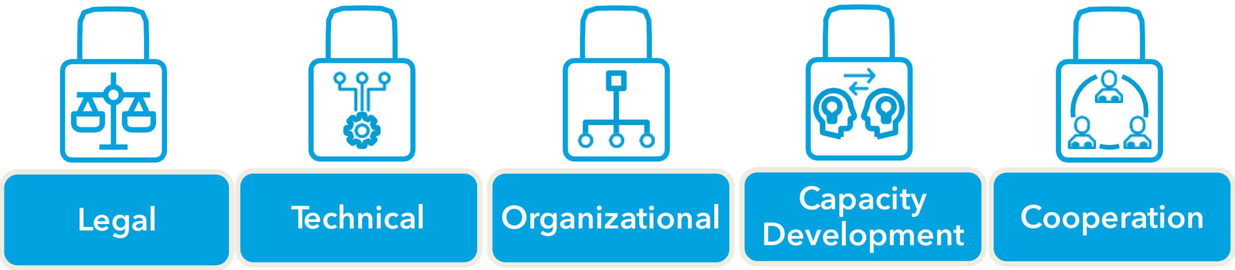
- the types, levels, and evolution over time of countries' cybersecurity commitments;
- progress in cybersecurity commitment from a global perspective;
- progress in cybersecurity commitment from regional perspectives;

- the cybersecurity commitment divide: the difference between countries in terms of their level of engagement in cybersecurity initiatives.

The Global Cybersecurity Index aims to help countries identify areas for improvement in the field of cybersecurity, thus helping to raise the overall level of cybersecurity worldwide. The GCI also collects good practices, which countries can learn from, in order to improve their own cybersecurity practices and adopt more harmonized approaches.

Conceptual Framework

The Global Cybersecurity Index focuses on following five pillars as overarching areas of cybersecurity commitments by countries:



Legal Measures: Legislative tools, such as laws, regulations, and policies, define the rights, responsibilities, and protections afforded on key issues related to cybersecurity, such as on the matter of prohibition of specified criminal conduct, or minimum regulatory requirements.

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 of digital technologies. 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 endorsed or created by the Member State for dealing with cybersecurity.

Organizational Measures: Organizational measures are necessary for the proper implementation of national initiative. A broad strategic objective needs to be set by the Member State, with a comprehensive plan for implementation, delivery, and measurement. Structures such as national agencies need to be established in order to put cybersecurity strategies 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.

Capacity Development Measures: Capacity development is intrinsic to legal, technical, and organizational measures. Understanding cybersecurity technologies, risks, and implications can help to develop better legislation, better policies, better strategies, and better organization as to roles and responsibilities. Capacity development encompasses both the development of knowledge and skills among the basic population, professionals whose work touches on cybersecurity, and as well as specialists within the sector.

Cooperation Measure: Cybersecurity efforts are more successful when they build on all impacted sectors and disciplines and needs to be tackled with a holistic multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Cooperation can include activities such as joint initiatives, information sharing, trainings, and other activities which connect professionals, officials, and other actors seeking to improve cybersecurity.

Computational Methodology

The fifth edition of the GCI questionnaire is divided into five pillars: Legal, Technical, Organizational, Capacity Development, and Cooperation Measures, which include a total of 20 indicators, with 64 sub-indicators and 28 micro indicators, based on 83 questions. The questions are intended to balance meaningful granularity in cybersecurity commitments, while maintaining a high-level view. The indicators can be found in the **Error! Reference source not found.** (Annex A).

The indicators are selected based on:

- relevance to the Global Cybersecurity Agenda pillars;
- relevance to the Global Cybersecurity Index scope and conceptual framework;
- ability of member states to accurately answer questions;
- possibility of cross verification through secondary data.

This edition uses ternary (yes, partial, no) answers to eliminate opinion-based evaluation and any possible bias towards certain types of responses. Moreover, a simple ternary concept allows quicker and more complex assessment as it does not require lengthy answers, which accelerates and streamlines providing answers and further evaluation. The respondent should only confirm the presence of, or lack of, specific pre-identified cybersecurity solutions.

To ensure accuracy, countries will be required to support their answer through a feature of uploading supporting documents and URLs. A comment section will be added to each pillar to allow countries provide good practices that tell the impact story of their cybersecurity evolution.

For this fifth edition and all future editions, the GCI will be restructured into levels of commitment as per Resolution 45 at WTDC (World Telecommunication Development Conference), Kigali, Rwanda, June 2022, where Member States recommended that the GCI adopts a tier-based approach of grouping countries rather than rankings to provide a more meaningful assessment of areas of strength and improvement to countries. Thus, the Methodology Expert Group meetings will be tasked to identify a suitable tier framework.

Overall GCI process flow

1. The GCI Questionnaire is revised considering feedback received from the Member States and the GCI Expert Group. The Questionnaire is submitted to the Study Group 2 meeting for further discussion.
2. As per ITU-D Resolution 45 (Rev. Kigali, 2022), the Global Cybersecurity Index will continue to be advised by a "GCI Expert Group" on issues related to methodology, structure, questions, and weightage.

3. A Correspondence Group, a working group of the GCI Expert Group is formed and comprises of experts and willing Member States representatives, to provide recommendations and feedback on the Questionnaire.
4. The BDT Secretariat makes appropriate revisions based on the consultations with the Correspondence Group, before BDT management approves the Questionnaire, or submits it, in part or as a whole, for further feedback from the Correspondence Group.
5. The approved Questionnaire is sent for translation into all six (6) official UN languages.
6. Two further working group meetings of the GCI Expert Group are held for consultation on tiers and weightage distribution.
7. The Director of BDT invites, via letter, all ITU Member States and the State of Palestine, to participate in the GCI survey. The letters serve to inform them of the GCI and requests them to designate a focal point responsible for collecting all relevant country data and completing the GCI Questionnaire.
8. The designated focal points are officially invited to respond to the Questionnaire via an online portal.
9. BDT Secretariat carries out secondary data collection for countries that respond to the questionnaire, which includes:
    - Identifying any missing responses, supporting documents, links, etc.
    - The focal point improving the accuracy of the responses where necessary.
    - The corrected draft questionnaire being sent to each focal point for final approval.
    - The validated questionnaire being used for analysis, scoring and ranking.
10. BDT Secretariat carries out primary data collection for countries that do not respond to the questionnaire, which includes:
    - ITU drafting initial response to the questionnaire using publicly available data and online research.
    - The draft questionnaire being sent to focal points for review.
    - Focal points improving the accuracy and returning the draft questionnaire.
    - The corrected draft questionnaire being sent to each focal point for final approval.
    - The validated questionnaire being used for analysis, scoring, and ranking.
11. A report is produced with summaries of key trends and best practices with consideration to recommendations on tiers and weightage made by the GCI Expert Group.

Note: Should a country not provide a focal point for the GCI questionnaire, ITU will establish contact with the institutional focal point from the ITU Global Directory.

ANNEX A: 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:

1.1. Cybercrime 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.

1.2. Cybersecurity Regulation

A regulation is a rule or principle governing behavior or practice; esp. such a directive established and maintained by an authority[1]. It is rule-based and meant to carry out a specific piece of legislation. Cybersecurity regulation designates 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.

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:

1.1. National/Government Computer Incidence Response Teams

CIRT (Computer Incident Response Team), CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team) 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. They have national responsibility to provide capabilities to identify, defend, respond, and manage cyber threats and enhance cyberspace security in the nation state. This ability needs to be coupled with the gathering of its own intelligence instead of relying on secondary reporting of security incidents whether from the CIRT's constituencies or from other sources.

1.2. 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, energy, academia, and the financial sector.

1.3. 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

[1] https://www.oed.com/view/Entry/161427?redirectedFrom=regulation

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.

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:

1.1. 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.

1.2. 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 solely responsible for the national CIRT.

1.3. 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.

1.4. Child Online Protection (COP) Strategies and Initiatives

A national Child Online Protection strategy should have an action plan to promote safe online environments for children worldwide. It will be necessary to put in place a body of policy that establishes a set of rules and objectives that makes it clear that any and every crime that can be committed against a child in the real world can, mutatis mutandis, also be committed on the Internet or any other electronic network.

Capacity Development Measures

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

1.1. 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.

1.2. 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 (ISC²), and other.

1.3. Cybersecurity educational programs as part of national academic curricula

Establishment and 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.

1.4. Cybersecurity Research and Development (R&D) 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.

1.5. National Cybersecurity Industry

A favorable economic, political, and social environment supporting cybersecurity development incentivizes the growth of cybersecurity-related enterprises in the private sector. The existence of public awareness campaigns, workforce development, capacity development, 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.

1.6. Government Incentive Mechanisms

This Indicator looks at any incentive efforts by the government to encourage capacity development 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:

1.7. Cybersecurity 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).

1.8. Cybersecurity Multilateral Agreements

Multilateral agreements (one to multiparty agreements) refer 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).

1.9. Cybersecurity Mutual Legal Assistance Agreements

It may also include ratification of international agreements containing clauses related to Mutual Legal Assistance and cybersecurity.

1.10. Public-Private Partnerships

Public-private partnerships (PPP) refer to ventures between the public and private sector. It may be in the form of a long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance[2]. 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.

1.11. 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.

[2] https://ppp.worldbank.org/public-private-partnership/overview/what-are-public-private-partnerships