ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection
4-6 April 2018
Odessa, Ukraine
ITU Regional Initiatives for Europe and for CIS on Building Confidence and Security in the use of Telecommunications/ICTs

Global Cybersecurity Index An overview

GLOBAL CYBERSECURITY INDEX
GCIv3
MEASURING COMMITMENT TO CYBERSECURITY

Rosheen Awotar-Mauree
Programme Officer
ITU Office for Europe

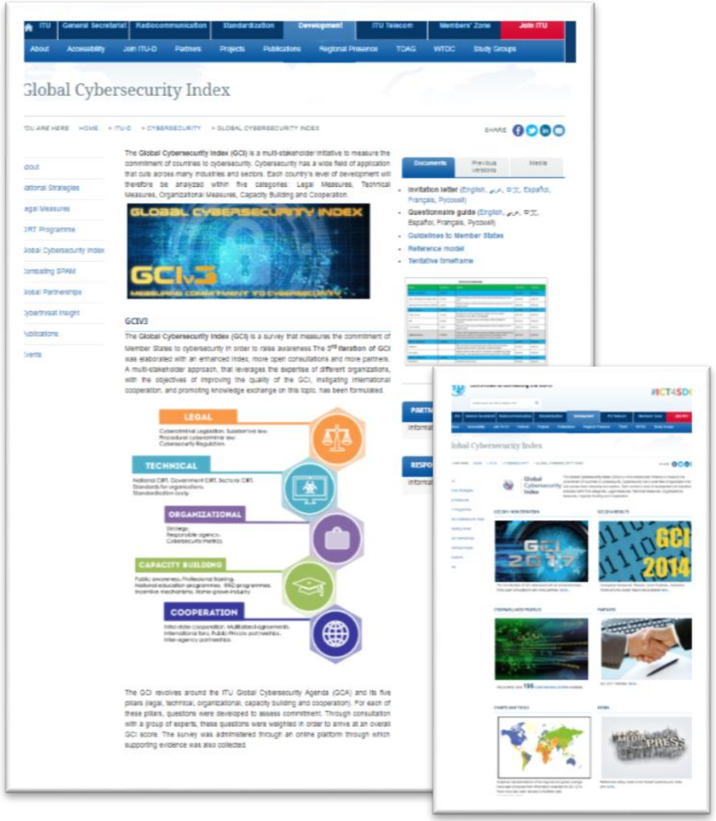
What is GCI …

GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States ***cybersecurity commitment*** with regard to the five pillars identified by the High-Leve Experts and endorsed by the GCA.

“GCI is a capacity building tool, to support countries to improve their national cybersecurity posture”

Background

- GCIv1 – the 1st iteration of the GCI has started in 2013-2014 period -**105** countries responded
- GCIv2 – the 2nd iteration covered 2016-2017 period – **134** countries responded
- **GCIv3 – 3rd iteration started in March 2018**


ITU | General Secretariat | Radiocommunication | Standardization | Development | ITU Telecom | Members' Zone | Join ITU

About | Accessibility | Join ITU-D | Partners | Projects | Publications | Regional Presence | TDAG | WTDC | Study Groups

Global Cybersecurity Index

YOU ARE HERE HOME > ITU-D > CYBERSECURITY > GLOBAL CYBERSECURITY INDEX — SHARE

About · National Strategies · Legal Measures · CIRT Programme · Global Cybersecurity Index · Combating SPAM · Global Partnerships · Cyberthreat Insight · Publications · Events

The **Global Cybersecurity Index** (GCI) is a multi-stakeholder initiative to measure the commitment of countries to cybersecurity. Cybersecurity has a wide field of application that cuts across many industries and sectors. Each country's level of development will therefore be analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.

Documents | Previous versions | Media

- **Invitation letter** (English, عربي, 中文, Español, Français, Русский)
- **Questionnaire guide** (English, عربي, 中文, Español, Français, Русский)
- Guidelines to Member States
- Reference model
- Tentative timeframe

GCIv3

The **Global Cybersecurity Index** (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.The 3rd **iteration of GCI** was elaborated with an enhanced index, more open consultations and more partners. A multi-stakeholder approach, that leverages the expertise of different organizations, with the objectives of improving the quality of the GCI, instigating international cooperation, and promoting knowledge exchange on this topic, has been formulated.

LEGAL: Cybercriminal Legislation. Substantive law. Procedural cybercriminal law. Cybersecurity Regulation.

TECHNICAL: National CIRT. Government CIRT. Sectoral CIRT. Standards for organizations. Standardization body.

ORGANIZATIONAL: Strategy. Responsible agency. Cybersecurity metrics.

CAPACITY BUILDING: Public awareness. Professional training. National education programmes. R&D programmes. Incentive mechanisms. Home-grown industry.

COOPERATION: Inter-state cooperation. Multilateral agreements. International fora. Public-Private partnerships. Inter-agency partnerships.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected.

GLOBAL CYBERSECURITY INDEX
GCIv3
MEASURING COMMITMENT TO CYBERSECURITY
#ICT4SDG
GCI 2017
GCI 2014

All iterations include primary research in order to provide global coverage of the 194 Member States

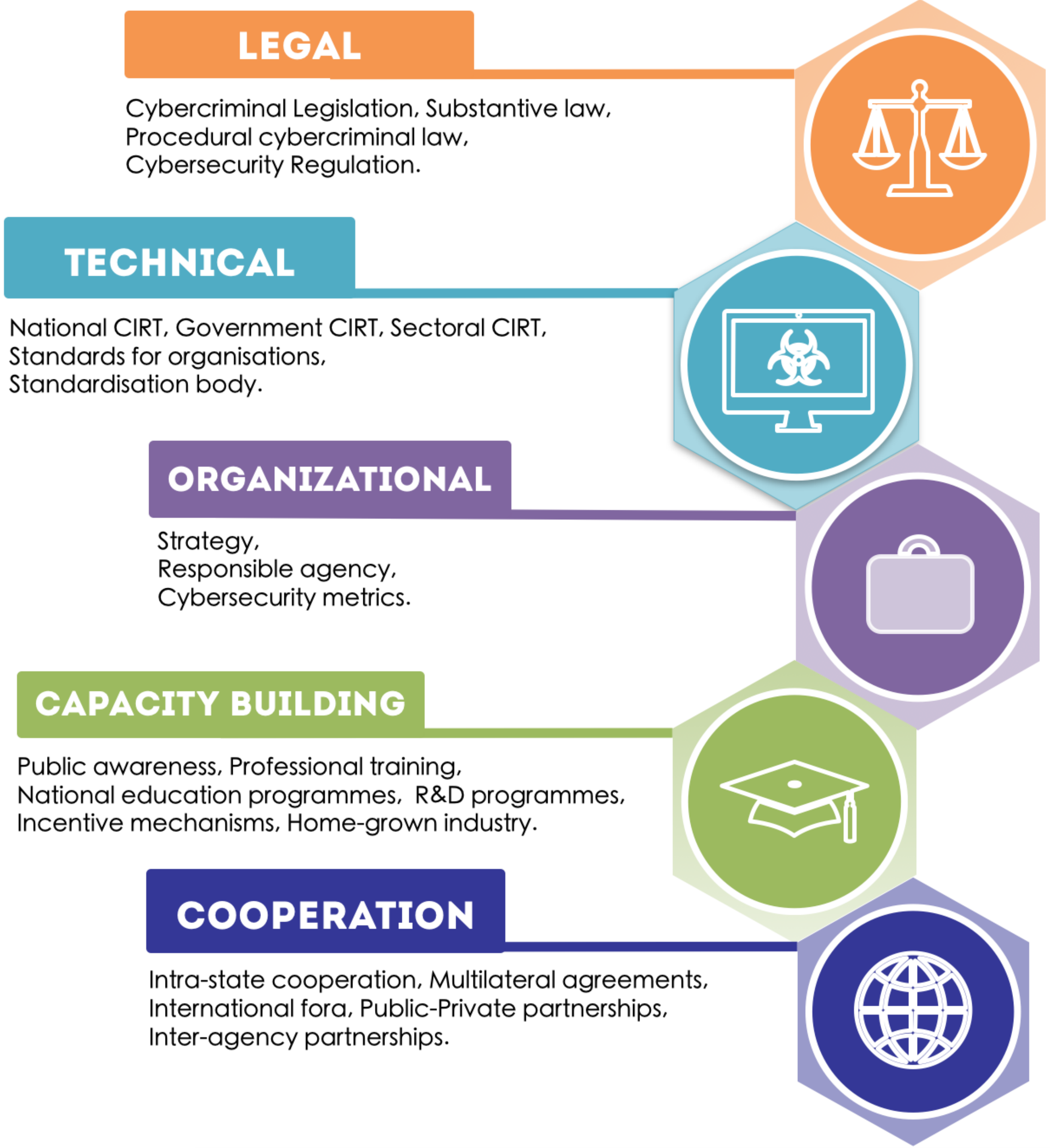
GCI aims to

- Help countries identify areas for improvement
- Motivate action to improve relative GCI rankings
- Raise the level of cybersecurity awareness worldwide
- Help to identify and promote best practices
- Foster a global culture of cybersecurity

GCI overall approach

The GCIv3 includes 25 indicators and 50 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

- relevance to the five GCA(Global Cybersecurity Agenda) pillars and in contributing towards the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data.



LEGAL

Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.

TECHNICAL

National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations,
Standardisation body.

ORGANIZATIONAL

Strategy,
Responsible agency,
Cybersecurity metrics.

CAPACITY BUILDING

Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.

COOPERATION

Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

GCI Indicators

Legal

- Cybercriminal legislation
- Cybersecurity regulation
- Cybersecurity training on regulation and laws

Technical

- National CIRT
- Government CIRT
- Sectoral CIRT
- Standards implementation framework for organizations
- Standards and certification for professionals

Organizational

- Strategy
- Responsible agency
- Cybersecurity metrics

Capacity Building

- Standardization bodies
- Best practice
- R & D programmes
- Public awareness campaigns
- Professional training courses
- National education programmes and academic curricula
- Incentive mechanisms
- Home-grown cybersecurity industry

Cooperation

- Bilateral agreements
- Multilateral agreements
- International fora participation
- Public-private partnerships
- Interagency partnerships

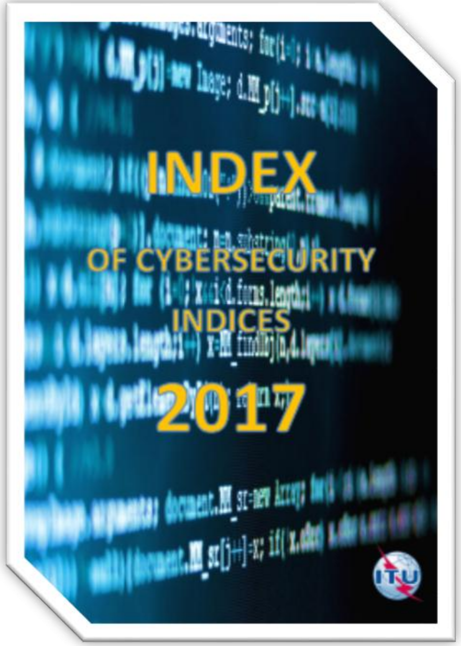
Unique Value

What makes the GCI unique is the balanced combination of:

- The **broad geographic range** covering all Member States
- The **multi-stakeholder** approach
- The **scoring and ranking** mechanisms
- The **cyberwellness** country **profiles**

Index of Indices – situates GCI unique value

	Metrics			Content										Presentation Format			
	Score	Ranking	Information Society Development Score (ISD) score)	Cyber Maturity	Cyber Threats	Cyber Vulnerabilities	Organizational	Technical	Economical	Legal Framework	Cooperation	Capacity Buiding	Recommandations	Profiles	Website	PDF	Visualization	No. of Iterations
Cyber Maturity in the Asia-Pacific Region	x			x					x	x	x			x	x	x		2
National Cyber Security Index	x	x	x	x	x		x	x		x	x	x			x	x	x	1
Global Cybersecurity Index	x	x					x	x		x	x	x		x	x	x	x	2
Kaspersky Cybersecurity Index	x				x				x					x	x	x	x	1
Asia-Pacific Cybersecurity Dashboard		x		x			x			x	x	x		x	x	x		2
Cyber Readiness Index 2.0	x	x		x		x	x		x	x	x			x	x	x		2
Cybersecurity Poverty Index	x			x			x	x							x		x	1
CyberGreen Index	x	x			x			x							x		x	1
The Accenture Security Index	x	x			x		x	x	x		x		x		x	x	x	1
Global Cybersecurity Assurance Report Cards	x				x	x		x							x		x	1
Index of Cybersecurity					x			x							x	x	x	73
Cybersecurity Capability Maturity Model				x			x	x		x	x	x			x	x		2
Cyber Power Index	x	x		x			x	x		x		x			x	x	x	1
IBM X-force Threat Intelligence Index					x			x							x			3


INDEX
OF CYBERSECURITY
INDICES
2017

Index from different organizations and companies are researched and compared

GCI v2 Partners

FIRST
Improving Security Together

unicri
United Nations
Interregional Crime and Justice
Research Institute

KISA
Korea Internet & Security Agency

INDIANA UNIVERSITY

ACTIONABLE
THREAT INTELLIGENCE
REDTEAM
CYBER

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE

POTOMAC INSTITUTE FOR POLICY STUDIES

RCC
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

NTRA
EGYPT
National Telecom
Regulatory Authority

INTERPOL

WORLD BANK GROUP

UNODC
United Nations Office on Drugs and Crime

European
Commission
Joint Research Centre

Score calculation

Panel of Expert: an average for each question weightage provided by GCI Partners

2. Do you have any technical measures?	19.12
2.1. Is there a CIRT, CSIRT or CERT with national responsibility?	4.65
2.1.1. Does it have a government mandate?	1.33
2.1.2. Does the CIRT, CSIRT or CERT conduct recurring cybersecurity exercise?	1.23
2.1.3. Is the CIRT, CSIRT or CERT affiliated with FIRST?	1.04
2.1.4. Is the CIRT, CSIRT or CERT affiliated with any other CERT communities? (regional CERT)	1.06
2.2. Is there a Government CERT?	3.03
2.3. Are there any sectoral CERTs?	2.71

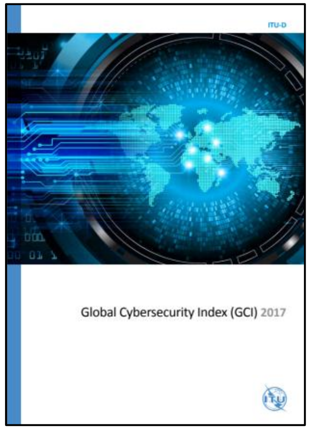
1. Is there any Cyber related legislation?	20.94
2. Do you have any technical measures?	19.12
3. Do you have any organizational measures?	19.67
4. Do you have any capacity building activities?	18.93
5. Do you have any cooperative measures?	21.34

Total of all weightages = 100

Presentation of analysed information

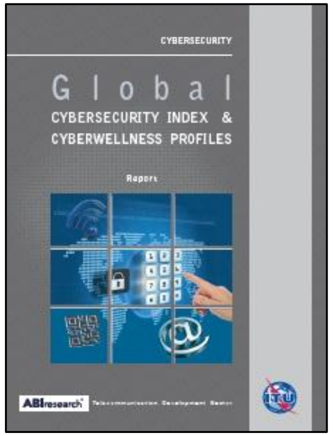
Global Report

Regional Report



ITU-D

Global Cybersecurity Index (GCI) 2017



CYBERSECURITY

Global

CYBERSECURITY INDEX & CYBERWELLNESS PROFILES

Report

ABIresearch

Telecommunication Development Sector

Cyberwellness Profiles

Factual information on cybersecurity achievements on each country

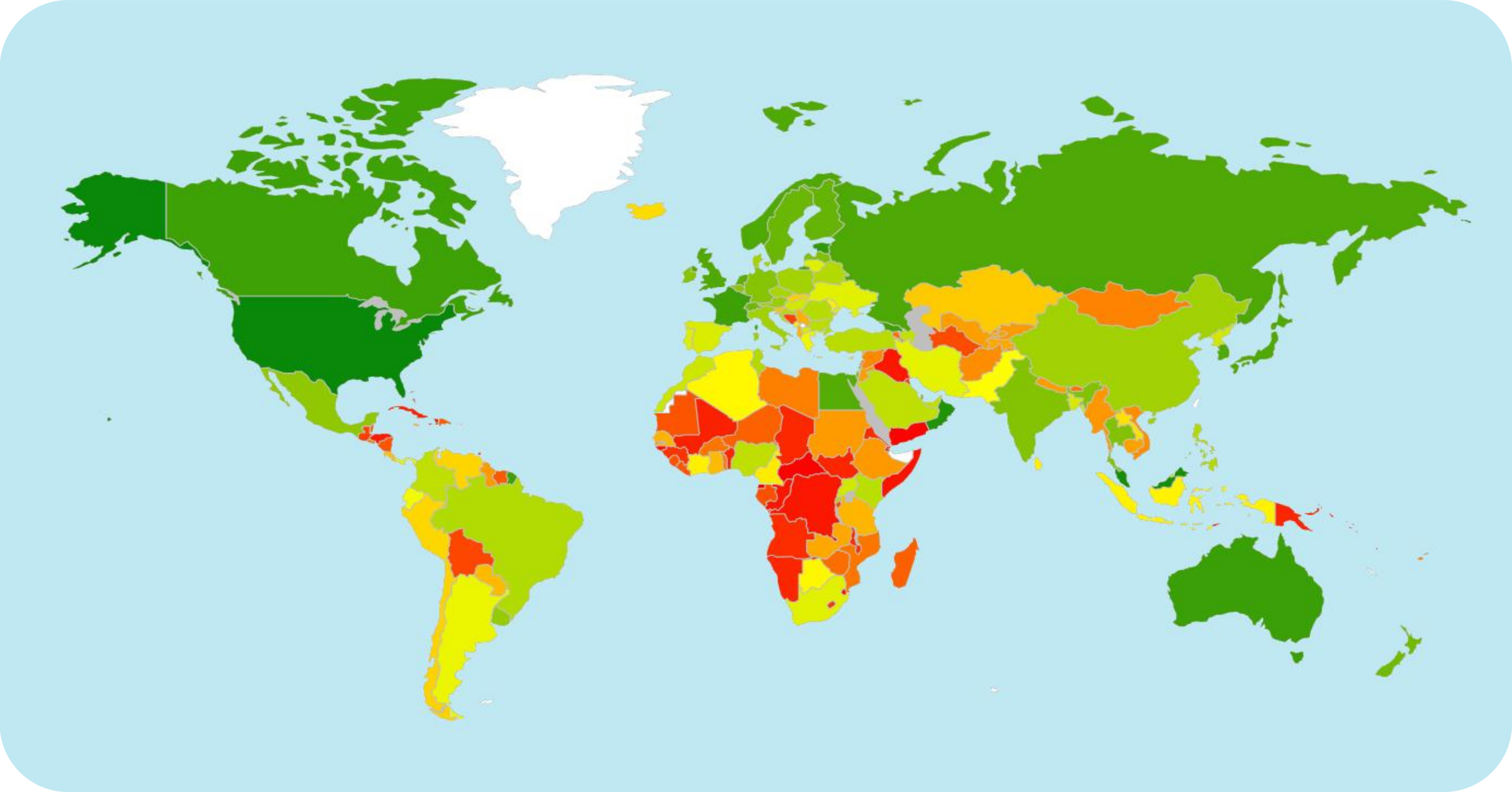
CYBERWELLNESS PROFILE ITALY

CYBERWELLNESS PROFILE RUSSIA

CYBERWELLNESS PROFILE UNITED KINGDOM

Focus on Europe and CIS Results

GCI 2017 Heat Map



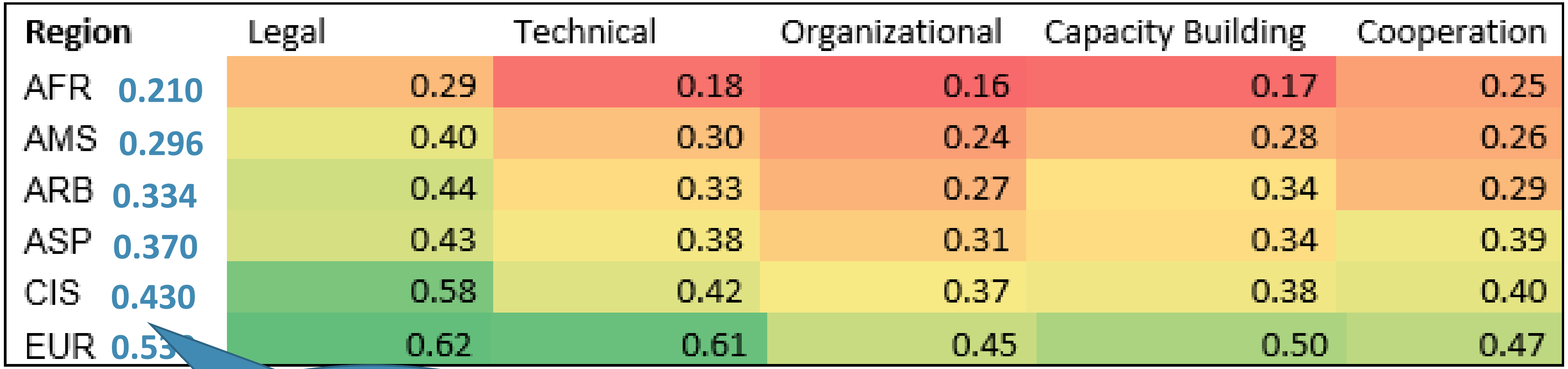
Commitment levels 🟩 High 🟨 Medium 🟥 Low

GCI 2017 : Global Top Ten

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Maximum score is 1

GCI 2017: Heat map – regional perspective



Region		Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.210	0.29	0.18	0.16	0.17	0.25
AMS	0.296	0.40	0.30	0.24	0.28	0.26
ARB	0.334	0.44	0.33	0.27	0.34	0.29
ASP	0.370	0.43	0.38	0.31	0.34	0.39
CIS	0.430	0.58	0.42	0.37	0.38	0.40
EUR	0.53	0.62	0.61	0.45	0.50	0.47

Regional Score on a maximum on 1

GCI 2017 for ITU Europe & CIS region

43 Countries EUROPE : Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lithuania,Luxembourg, Malta, The Former Yugoslav Republic of Macedonia, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Vatican,United Kingdom

11 Countries CIS : Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Moldova, Russian Federation, Tajikistan, Turkmenistan, Ukraine, Uzbekistan

GCI TIERS out of 54 countries

- *Leading stage* refers to the **22** countries (i.e., GCI score in the 60th percentile and higher) that demonstrate high commitment.
- *Maturing stage* refers to the **22** countries (i.e., GCI score between the 30th and 59th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Initiating stage* refers to the 10 countries (i.e., GCI score less than the 30th percentile) that have started to make commitments in cybersecurity.

Some responses for Europe & CIS regions

Out of 54

- ✓ 24 countries have Cybercriminal legislation
- ✓ 32 countries have Cybersecurity legislation
- ✓ 20 countries have Cybersecurity training on regulation and laws
- ✓ 35 countries have National CIRTs
- ✓ 43 countries have Government CIRTs
- ✓ 34 countries have sectoral CIRTs
- ✓ 38 countries have an entity responsible for Child Online Protection
- ✓ 7 countries use Cybersecurity metrics at national level
- ✓ 12 countries have standardization bodies handling Cybersecurity
- ✓ 23 countries have good practices in Cybersecurity
- ✓ 17 countries have R&D programmes in Cybersecurity

Some Noteworthy practices

United Kingdom issued in 2016 its second five years *National Cyber Security Strategy*. The strategy, issued by the Cabinet Office, aims to make the country one of the safest places in the world to carry out online business and doubles investment in cybersecurity compared to the first plan.

Netherlands uses metrics annually in order to measure cybersecurity development at a national level, summarized in the Cyber Security Assessment Netherlands report. The National Cyber Security Centre (NCSC) compiles disclosure reports, security advisories and incidents using a registration system. The metrics allow trends to be observed and acted on.

UK and China agreed to establish a high-level security dialogue to strengthen exchanges and cooperation on security issues such as non-proliferation, organized crime, cyber crime and illegal immigration. The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage

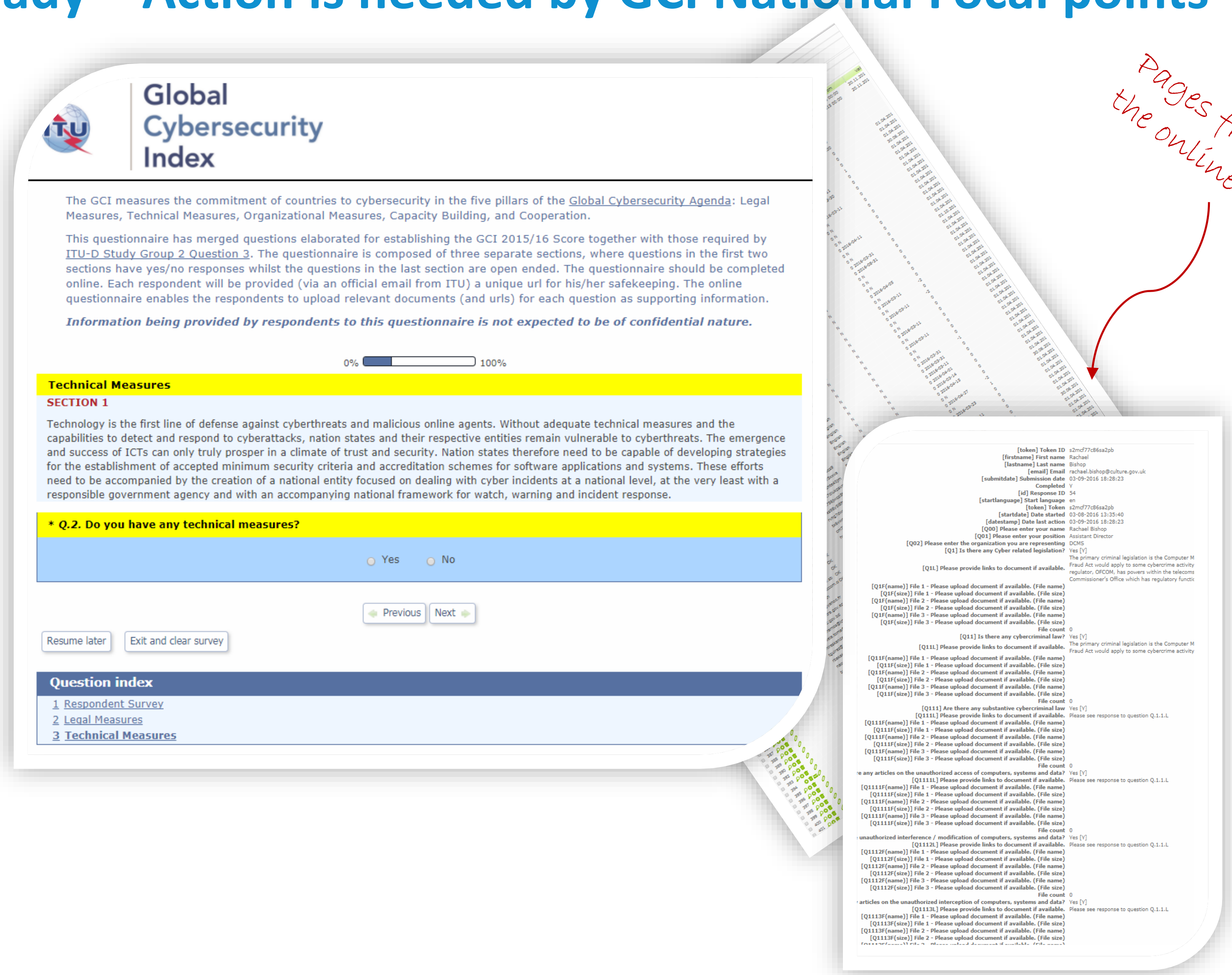
- Cyber Security information Sharing Partnership (CiSP) - https://www.cert.gov.uk/cisp/

Online Survey is Ready – Action is needed by GCI National Focal points

GCIv3

50

questions



Global Cybersecurity Index

The GCI measures the commitment of countries to cybersecurity in the five pillars of the Global Cybersecurity Agenda: Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation.

This questionnaire has merged questions elaborated for establishing the GCI 2015/16 Score together with those required by ITU-D Study Group 2 Question 3. The questionnaire is composed of three separate sections, where questions in the first two sections have yes/no responses whilst the questions in the last section are open ended. The questionnaire should be completed online. Each respondent will be provided (via an official email from ITU) a unique url for his/her safekeeping. 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.

0% 100%

Technical Measures

SECTION 1

Technology is the first line of defense against cyberthreats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, nation states and their respective entities remain vulnerable to cyberthreats. The emergence and success of ICTs can only truly prosper in a climate of trust and security. Nation 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. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents at a national level, at the very least with a responsible government agency and with an accompanying national framework for watch, warning and incident response.

***** Q.2. Do you have any technical measures?**

○ Yes ○ No

Question index

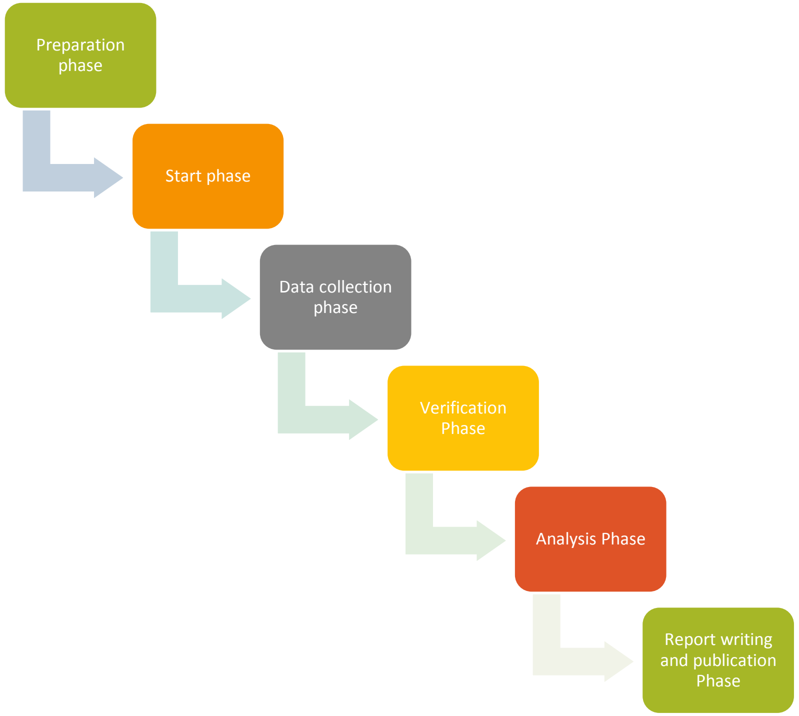
1 Respondent Survey
2 Legal Measures
3 Technical Measures

[token] Token ID	s2mcf77c86sa2pb
[firstname] First name	Rachael
[lastname] Last name	Bishop
[email] Email	rachael.bishop@culture.gov.uk
[submitdate] Submission date	03-09-2016 18:28:23
Completed	Y
[id] Response ID	54
[startlanguage] Start language	en
[token] Token	s2mcf77c86sa2pb
[startdate] Date started	03-08-2016 13:35:40
[datestamp] Date last action	03-09-2016 18:28:23
[Q00] Please enter your name	Rachael Bishop
[Q01] Please enter your position	Assistant Director
[Q02] Please enter the organization you are representing	DCMS
[Q1] Is there any Cyber related legislation?	Yes [Y]
[Q1L] Please provide links to document if available.	The primary criminal legislation is the Computer M Fraud Act would apply to some cybercrime activity regulator, OFCOM, has powers within the telecoms Commissioner's Office which has regulatory functic
[Q1F(name)] File 1 - Please upload document if available. (File name)	
[Q1F(size)] File 1 - Please upload document if available. (File size)	
[Q1F(name)] File 2 - Please upload document if available. (File name)	
[Q1F(size)] File 2 - Please upload document if available. (File size)	
[Q1F(name)] File 3 - Please upload document if available. (File name)	
[Q1F(size)] File 3 - Please upload document if available. (File size)	
File count	0
[Q11] Is there any cybercriminal law?	Yes [Y]
[Q11L] Please provide links to document if available.	The primary criminal legislation is the Computer M Fraud Act would apply to some cybercrime activity
[Q11F(name)] File 1 - Please upload document if available. (File name)	
[Q11F(size)] File 1 - Please upload document if available. (File size)	
[Q11F(name)] File 2 - Please upload document if available. (File name)	
[Q11F(size)] File 2 - Please upload document if available. (File size)	
[Q11F(name)] File 3 - Please upload document if available. (File name)	
[Q11F(size)] File 3 - Please upload document if available. (File size)	
File count	0
[Q111] Are there any substantive cybercriminal law	Yes [Y]
[Q111L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q111F(name)] File 1 - Please upload document if available. (File name)	
[Q111F(size)] File 1 - Please upload document if available. (File size)	
[Q111F(name)] File 2 - Please upload document if available. (File name)	
[Q111F(size)] File 2 - Please upload document if available. (File size)	
[Q111F(name)] File 3 - Please upload document if available. (File name)	
[Q111F(size)] File 3 - Please upload document if available. (File size)	
File count	0
re any articles on the unauthorized access of computers, systems and data?	Yes [Y]
[Q1111L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q1111F(name)] File 1 - Please upload document if available. (File name)	
[Q1111F(size)] File 1 - Please upload document if available. (File size)	
[Q1111F(name)] File 2 - Please upload document if available. (File name)	
[Q1111F(size)] File 2 - Please upload document if available. (File size)	
[Q1111F(name)] File 3 - Please upload document if available. (File name)	
[Q1111F(size)] File 3 - Please upload document if available. (File size)	
File count	0
unauthorized interference / modification of computers, systems and data?	Yes [Y]
[Q1112L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q1112F(name)] File 1 - Please upload document if available. (File name)	
[Q1112F(size)] File 1 - Please upload document if available. (File size)	
[Q1112F(name)] File 2 - Please upload document if available. (File name)	
[Q1112F(size)] File 2 - Please upload document if available. (File size)	
[Q1112F(name)] File 3 - Please upload document if available. (File name)	
[Q1112F(size)] File 3 - Please upload document if available. (File size)	
File count	0
articles on the unauthorized interception of computers, systems and data?	Yes [Y]
[Q1113L] Please provide links to document if available.	Please see response to question Q.1.1.L
[Q1113F(name)] File 1 - Please upload document if available. (File name)	
[Q1113F(size)] File 1 - Please upload document if available. (File size)	
[Q1113F(name)] File 2 - Please upload document if available. (File name)	
[Q1113F(size)] File 2 - Please upload document if available. (File size)	

Pages from the online survey.

How it functions. Main steps.

- Preparation phase
  - Elaboration of the survey in collaboration with experts an partners
  - Development of online survey system
  - Preparation of supporting documentation (guides, conceptual framework, letters etc.)
  - Announcement on the ITU website
- Start phase
  - Informing/invitation Member States via official letter from the BDT Director to Administrations (Responsible Ministry, organization, agency…)
  - Collection of contact details of Focal Point(s) assigned by the Administration
  - Contacting FPs and providing access to the online survey together with all necessary documents and instructions
  - Technical Support
- Data collection phase
  - Filling the questionnaire (FPs provide data, links, supporting documents etc.)
  - Collection of data from open sources for non-respondents (ITU helps Member States to appear in the Report)
- Verification Phase
  - ITU specialists verify and all provided data and contact FPs for more details if needed.
  - ITU shares the verified data with FPs
- Analysis Phase
  - Analysis of all collected data (for respondents and non-respondents).
  - Ranking. Preparation of comparison charts, maps, tables and other statistical elements.
  - Illustrative practices extraction.
- Report writing and publication Phase
  - Elaboration of the GCI Report
  - Publication on the ITU website and printing
  - Official launch and informing Member States
  - Follow-up



How to improve GCI score and position

- Identify a National GCI Focal point and inform ITU
- Make all relevant data available to the National GCI Focal point
- Seek clarifications by connecting the ITU GCI team

cybersecurity@itu.int

JOIN US

- As a partner
  - Add to this body of knowledge under construction
  - Your expertise on thematics to help enhance the GCI process and deliverables
  - Connect better with ITU and Member States

- As a respondent to questionnaire
  - Reflect your Country's achievements and plans for enhancing Cybersecurity
  - Share best practices
  - Position your country on the cybersecurity commitment scale

Thank you

www.itu.int

EURregion@itu.int

@ITU_EUR