ITU Global Cybersecurity Index 2020, 4th edition Weightage Recommendations

	Average of Weightage Recs
Legal Measures	
1 Cybercrime substantive law	6.22
1.1 Do you have substantive law on unauthorized online behavior?	4.11
1.1.1 Do you have substantive law on illegal access on devices, computer systems and data?	2.02
1.1.2 Do you have substantive law on illegal interferences (through data input, alteration, and suppression) on devices, data and computer system?	2.56
1.1.3 Do you have substantive law on illegal interception on devices, computer systems and data?	2.39
1.1.4 Do you have substantive law on online identity and data theft?	3.03
1.2 Do you have dispositions on computer-related forgery (piracy/copyright infringements)?	3.53
1.3 Do you have substantive law on online safety?	2.36
1.3.1 Do you have dispositions/legal measures on offences related to racist and xenophobic online material?	2.99
1.3.2 Do you have dispositions/legal measures on online harassment and abuse against personal dignity/integrity?	3.47
1.3.3 Do you have dispositions/legal measures related to Child Online Protection?	3.54
2 Is there any cybersecurity regulation related to…	3.78
2.1 Personal data/privacy protection?	2.70
2.2 Data breach/incident notification?	2.05
2.3 Cybersecurity audit requirements?	1.41
2.4 Implementation of standards?	0.82
2.5 Use of digital signatures in government services and applications (e-govt)?	0.79
2.6 Curbing of spam?	0.67
2.7 Identifying and protecting the national critical infrastructures?	1.55

	Average of Weightage Recs
Technical Measures	
1 National CERT/CIRT/CSIRT	3.04
1.1 Is there a National/Government CIRT, CSIRT or CERT?	2.41
1.2 Does your National/Government CIRT/CSIRT, CERT…	2.31
1.2.1 Develop and execute cybersecurity awareness activities?	2.63
1.2.2 Conduct regular cyber security exercises (CyberDrills)?	2.61
1.2.3 Provide publicly available Advisories?	2.44
1.2.4 Contribute to the issues of Child Online Protection?	2.31
1.3 Is the above CIRT, CSIRT or CERT affiliated with FIRST?	1.96
1.4 Is the above CIRT, CSIRT or CERT affiliated with a regional CERT (APCERT, AFRICACERT, EGC, OIC, OAS)?	1.80
1.5 Was the maturity level of the above CIRT, CSIRT or CERT services certified (ex. TI certification scheme under TF-CSIRT - SIM3 is a basis for certification)?	1.51
2 Sectorial CERT/CIRT/CSIRT (ex: financial, academia etc...)	2.44
2.1 Are there sectorial CIRTs, CSIRTs or CERTs in your country?	5.09
2.2 Does your sectorial CIRT/s, CSIRT/s or CERT/s:	4.91
2.2.1 Develop and execute cybersecurity awareness activities for the sector?	3.40
2.2.2 Actively participate in national CyberDrills?	3.38
2.2.3 Share sectorial related incidents within its constituency?	3.22
3 National framework for implementation of cybersecurity standards	2.46
3.1 Is there a framework for implementation/adoption of cybersecurity standards?	5.15
3.2 Does the framework include international standards (ITU-T, ISO/IEC, NIST, ANSI/ISA etc...)?	4.85
4 Child Online Protection	2.06
4.1 Are there any reporting mechanisms and capabilities deployed to help protect children online?	

	Average of Weightage Recs
Organizational Measures	
1 National Cybersecurity Strategy	4.76
1.1 Does your country have a national cybersecurity strategy/ policy ?	4.53
1.1.1 Does it address the protection of national critical infrastructures, including in the telecommunication sector?	2.49
1.1.2 Does it include reference to the national cybersecurity resilience?	2.86
1.1.3 Is the life cycle management (cybersecurity strategy) revised and updated on a continuous basis?	2.41
1.1.4 Is the cybersecurity strategy open to any form of consultation with national experts in cybersecurity?	2.23
1.2 Is there a defined action plan/roadmap for the implementation of cybersecurity governance?	3.33
1.3 Is there a national strategy for Child Online Protection?	2.14
2 Responsible Agency	3.09
2.1 Is there an agency responsible for cybersecurity at a national level?	2.73
2.2 Does the agency cover National Critical Infrastructure Protection?	2.89
2.3 Is there an agency overseeing national cybersecurity capacity development?	2.34
2.4 Is there any agency overseeing the child online protection initiatives at the national level?	2.04
3 Cybersecurity metrics	2.15
3.1 Are there any cybersecurity audits performed at a national level?	3.40
3.2 Are there metrics for assessing cyberspace associated risk at a national level?	3.16
3.3 Are there measures for assessing the level of cybersecurity development at a national level?	3.44

	Average of Weightage Recs
Capacity Development	
1 Public cybersecurity awareness campaigns	2.07
1.1 Are there public awareness campaigns targeting SMEs, private sector companies and government agencies?	2.27
1.2 Are there public awareness campaigns targeting civil society (ex: NGOs, community-based organizations?)	1.79
1.3 Are there public awareness campaigns targeting citizens?	1.87
1.4 Are there public awareness campaigns targeting the elderly?	1.07
1.5 Are there public awareness campaigns targeting persons with special needs?	1.25
1.6 Are there any public awareness campaigns involving parents, educators and children (COP)?	1.75
2 Training for Cybersecurity Professionals	1.41
2.1 Does your government develop/support professional training courses in cybersecurity?	3.66
2.2 Is there an accreditation program for cybersecurity professionals in your country? (ex: Institutes accrediting cybersecurity professionals, or any other mechanism)?	3.21
2.3 Are there a national sector-specific educational programs/trainings for professionals on cybersecurity courses?	3.13
2.3.1 For law enforcement (police officers and enforcement agents)?	2.45
2.3.2 For judicial and other legal actors (judges, solicitors, barristers, attorneys, lawyers, paralegals etc.)?	2.30
2.3.3 For SMEs/private companies?	2.66
2.3.4 For other public sector/government officials?	2.59
3 Does your government/organization develop or support any educational programs or academic curricula in cybersecurity…	1.51
3.1 In primary education?	2.91
3.2 In secondary education?	3.00
3.3 In higher education?	4.09
4 Research and development programs	1.47
4.1 Are there cybersecurity R&D activities at the national level?	
4.1.1 Are there private sector cybersecurity R&D programs?	3.16
4.1.2 Are there public sector cybersecurity R&D programs?	3.09
4.1.3 Are higher education institutions (ex: academia, universities) engaged in R&D activities?	3.75
5 National cybersecurity industry	1.81
5.1 Is there a national cybersecurity industry (service providers, system integrators, system developers etc.)?	
6 Are there any government incentive mechanisms in place…	1.73
6.1 to encourage capacity development in the field of cybersecurity?	5.07

	Average of Weightage Recs
6.2 for the development of a cybersecurity industry (ex: support to start-ups and R&D activities in academia and other)?	4.93

	Average of Weightage Recs
Cooperative Measures	
1 Bilateral agreements on cybersecurity cooperation with other countries	2.06
1.1 Do you have bilateral agreements on cybersecurity cooperation with other countries?	
1.1.1 Is information sharing part of the agreement(s)?	3.76
1.1.2 Is capacity building part of the agreement(s)?	3.35
1.1.3 Is mutual legal assistance part of the agreement(s)?	2.89
2 Government participation in international mechanisms related to cybersecurity activities	2.13
2.1 Does your government/organization participate in international mechanisms related to cybersecurity activities?	
3 Cybersecurity multilateral agreements	2.04
3.1 Does your government have multilateral agreements on cybersecurity cooperation?	
3.1.1 Is information sharing part of the agreement(s)?	5.33
3.1.2 Is capacity building part of the agreement(s)?	4.67
4 Partnerships with the private sector (PPPs)	1.89
4.1 Does your government engage in PPPs with locally established companies?	5.47
4.2 Does your government engage in PPPs with foreign owned companies in your country?	4.53
5 Inter-agency partnerships	1.89
5.1 Are there inter-agency partnerships/agreements among different governmental bodies in relation to cybersecurity (ex: cooperation between ministries)?	