ITU-D Cybersecurity

Global Cybersecurity Index – GCIv5

Final Questionnaire

Table of Contents

Legal Measures.....2
Technical Measures.....8
Organizational Measures.....14
Capacity Development Measures.....19
Cooperation Measures.....28

Legend

Code-[EDITION NUMBER] – the code for the question/section in the corresponding edition number

Rationale-[EDITION NUMBER] – Any logic or background reasoning given for the question in the corresponding edition

---

Global Cybersecurity Index Indicators by Pillar

Legal Measures

Rationale-GCIv5: Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common regulatory basis, whether on the matter of prohibition of specified criminal conduct or minimum regulatory requirements. Legal frameworks outline the roles, duties, and responsibilities for various stakeholders. Cybersecurity law can be defined as having five fundamental questions: "1) What are we securing?; (2) Where and whom are we securing?; (3) How are we securing?; (4) When are we securing?; and (5) Why are we securing?"[1] Data security is an important part of cybersecurity, but is not the only component, as cybersecurity comprises of the "systems on which data are stored and the networks on which data are transmitted." [2]

Legal measures also allow a country to set down the basic response mechanisms to breach: through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. Laws protect general security and guarantee rights of citizens against abuse by others and ensures the protection against the misuse of the latest technologies. A legislative framework sets the minimum standards of behavior across the board, applicable to all, and on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable countries to have adequate legislation in place in order to

[1] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022
[2] https://heinonline.org/HOL/P?h=hein.journals/ilr103&i=1022

harmonize practices supranationally and offer a setting for interoperable measures, facilitating international combat against cybercrime.

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

1. Cybercrime law

Code-GCIv5: Legal1
Rationale-GCIv5: Cybercrime laws designate unauthorized (without right) access, interference, interception of computers, systems, and data. These laws may take the form of substantive and/or procedural law, public and/or private law, common law, case law, statutory law, administrative law, or other applicable forms of law.

1.1 Laws on unauthorized online behavior

Code-GCIv5: Legal1.1
Rationale-GCIv5: Various online behaviors can negatively impact the safety and confidence of online activities. Some of these behaviors have been noted in international agreements, such as the 2011 Council of Europe Convention on Cybercrime ("Budapest Convention"). Legislation in force regarding such behaviors can provide clear guidelines for law enforcement, provide judicial clarity, and remit to those impacted by those behaviors.

1.1.1. Does your country have legislation in force on illegal access on devices, computer systems, and data?

Code-GCIv5: Legal1.1.1
Rationale-GCIv5: Various online behaviors can negatively impact the safety and confidence of online activities. One way to address such behaviors is through legislation. The intent of this question is to measure if a country, at the time of the GCI Questionnaire, had specific legislation in force which addresses the illegal access on devices, computer systems, and data, which can in turn lead to harms to privacy, property, or personal dignity, among other harms or damage. Planned, draft, and currently not in force legislation are not considered for a full point here.

1.1.2. Does your country have legislation in force on illegal interferences (through data input, alteration, and/or suppression) on devices, data, and computer system?

Code-GCIv5: Legal1.1.2
Rationale-GCIv5: Various online behaviors can negatively impact the safety and confidence of online activities. One way to address such behaviors is through legislation. The intent of this question is to measure if a country, at the time of the GCI Questionnaire, had specific legislation in force which addresses the on illegal interferences (through data input, alteration, and/or suppression) on devices, data, and computer system. Planned, draft, and currently not in force legislation is not considered for a full point here.

1.1.3. Does your country have legislation in force on illegal interception on devices, data, and computer systems?

Code-GCIv5: Legal1.1.3
Rationale-GCIv5: Various online behaviors can negatively impact the safety and confidence of online activities. One way to address such behaviors is through legislation. The intent of this

question is to measure if a country, at the time of the GCI Questionnaire, had specific legislation in force which addresses the on illegal interception on devices, data, and computer systems. Planned, draft, and currently not in force legislation are not considered for a full point here.

1.1.4. Does your country have substantive law on online identity?

***Code-GCIv5**:* Legal1.1.4
Rationale-GCIv5: With an increasing amount of online activity needing people to be able to identify themselves online in reliable and trustworthy ways. Laws, whether specific to online activities, part of other identity-related laws, or other, help provide a legal basis for online identity usage, management, and behaviors.

1.2 Does your country have legislation in force related to computer-related forgery? (piracy/copyright infringements)?

Code-GCIv5: Legal1.2
Rationale-GCIv5: Trust is foundational to the digital ecosystem. Computer-related forgery erodes this trust. Computer-related forgery encompasses "intentional acts and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible''[3]. "This is the case, for example, if a perpetrator modifies an authentic email from a financial institution and sends the modified version to a number of recipients (also referred to as 'phishing'). Some national approaches require that the original computer data relate to documentation intended to create binding legal obligations. Others require only that a perpetrator intends the resultant modified version to be considered as or acted upon with respect to legal obligations."[4]

1.3 Laws on online safety

Code-GCIv5: Legal1.3
Rationale-GCIv5: Given the dampening activity of anti-social behaviors on online activities, making users and communities feel less safe, the regulation of certain behaviors is measured below. The regulation of these behaviors must often carefully balance against human right and other values espoused by the UN Convention on Human Rights, amongst others. Note that the laws do not need to explicitly mention that they apply to online digital/circumstances, but that, within the country, it is accepted by judicial bodies that they are applicable to digital/online circumstances.

1.3.1 Does your country have legislation in force applicable to racist and xenophobic online material?

Code-GCIv5: Legal1.3.1
Rationale-GCIv5: Racist and xenophobic online material carry significant negative effects on online communities including reducing diversity, inflaming divisions, and can cause harm to individuals. Legislation in force that addresses racist and xenophobic should be clear, making it easy for individuals to understand and abide by. Technology-neutral legislation is accepted; the legislation does not need to specify that it applies to online racist and xenophobic material if

[3] https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html
[4] http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime_questionnaires/Member_State_questionnaire.xls

associated legal statements, amicae curae, case law, past prosecutions, or other appropriate materials exist demonstrating the applicability to online circumstances.

1.3.2 Does your country have legislation in force applicable to online harassment and abuse against personal dignity/integrity?

Code-GCIv5: Legal1.3.2

Rationale-GCIv5: Harassment and abuse against personal dignity/integrity can have significant negative effects on people, especially when it takes place online. Legislation in force offers guidance for law enforcement on what cases to act on, for judiciary in how to handle cases, and remit opportunities for those impacted, ultimately contributing to online trust and safety. Technology-neutral legislation is accepted; the legislation does not need to specify that it applies to online harassment and abuse or xenophobic material if associated legal statements, amicae curae, case law, past prosecutions, or other appropriate materials exist demonstrating the applicability to online circumstances.

2 Cybersecurity regulations

Code-GCIv5: Legal2

Rationale-GCIv2: Cybersecurity regulation designates rules dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection (COP), digital signatures and e-transactions, and the liability of internet service providers. Regulations are often the implementing framework for laws, specifying how the laws should be carried out. Countries can improve their commitment to cybersecurity through clear, consistent, applicable, and up-to-date regulations.

2.1 Does your country have regulation(s) related to personal data protection?

Code-GCIv5: Legal2.1

Rationale-GCIv5: Personal data regulation strengthens data management, outlining data holders' responsibilities and individuals' rights. It can give directives for data holders to be held accountable for how they use personal data and ensure that organizations do not abuse collected data.

2.2 Does your country have regulation(s) related to privacy protection?

Code-GCIv5: Legal2.2

Rationale-GCIv5: Privacy protection regulations ensure that personal data is protected, organizations are transparent in how they use data, and individuals have the right to access and correct their personal data. Regulation can prohibit organizations from selling or sharing personal data without the consent of the individual. Privacy protection can ensure that individuals can exercise control over their personal data. Misuse of personal data can contribute to cybercrime and an erosion of trust in digital technologies.

2.3 Does your country have regulation(s) related to data breach/incident notification applying to private sector actors?

Code-GCIv5: Legal2.3

Rationale- GCIv5: A data breach can negatively impact individuals, businesses, and governments, through financial and identity theft, negative reputational impacts, and punitive consequences for data holders. Effective regulation can include data breach notifications, requiring actors to notify individuals, businesses, and governments of data breaches in a timely manner. This would allow individuals, businesses, and governments to take steps to protect themselves from harm that can result from a data breach. Regulations for data breach notification can encourage good practices in data management, require timely notification, and provide recourse to those impacted.

2.4 Does your country have regulation(s) related to cybersecurity audit requirements applying to national government agencies, departments, or their contractors?

Code-GCIv5: Legal2.4

Rationale-GCIv5: Regulations regarding cybersecurity audit requirements can promote the identification of cybersecurity risks and promote better cybersecurity practices by encouraging agencies, departments, and contractors to identify and fix vulnerabilities in their systems. Additionally, regulations can encourage agencies, departments, and contractors to follow best practices for cybersecurity and follow international standards.

2.5 Does your country have regulation(s) related to cybersecurity standards applying to national public sector actors?

Code-GCIv5: Legal2.5

Rationale-GCIv5: Public sector actors are often the target of cyberattacks. As such, it is important that these actors have robust cybersecurity protections in place so that they can protect themselves and their citizens. Having a regulation related to cybersecurity standards applying to national public sector actors can help to ensure that these actors are better protected from cyberattacks, and that they are following best practices when it comes to cybersecurity.

Standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC^2), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), those related to ISO 27001 Information Security Management system standards requirements, ISO 28000 Supply Chain Management Security, ISA 62443 Security for Industrial Automation and Control Systems, among others.

2.6 Does your country have regulation(s) related to use of digital signatures and e-transactions in government services and applications (e-govt)?

Code-GCIv5: Legal2.6

Rationale GCIv5: Governments are increasingly using digital signatures and e-transactions in their services and applications. This shift to electronic systems has a number of benefits,

including increased efficiency and security. However, without appropriate regulation in place, there is a risk that these systems may not be used effectively or securely.
Regulation helps ensure that citizens can trust that their data is secure, and that government systems are efficient and reliable.

2.7 Does your country have regulation(s) related to unsolicited communication, also known as spam?

Code-GCIv5: Legal2.7
Rationale-GCIv5: By regulating unsolicited communication, countries can create a safer and more enjoyable online experience for everyone. These regulations help to protect citizens from the negative effects of spam, and prevent spammers from taking advantage of people.

2.8 Does your country have regulation(s) related to identifying and protecting national critical infrastructures?

Code-GCIv5: Legal2.8
Rationale-GCIv5: By identifying and protecting national critical infrastructures, a country can manage cyber related risks. A regulation for protecting critical national infrastructure helps a country plan how to respond to a major disaster or aggression, ensuring that it can respond quickly and effectively to a major disaster or attack. A country also needs to have a plan to recover from a major disaster or attack.

2.9 Does your country have regulation(s) related to Child Online Protection?

Code-GCIv5: Legal2.9
Rationale-GCIv5: Addressing Child Online Protection through relevant regulations enables relevant agencies and actors take action and implement specific requirements and rules to deal with and combat online / cyber-crimes against children and young people. It is fundamental that such rules are implemented by the wide range of stakeholders across all sectors and layers of society – from industry operators to law enforcement and civil society stakeholders – that should act collectively to support the achievement of a secure and safe digital environment for children and young people.

Technical Measures

Rationale-GCIv5: Technology is the first line of defense against cyberthreats and malicious online agents. Without adequate technical measures and capabilities to detect and respond to cyberattacks, countries 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. Countries 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.

Technical measures can be measured based on the existence and number of technical institutions and frameworks dealing with cybersecurity endorsed or created by a country. The pillar is composed of the following performance indicators:

1. National CERT/CIRT/CSIRT or SOC

Code-GCIv5: Tech1

Rationale-GCIv5: Effective mechanisms and institutional structures at the national level are necessary to detect, prevent, respond to, and mitigate cyber threats and incidents. Computer Incident Response Teams (CIRTs), as well as Computer Security Incident Response Teams (CSIRTS) and Computer Emergency Response Teams (CERTs) and Security Operations Centers (SOC)[5]are responsible for the protection against, detection of, and response to cybersecurity incidents, and can enhance a country's ability to manage cybersecurity incidents. CIRTs or SOCs can serve to build knowledge base that supports the country's implementation of a national cybersecurity strategy, as well as an approach for the protection of critical information infrastructures; supporting the building of a national culture and ecosystem of cybersecurity, and related awareness raising initiatives; supporting the development of related national cybersecurity platforms, such as e-government services, national identity and access management frameworks; and further enabling the country to develop and enhance its incident response and coordination capabilities.

1.1 Does your country have a fully operational National/Government CIRT/CSIRT/CERT or SOC?

Code-GCIv5: Tech1.1

Rationale-GCIv5: Computer Incident Response Teams (CIRTs), as well as Computer Security Incident Response Teams (CSIRTs),Computer Emergency Response Teams (CERTs) and Security Operation Centers (SOCs) are responsible for the protection against, detection of, and response to cybersecurity incidents. A CIRT/CSIRT/CERT and SOC are considered fully operational, as follows:

- Defined and approved organisational structure
- Staffed with trained and qualified personnel

[5] https://ieeexplore.ieee.org/document/9296846

- Implemented secure facilities (appropriate measures are implemented to protect facilities against physical and environmental threats)
- Developed and implemented detailed processes and procedures for its operations
- Adoption and implementation of the required technology for its operations
- Implemented processed for interactions with key stakeholders and partners
- Effective and efficient delivery of services to its Constituency.

Initial processes to implementing a CIRT may involve assessment (measuring the readiness for the establishments of the CIRT, as well as preparing relevant stakeholders of the needed involvement), design (preparing the detail design document for the CIRT), and the process of establishment (implementing infrastructure, establishing relationships with stakeholders, constituency, establishing mandate processes, services, launching operations, and applying to international association membership).

1.2 National CIRT/CSIRT/CERT or SOC activities

Code-GCIv5: Tech1.2

Rationale-GCIv5: A National Computer Incident Response Teams (CIRTs), as well as Computer Security Incident Response Teams (CSIRTs), Computer Emergency Response Teams (CERTs) and Security Operation Centers (SOCs)are responsible for the protection against, detection of, and response to cybersecurity incidents. It is a central point for cybersecurity incident reporting. It also provides information and technical assistance to help organizations prevent, mitigate, and respond to cyber incidents. In addition, a National CIRT or SOC conducts research on cybersecurity issues and develops best practices and guidelines for responding to cyber incidents.

1.2.1 Does your National/Government CIRT/CSIRT/CERT or SOC develop and execute cybersecurity awareness activities?

Code-GCIv5: Tech1.2.1

Rationale-GCIv5: National CIRTs or SOCs can play an important role of executing cybersecurity awareness campaigns; in their role as central coordinating bodies,they might acquire increasing visibility on current and emerging cyber threats, cybersecurity challenges, vulnerabilities, insights on cybersecurity major trends, technological advancements in cybersecurity and best practices to detect and respond to cyber threats. To enhance cybersecurity culture and and promote knowledge on cybersecurity measures, good practices and behaviors, CIRT/CSIRT/CERT or SOC should design, execute and / or coordinate cybersecurity awareness initiatives and activities tailored to various stakeholders which are based on information gathered on the evolving threat landscape, cybersecurity major trends and best practices.

1.2.2 Does your National/Government CIRT/CSIRT/CERT or SOC conduct regular cybersecurity exercises (CyberDrills)?

Code-GCIv5: Tech1.2.2

Rationale-GCIv5: Cybersecurity exercises are planned events 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. Cybersecurity exercises held on a regular basis, in association with relevant stakeholders are a proactive measure to enhance cybersecurity readiness and resilience. CIRT/CSIRT/CERT or SOC should periodically develop and conduct cyber incident / crisis management exercises, involving also any relevant public or private entities across the country, to test their incident response capabilities.

1.2.3 Does your National/Government CIRT/CSIRT/CERT or SOC provide publicly available cybersecurity advisories?

Code-GCIv5: Tech1.2.3
Rationale-GCIv5: Publicly available cybersecurity advisories ensures that agencies and departments are made aware of potential cybersecurity threats and can take precautions. Additionally, advisories can help promote coordinated responses to cybersecurity threats.

1.3 Is the National/Government CIRT/CSIRT/CERT or SOC affiliated with FIRST and/or listed by TF-CSIRT?

Code-GCIv5: Tech1.3
Rationale-GCIv5: National CIRTs or SOC affiliated with FIRST have the benefit of a global network of CIRTs, training and resources, expertise from FIRST staff, and opportunities to collaborate and share best practices. FIRST's eligibility criteria require active commitment by countries. TF-CSIRT listed status will be considered for this question.

1.4 Is the above National/Government CIRT/CSIRT/CERT or SOC affiliated with a regional CIRT (such as APCERT, PACSON, AFRICA CERT, ENSIA, OIC, OAS)?

Code-GCIv5: Tech1.4
Rationale-GCIv5: Affiliation with a regional CIRT encompasses any formal or regular relation with any other regional CIRT group. There are many advantages to being affiliated with a regional CIRT or CERT, including exchange of knowledge and experience. Regional CIRTs and CERTs are often able to share relevant knowledge and experience relevant to a country's circumstances.

2. Sectoral CERT/CIRT/CSIRT or SOCs

Code-GCIv5: Tech2
Rationale-GCIv5: A sectoral CERT/CIRT/CSIRT or SOC serves constituents that work in a specific sector, such as the financial sector, academia, energy, health, telecommunication, public utilities, critical infrastructure, among others. A sectoral CIRT or SOC serves its constituents through tailored, specialized threat intelligence and services. Countries may have joint sectoral CIRTs or SOCs with other countries, in that the sectoral CIRT or SOC serves constituencies from a specific sector across multiple countries. For the purposes of this indicator, military CIRTs are not accepted.

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

Code-GCIv5: Tech2.1
Rationale-GCIv5: A sectoral CERT/CIRT/CSIRT or SOC serves constituents that work in a specific sector, such as the financial sector, academia, energy, health, telecommunication, public utilities, critical infrastructure, among others. A sectoral CIRT or SOC serves its constituents through tailored, specialized threat intelligence and services. Countries may have joint sectoral CIRTs or SOCs with other countries, in that the sectoral CIRT serves constituencies from a specific sector across multiple countries. For the purposes of this indicator, military CIRTs are not accepted. A sectoral CIRT/CSIRT/CERT or SOC are considered fully operational, as follows:

- Defined and approved organisational structure
- Staffed with trained and qualified personnel

- Implemented secure facilities (appropriate measures are implemented to protect facilities against physical and environmental threats)
- Developed and implemented detailed processes and procedures for its operations
- Adoption and implementation of the required technology for its operations
- Implemented processed for interactions with key stakeholders and partners
- Effective and efficient delivery of services to its Constituency.

Partially implemented sectoral CIRTs may involve assessment (measuring the readiness for the establishments of the sectoral CIRT, as well as preparing relevant stakeholders of the needed involvement), design (preparing the detail design document for the CIRT), and the process of establishment (implementing infrastructure, establishing relationships with stakeholders, constituency, establishing mandate processes, services, launching operations, and applying to international association membership).

2.2 Sectoral CIRTs/CSIRTs/CERTs or SOC Activities

Code-GCIv5: Tech2.2

Rationale-GCIv5: A Sectoral Computer Incident Response Teams (CIRTs), or Sectoral Computer Security Incident Response Teams (CSIRTS), Sectoral Computer Emergency Response Teams (CERTs) or Sectoral Security Operation Centers (SOCs) are responsible for the protection against, detection of, and response to cybersecurity incidents.

The sectoral CIRT or SOC is a central point for cybersecurity incident reporting within the sector. It also provides information and technical assistance to help organizations within the sector prevent, mitigate, and respond to cyber incidents. In addition, a sectoral CIRT or SOC conducts research on cybersecurity issues and develops best practices and guidelines for responding to cyber incidents.

2.2.1 Does the sectoral CIRT/s, CSIRT/s or CERT/s or SOCs develop and execute cybersecurity awareness activities for the sector?

Code-GCIv5: Tech2.2.1

Rationale-GCIv5: Sectoral CIRTs or SOCs can play an important role of executing cybersecurity awareness campaigns for a specific sector. In their role as central coordinating bodies for the sector, they have insights into cybersecurity trends relevant to their stakeholders. Based on sector specific and general threat intelligence, sectoral CIRTs can help develop and execute awareness activities to various sector related stakeholder groups to improve cybersecure behaviors.

2.2.2 Does the sectoral CIRT/s, CSIRT/s or CERT/s or SOCs regularly participate in national cybersecurity exercises (CyberDrills)?

Code-GCIv5: Tech2.2.2

Rationale-GCIv5: Cybersecurity exercises are planned events 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. The participation in national cybersecurity exercises by sectoral CIRTs are a proactive measure to enhance overall cybersecurity capabilities.

2.2.3 Does the sectoral CIRT/s, CSIRT/s or CERT/s or SOCs share sectoral related incidents within its constituency?

Code-GCIv5: Tech2.2.3

Rationale-GCIv5: Sharing sectoral relevant threat intelligences can enable sector stakeholders become more aware of relevant threats and vulnerabilities, and improve incident response times and effectiveness. Additionally, this can help create a more coordinated response to cybersecurity incidents across the government, the private sector, and the general public.

3. National framework for implementation of cybersecurity standards

Code-GCIv5: Tech3

Rationale GCIv5: National frameworks for the implementation of cybersecurity standards encompass 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), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), those related to ISO 27001 Information Security Management system standards requirements, ISO 28000 Supply Chain Management Security, ISA 62443 Security for Industrial Automation and Control Systems, among others.

3.1 Does your government have a framework for the implementation/adoption of nationally or internationally recognized cybersecurity standards?

Code-GCIv5: Tech3.1

Rationale-GCIv5: National frameworks for the implementation of cybersecurity standards encompass the existence of a government approved (or endorsed) framework (or frameworks)for the implementation/adoption of nationally or internationally recognized cybersecurity standards. A framework could define a plan or roadmap for the implementation/adoption of standards, stakeholders will be involved, processes will be used for future updates, and other methods guide the implementation.
Standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), those related to ISO 27001 Information Security Management system standards requirements, ISO 28000 Supply Chain Management Security, ISA 62443 Security for Industrial Automation and Control Systems, among others.

3.2 Does the framework for implementation/adoption of nationally or internationally recognized cybersecurity standards address critical infrastructure?

Code-GCIv5: Tech3.2

Rationale-GCIv5: Addressing critical infrastructure as part of any framework for the implementation/adoption of nationally or internationally recognized cybersecurity standards is fundamental to enhance the protection and resilience of Critical Infrastructure and help them in reducing vulnerabilities and effectively managing cybersecurity risks.

Organizational Measures

Rationale-GCIv5: Organizational measures are necessary for the proper implementation of the national cybersecurity posture. Strategic objectives need to be set by the government, with a comprehensive plan in implementation, delivery, and measurement. Governance structures need to be established and enabled to put the cybersecurity posture into effect, monitor the implementation and evaluate the outcomes. Without a well-defined organizational network of partners, working together across industry, civil society and academia efforts in different sectors and industries become disparate and unconnected, thwarting efforts to reach national harmonization in terms of cybersecurity capability development.

The organizational structures can be measured based on the existence and number of institutions and strategies organizing cybersecurity development at the national level. The creation of effective organizational structure is necessary for promoting cybersecurity development, combating cybercrime and promoting the role of watch, warning and incident response to ensure intra-agency, cross-sector and cross-border coordination between new and existing initiatives. The pillar is composed of the following performance indicators:

1. National Cybersecurity Strategy

Code-GCIv5: Org1

Rationale-GCIv5: A National Cybersecurity Strategy provides a framework for allocating resources[6] to identify the national cybersecurity objectives and prioritize the resources for their implementation with the aim to improve security and resilience of a country[7]. It also enables the government to cooperate with all the relevant stakeholders at the national level. Additionally, a National Cybersecurity Strategy might help promote innovation and protect privacy and civil liberties. The Strategy should clearly identify the national cybersecurity objectives and identify the governance structure for their implementation.[8]

1.1 Does your country have a National Cybersecurity Strategy (NCS) or policy, whether stand-alone or part of another document?

Code-GCIv5: Org1.1

Rationale-GCIv5: There is no doubt that cybersecurity is a critical issue for all nations. A National Cybersecurity Strategy provides a framework for allocating resources to protect a nation's critical infrastructure. It also enables governments to work with the private sector to identify and mitigate cyber threats. Additionally, a National Cybersecurity Strategy can help promote innovation and protect privacy and civil liberties.

1.2 National Cybersecurity Strategy Priorities

Code-GCIv5: Org1.2

Rationale-GCIv5: A national strategy with priorities enables a coordinated response to cyber risks. As every country faces different cybersecurity challenges, focusing on specific area of cybersecurity help countries prioritize resources and coordinate a response to cyber threats**.** Most guides to developing a National Cybersecurity Strategy may focus on different priorities

[6] https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained
[7] https://www.enisa.europa.eu/topics/national-cyber-security-strategies
[8] https://ncsguide.org/the-guide/

such as "Developing a National Cybersecurity Strategy."[9] Priority areas may also refer to "Focus Areas" for some strategies[10] Questions 1.2.1. to 1.2.4 include priority areas that could be addressed within a country's National Cybersecurity Strategy. However, countries may have other priority areas.

1.2.1 Does your country's NCS address the protection of national critical infrastructures?

Code-GCIv5: Org1.2.1

Rationale-GCIv5: National critical infrastructure includes everything from the electrical grid and water systems to transportation networks and financial institutions. If any of these were to break down, a country would be in chaos. That's why it's so important that a National Cybersecurity strategy should have a plan to ensure they are well-protected as critical infrastructure is essential for maintaining public order and safety, important for a country's economy and it's crucial for national security.

1.2.2 Does your country's NCS incorporate life cycle management principles, with monitoring, evaluation, and updates on a regular basis?

Code-GCIv5: Org1.2.2

Rationale-GCIv5: A country's National Cyber Security Strategy (NCS) should incorporate life cycle management principles,[11] with monitoring, evaluation, and updates on a regular basis to ensure that the strategy remains effective and relevant. This helps to ensure that the risks associated with a particular strategy are identified and addressed, and that the strategy is adapted as necessary to reflect changes in the environment. The life cycle management approach also helps to ensure that all stakeholders are engaged in the development and implementation of the strategy, and that everyone has a clear understanding of their role and responsibilities. This helps to ensure that the strategy is implemented effectively and that everyone is working towards the same goal. Finally, by using life cycle management principles, it is possible to monitor the implementation of the strategy and evaluate its outcomes. This allows for timely course corrections where necessary, and helps to ensure that the strategy remains relevant and effective over time.

1.2.3 Does your country's NCS have a mechanism to ensure regular consultation with cybersecurity experts and stakeholders?

Code-GCIv5: Org1.2.3

Rationale-GCIv5: The cybersecurity landscape is constantly changing, and it is important to have a mechanism in place to ensure that the NCS is updated regularly. Cybersecurity experts can provide valuable input on the latest threats and how best to counter them. Stakeholders such as businesses and citizens also need to be consulted during the NCS process to ensure more effective policy outcomes. They can provide feedback on how the strategy is working and offer suggestions for improvements. By consulting with experts and stakeholders, the NCS can be tailored to meet the needs of the country.

1.2.4 Does your country have a defined action plan/roadmap for the implementation of its cybersecurity strategy?

Code-GCIv5: Org1.2.4

---

[9] http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf

[10] https://ncsguide.org/the-guide/

[11] https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

Rationale-GCIv5: A defined action plan or roadmap for the implementation of a cybersecurity strategy is a critical part of protecting a nation's digital infrastructure and citizens. Without a plan, it's difficult to allocate resources and measure progress, which can lead to a lack of effectiveness and gaps in coverage. A well-defined action plan/roadmap can help to ensure that all stakeholders are aware of their roles and responsibilities in implementing the strategy, and that the plan is achievable and realistic. It can also help to track and assess the impact of the strategy over time, so that any necessary adjustments can be made.

2. Responsible agency

Code-GCIv5: Org2

Rationale-GCIv5: A responsible agency is a competent authority with the responsibility for managing cybersecurity. This authority should be a leader (whether an individual or an entity) who is elevated and strongly anchored at the highest level of government to provide direction, to coordinate action, and to monitor the implementation of cybersecurity activities and programmes. A national competent authority should also act as management entity to define and clarify roles, responsibilities, processes, decision rights, and the tasks required to ensure effective cybersecurity posture.

2.1 In your country, is there an agency or ministry with the responsibility for cybersecurity at the national level?

Code-GCIv5: Org2.1

Rationale-GCIv5: A national agency or ministry with the responsibility for cybersecurity at the national level can support cohesive cybersecurity threat management and proactive cybersecurity actions This agency or ministry should work with other government departments, the private sector, civil society, and other relevant actors to develop and implement a national cybersecurity strategy."

2.2 In your country, is there an agency or ministry with the responsibility for cybersecurity related to National Critical Infrastructure Protection?

Code-GCIv5: Org2.2

Rationale-GCIv5: An agency or ministry with the responsibility for critical infrastructure at the national level supports resiliency and continuation of operations. Critical infrastructure can include essential services like water, electricity, and telecommunications, which, are essential for the functioning of a society. A national agency or ministry responsible for critical infrastructure can help prevent or mitigate these disruptions by working with relevant stakeholders***.***

2.3 In your country, is there an agency, ministry, task force, or other body with the responsibility for overseeing national cybersecurity capacity development?

Code-GCIv5: Org2.3

Rationale-GCIv5: A coordinated and comprehensive approach to developing necessary cybersecurity skills and capabilities can reduce the likelihood of cybersecurity incidents and improve resilience. Cybersecurity is a multidimensional concern that requires the coordination and cooperation of multiple government agencies and private sector entities.

2.4 In your country, is coordination of Child Online Protection initiatives and activities within the responsibility of any agency, ministry, task force, or other body?

Code-GCIv5: Org2.4

Rationale-GCIv5: Coordination between stakeholders and target groups, and ensure overseeing of activities, is important to ensure mutually complementary Child Online Protection (COP) interventions. The responsibility for coordinating COP initiatives and activities at the national level can be the role of either a stand-alone agency, ministry, task force, or other body, or as part of a larger set of responsibilities by any such body.

3. Cybersecurity metrics

Code-GCIv5: Org3

Rationale-GCIv5: Cybersecurity metrics include 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, ISO/IEC 27004[12] is concerned with measurements relating to information security management.

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

Code-GCIv5: Org3.1

Rationale-GCIv5: Performing cybersecurity audits at the national level may be done due to security concerns, regulations, or other guiding documents. While cybersecurity audit regulations, effective national level cybersecurity audits are needed. Audit reports, summaries, presentations, memos, or other similar materials may be the output of these audits. Cybersecurity audit is the identification of potential vulnerabilities. Once these have been identified, they can be assessed and prioritized in order to determine the level of risk that they pose to the organization. There are a variety of tools that can be used to assess these vulnerabilities, including vulnerability scanners, penetration testers, and red teaming exercises. Each of these tools has its own strengths and weaknesses, and it is important to select the right tool for the job. Once the vulnerabilities have been identified, it is important to determine the level of risk that they pose to the organization.

3.2 Are there metrics/tools for assessing cybersecurity risks at a national level?

Code-GCIv5: Org3.2

Rationale-GCIv5: Metrics for assessing cybersecurity risks at the national level will vary between countries, and should reflect a country's specific threats, capabilities, and challenges**.** This can be done using a variety of metrics, including impact factors, probability factors, and asset values. By using these metrics, it is possible to determine the level and severity of risk that each vulnerability poses and take appropriate corrective action.[13] ISO/IEC 27004[14] offers security techniques that be used to monitor, measure, analyze and evaluate cybersecurity related risks.

[12] https://www.iso.org/standard/64120.html
[13] https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf
[14] https://www.iso.org/standard/64120.html

3.3 Are there measures for assessing the level of cybersecurity development at a national level using tools such as the Cybersecurity Capacity Maturity Model, Cyber Readiness, or any other relevant assessment tools?

Code-GCIv5: Org3.3

Rationale-GCIv5: Assessing the level of cybersecurity development can enable countries to understand the maturity and reliability of their cybersecurity infrastructure, and the specific assessment measures may vary between countries. Some commonly used tools to assess the level of cybersecurity development at the national level include the Cybersecurity Maturity Model[15], Cyber Readiness[16] or any other measure taken by a country. Assessment tools in this question exclude country participation in the ITU Global Cybersecurity Index.

4. Child Online Protection strategies and initiatives

Code-GCIv5: Org4

Rationale-GCIv5: Child online protection (COP) is the umbrella term for strategies and initiatives designed to protect children from harm or exploitation when accessing the internet. This can include ensuring children are using age-appropriate software and filtering tools, to educating parents and children about staying safe online. There are a variety of different COP strategies and initiatives in place, usually tailored to meet the specific needs of children in the target country.

4.1 Does your country have a national strategy addressing Child Online Protection, with associated current Child Online Protection initiatives?

Code-GCIv5: Org4.1

Rationale-GCIv5: In the COP Guidelines, it is recommended to have a dedicated, separate holistic strategy on COP, as it should cover areas related to children of health, wellness, skills development. When a COP strategy is integrated elsewhere, it is often not holistic, and often focuses on only sexual abuse or child pornography.

4.2 Within your country, are there any government reporting mechanisms and capabilities at the national level deployed to help protect children online?

Code-GCIv5: Org4.2

Reasoning GCIv5: Reporting mechanisms available to the general public for the identification, tracking, and follow-up of issues associated with children online empowers individuals to identify and report issues impacting children online. These mechanisms can also encompass technical capabilities such as content warning. CIRTs and law enforcement agencies may offer reporting mechanisms. Ideally, a variety of systems, such as national helplines or online portals with referral and support systems, should be available.

[15] https://gcscc.ox.ac.uk/cmm-2021-edition

[16] https://www.potomacinstitute.org/images/CRIndex2.0.pdf

Capacity Development Measures

Rationale-GCIv5: Capacity development is intrinsic to legal, technical, and organizational measures within the Global Cybersecurity Index and a driving force for digital development. Capacity development programs aim to build local skills, knowledge, and confidence, in turn closing the skills gap and building a more inclusive technology ecosystem. Further, the ability to deliver inclusive digital services is increasingly reliant on a skilled workforce. Capacity development frameworks for promoting cybersecurity may include awareness-raising, and can be measured based on the existence and number of research and development programs, education and training programs, and certified professionals and public sector agencies.

1. Public cybersecurity awareness campaigns

Code-GCIv5: CapDev1

***Rationale-GCIv5*:** Public cybersecurity-awareness campaigns primarily aim to influence the adoption of secure behaviour online. To achieve meaningful behaviour change, public awareness campaigns need to convince people that the information is relevant, help them understand how to respond, and persuade them to be willing to respond in light of other priorities.[17] Awareness campaigns face numerous challenges, especially due to the "demand of a lot of effort and skills" and that "fear invocations have often provided insufficient to change behaviour."[18] Targeted awareness campaigns can tailor interventions to better address these concerns.

1.1 Does your government have public awareness campaigns specifically targeting MSMEs?

Code-GCIv5: CapDev1.1

***Rationale-GCIv5*:** Micro, Small and medium businesses (SMEs) are a vital part of a country's economy and need to be aware of the cybersecurity threats that could impact their business. They face specific challenges in terms of improving cybersecurity, such as lack of resources and technical expertise. Targeted interventions can address these specific challenges and focus on maximizing impact for MSMEs. Cybersecurity awareness campaign specifically for SMEs can provide MSMEs with information on how to protect themselves from cyberattacks, as well as how to respond if they are attacked.

1.2 Does your government have public awareness campaigns specifically targeting the private sector in general?

Code-GCIv5: CapDev1.2

***Rationale-GCIv5*:** Any private sector actor faces cybersecurity challenges. Beyond the specific needs of MSMEs, public awareness campaigns on the cybersecurity risks faced by the private sector can help improve behavior.

---

[17] Rogers, R.W. Attitude change and information integration in fear appeals. Psychological Reports, 56, (1985) 183–188
Witte, K. Message and conceptual confounds in fear appeals: The role of threat, fear and efficacy. The Southern Communication Journal, 58(2), (1993) 147-155.
https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

[18] https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

1.3 Does your government have public awareness campaigns specifically targeting public sector agencies at local, municipal, and national levels, and public sector workers?

Code-GCIv5: CapDev1.3

***Rationale-GCIv5*:** Public sector agencies can benefit from cybersecurity awareness campaigns. Cybersecurity awareness campaigns are specifically designed to reach public sector workers, and they provide important information about how to protect sensitive data and critical infrastructure.

1.4 Does your government have public awareness campaigns specifically targeting civil society?

Code-GCIv5: CapDev1.4

***Rationale-GCIv5*:** Civil society organizations can be targets of cyberattacks. These attacks can include online harassment, data theft, or financial information. Civil society organizations need to be aware of the risks and protect themselves. This includes training their staff, using secure passwords, and having up to date antivirus software. Countries can help protect these vital organizations from harm through awareness to help them safely defend their organizations, networks and citizens' data.

1.5 Does your government have public awareness campaigns targeting the population in general?

Code-GCIv5: CapDev1.5

Rationale-GCIv5: Cybersecurity is not just for businesses and governments. Citizens are the most vulnerable to cybercrime, yet they often lack the knowledge and tools to protect themselves. Cybercriminals constantly look for new ways to steal data, money, or identities. They can do this by hacking into computer systems, stealing passwords, or creating fake websites. At the national level, governments can raise awareness to protect citizens. Educate Citizens to protect themselves by using strong passwords, being careful when opening emails, and never giving out personal information online. They should also be aware of the warning signs of a scam or phishing attack. Governments should be committed to cybersecurity awareness for all citizens and urge everyone to take the necessary steps to protect themselves online.

1.6 Does your government have public awareness campaigns specifically targeting older persons (elderly)?

Code-GCIv5: CapDev1.6

Rationale-GCIv5: As our population continues to age, more and more seniors are going to be using the internet and electronic devices. Unfortunately, this makes them a prime target for cybercriminals. Seniors are more vulnerable to cyber threats for several reasons: They may not be as aware of the dangers that come with using the internet, lack technical skills to protect themselves, may be more likely to fall for scams, less likely to report a cybercrime.
For this reason, governments are developing cybersecurity awareness for the elderly population to stay safe online and protect their personal information.

1.7 Does your government have public awareness campaigns specifically targeting persons with specific needs including persons with disabilities?

Code-GCIv5: CapDev1.7

Rationale-GCIv5: With increasing shift from a medical to a human rights model of disability, addressing the societal barriers faced by those with special needs, such as "architectural and communicative barriers, attitudes and structures of society,"[19] can enhance the capability and safety of persons with disability. There is also a heightened need for cybersecurity awareness and training that specifically targets persons with disabilities. Persons with disabilities are more vulnerable to cyber-attacks for a number of reasons, including their lack of familiarity with technology, dependence on others for help, and reluctance to ask for help. Therefore, education and awareness are essential, and governments need to ensure that all community members are included in our cybersecurity efforts. Addressing the needs to this population in terms of public awareness campaigns is important for inclusive and effective cybersecurity capacity development.

1.8 Does your government have any public awareness campaigns specifically targeting parents, educators, and children as part of Child Online Protection (COP) efforts?

Code-GCIv5: CapDev1.8

Rationale-GCIv5: Government should promote the development of public awareness campaigns specifically targeting parents and educators to enable them to gain more knowledge about the risks and harms to which children and young people are exposed and increase capabilities to deal with COP related issues.

1.9 Does your government have any public awareness campaigns specifically targeting children as part of Child Online Protection (COP) efforts?

Code-GCIv5: CapDev1.9

Rationale-GCIv5: With increased time spent online, children are vulnerable. Children are particularly vulnerable to cyber threats, as they may not be as aware of the dangers and may not have the same level of cybersecurity knowledge and experience as adults. Governments should promote the development of public awareness campaigns targeting children to help them acquiring knowledge on the various online risks they may encounter, to enhance their capabilities to identify and mitigate those risks and promote the adoption of online responsible behaviors.

2. Training for cybersecurity professionals

Code-GCIv5: CapDev2

Rationale-GCIv5: Skills development can support the development of a capable and up-to-date cybersecurity workforce. The training of the cybersecurity workforce necessitates ongoing efforts to address changes and developments in the field.

2.1 Does your government develop or support cybersecurity training courses for cybersecurity professionals?

Code-GCIv5: CapDev2.1

[19] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e777?rskey=sn89T4&result=201&prd=MPIL#

Rationale-GCIv5*:* As more and more businesses move their operations online, the need for cybersecurity professionals has never been greater. But too often, these professionals lack the necessary training to protect their employers from cyberattacks. Cybersecurity training is important for several reasons including helping cybersecurity professionals build a strong foundation in cybersecurity, capabilities on how to apply their knowledge practically, staying up to date with the latest cybersecurity trends and developments, and helping them develop the necessary skills to secure their organizations' networks and data.

2.2 Within your country, are there domestically or internationally recognized accreditation programs for cybersecurity professionals?

Code-GCIv5: CapDev2.2

Rationale-GCIv5: Cybersecurity accreditation programs help ensure that the professionals working in this field are held to a high standard. This can help improve the overall quality of cybersecurity professionals and help to protect individuals and organizations from potential harm. In addition, countries can build trust among cybersecurity professionals and their clients. Having a universally recognized accreditation program can help ensure that all parties involved can trust the qualifications of the professionals they are working with.

2.3 National sector-specific cybersecurity educational programs/trainings for professionals

Code-GCIv5: CapDev2.3

Rationale-GCIv5: Within a country, professionals working in various sectors can benefit from cybersecurity programs/trainings which address the specific concerns and situations faced by those professionals, and work to equip them with the appropriate skills needed.

2.3.1 Does your government develop or support cybersecurity educational programs or trainings for law enforcement at the national level?

Code-GCIv5: CapDev2.3.1

Rationale-GCIv5: Law enforcement such as police officers, enforcement agents plays a critical role in helping to protect our country from cyberattacks. They can help identify and investigate cybercrime and work with businesses and other organizations to improve their cybersecurity posture. Law enforcement needs to be equipped with the knowledge and tools necessary to respond to these growing threats. Cybersecurity training can help them understand the latest threats better, identify malicious activity, and protect their networks.

2.3.2 Does your government develop or support cybersecurity educational programs or trainings for national judicial actors at the national level?

Code-GCIv5: CapDev2.3.2

Rationale-GCIv5: National judicial actors play a critical role in ensuring the safety and security of their countries, and they need to be equipped with the knowledge and tools to deal with cybersecurity threats**.** Cybersecurity training for judicial and other legal actors, professional and technical training that can be recurring for judges, solicitors, barristers, attorneys, lawyers, paralegals, and other persons of the legal and law enforcement profession needs to be considered when planning national cybersecurity trainings.

2.3.3 Does your government develop or support cybersecurity educational programs or trainings for MSMEs? [NOT SCORED]

Code-GCIv5: CapDev2.3.3
Rationale-GCIv5: MSMEs need cybersecurity trainings because they hold a large amount of sensitive data, which can be stolen or compromised in the event of a cyberattack. In addition, MSMEs are often not aware of the risks associated with using technology and may not have the necessary tools or resources to protect their data. Cybersecurity training can help MSMEs understand the risks associated with using technology and how to protect their data. In addition, training can help MSMEs identify suspicious activity and respond to cyberattacks. By providing MSMEs with the tools and knowledge they need to protect their data, countries in turn help protect its economic development.

2.3.4 Does your government develop or support cybersecurity educational programs or trainings for the private sector in general?

Code-GCIv5: CapDev2.3.4
Rationale-GCIv5: The private sector increasingly faces growing scope, scale, and complexity of cyber risks which impact corporations' finances, reputation, and property. As technology is only one component of cybersecurity, implementing policies and programs to change people's behavior in the private sector can improve resilience and reduce cyber risks.

2.3.5 Does your government develop or support cybersecurity educational programs or trainings for public sector/government officials in general?

Code-GCIv5: CapDev2.3.5
Rationale-GCIv5: The public sector provides essential services to citizens and businesses. To deliver services securely, public sector actors need a strong understanding of cybersecurity and how to protect themselves and their constituents from digital threats. Public sector/government officials working outside of the judiciary and law enforcement can benefit from cybersecurity educational programs and trainings.

2.3.6 Does your government develop or support cybersecurity educational programs or trainings for financial, health, telecommunication, transport, and/or energy sector actors?

Code-GCIv5: CapDev2.3.6
Rationale-GCIv5: Cybersecurity concerns often vary by sector. Given the critical roles of the financial, health, telecommunications, transport, and energy sector, targeted trainings for these actors can support a country's overall cybersecurity posture.

2.3.7 Does your government develop or support cybersecurity educational programs or trainings for youth?

Code-GCIv5: CapDev2.3.8
Rationale-GCIv5: Governments traditionally step in to correct negative market externalities, and to support groups which otherwise be underserved. Government development and support of cybersecurity educational programs and trainings is such an area where the private sector may lack strong returns to incentivize participation. The government can provide support through financial grants, studies support, apprenticeship support, among other options. Young people looking at a career in cybersecurity may be at higher need for this support as they lack financial capital to invest in education on their own.

2.3.8 Does your government develop or support cybersecurity educational programs or trainings for educators, such as Child Online Protection educational programs?

Code-GCIv5: CapDev2.3.9

Rationale-GCIv5: Educators are in a position to impart positive cybersecurity behaviors in children and young people due to their role children and young peoples' education. Providing training for educators on issues related to cybersecurity, such as Child Online Protection, demonstrates that countries are working towards long term cybersecurity measures, by supporting educators working with the next generation of internet users as they come online.

3. Cybersecurity educational programs as part of national academic curricula

Code-GCIv5: CapDev3

Rationale-GCIv5: To establish a more cybersecurity-capable population, integrating principles essential to cybersecurity into national academic curricula can equip students of all ages to better address cybersecurity risks.

3.1 Does your government develop or support any cybersecurity educational programs included as part of academic curricula in primary education?

Code-GCIv5: CapDev3.1

Rationale-GCIv5: Primary school children, or those at ISCED 1, are beginning their schooling and are typically learning fundamental skills in reading, writing, and mathematics.[20] Integrating activities at this stage to build a foundation in cybersecure behaviour can help promote lifelong cyber awareness and security. However, children at this level may not yet have the critical thinking skills and agency to be able to independently assess cybersecurity risks, and thus have particular risks.[21] Activities at this level could include Child Online Protection activities.

3.2 Does your government develop or support any cybersecurity educational programs included as part of academic curricula in secondary education?

Code-GCIv5: CapDev3.2

Rationale-GCIv5: Students in secondary education, in schooling programmes at ISCED level 2 and 3, are often engaged in educational activities which aim "lay the foundation for lifelong learning and human development upon which education systems may then expand further educational opportunities," and then "designed to complete secondary education in preparation for tertiary education or provide skills relevant to employment, or both."[22] Introducing cybersecurity at this stage can not only help prepare students with skills to be safer online, but also promote an interest that can lead to a career in technology and cybersecurity.

3.3 Does your government develop or support any cybersecurity educational programs included as part of academic curricula in higher education?

Code-GCIv5: CapDev3.3

Rationale-GCIv5: Students in tertiary education, also known as ICSED 5-8, have often completed compulsory education courses. Programmes in tertiary education can include courses to:

[20] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

[21] https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/

[22] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

provide participants with professional knowledge, skills and competencies (ICSED 5); provide participants with intermediate academic and/or professional knowledge, skills and competencies, leading to a first degree or equivalent qualification (ICSED 6); provide participants with advanced academic and/or professional knowledge, skills and competencies, leading to a second degree or equivalent qualification, such as a Master's or equivalent level (ICSED 7); or, to lead to an advanced research qualification, such as a doctoral level qualification (ICSED 8).[23] Addressing cybersecurity at these educational level can support a cyberaware and capable workforce, as well as promote capacity development for the purposes of research and development.

4. Cybersecurity Research and Development (R&D) programs

Code-GCIv5: CapDev4

Rationale-GCIv5: Research and development in the public, private, and academic sectors, can support cybersecurity efforts through the development of human capacity, development of new techniques and products, and better understanding of risks and mitigations. Research and development can encompass both technical and non-technical solutions.

4.1 Do private sector actors within your country carry out cybersecurity-related R&D activities?

Code-GCIv5: CapDev4.1

Rationale-GCIv5: Private sector-led research and development demonstrates private sector willingness to both invest in further growth and innovation within cybersecurity and improve cybersecurity solutions available in the market.

4.2 Do national public sector actors within your country carry out cybersecurity-related R&D activities?

Code-GCIv5: CapDev5.2

Rationale-GCIv5: Public sector actors' active involvement in cybersecurity-related R&D activities can contribute to better identification and remediation of vulnerabilities in a country's cybersecurity infrastructure. It can also promote the development of cybersecurity solutions that can be used to protect a country's critical infrastructure. Cybersecurity-related R&D activities by the public sector can also prepare for cyberattacks***.*** For the purposes of this question public sector actors should belong to the national government, and not a state or local government.

4.3 Do academic institutions within your country carry out cybersecurity-related R&D activities?

Code-GCIv5: CapDev5.3

Rationale-GCIv5: Academia has a critical role to play in cybersecurity-related R&D. Academia contributes cutting edge research and new thinking, trains the next generation of professionals, and acts as a bridge with the private and public sectors.

[23] http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

4.4 Within your country, are there programs/initiatives conducted for evaluating the cybersecurity of ICT products, such as labelling or certification schemes?

Code-GCIv5: CapDev4.2

Rationale-GCIv5: Certification and labelling schemes under which the cybersecurity of ICT products are evaluated can help promote higher standards of cybersecurity by manufactures, provide accountability, and facilitate consumers selection of products. Countries may implement different types of schemes depending on their national contexts and needs.

5. National cybersecurity industry

Code-GCIv5: CapDev5

Rationale-GCIv5: The development and support of a national cybersecurity industry can both support domestic capacity to address and improve cybersecurity challenges, and can lead to proactive cybersecurity management.

5.1 Is there a domestic cybersecurity industry within your country?

Code-GCIv5: CapDev5.1

Rationale-GCIv5: A favorable economic, political and social environment supporting cybersecurity development will incentivize the growth of a private sector around cybersecurity. The existence of public awareness campaigns, manpower development, capacity building and government incentives will drive a market for cybersecurity products and services. The existence of a home-grown cybersecurity industry is testament to such a favorable environment and will drive the growth of cybersecurity startups and associated cyber-insurance markets.

5.2 Are there any organizations or associations in your country which promote the development of your country's cybersecurity industry?

Code-GCIv5: CapDev5.4

Rationale-GCIv5: An active and engaged cybersecurity industry can be enhanced by organizations and associations by the promotion the exchange of knowledge, the development of talent, access to investment and funding, among others. These organizations and associations can be industry supported, or may derive support from national governments or other agencies.

6. Government incentive mechanisms

Code-GCIv5: CapDev6

Rationale-GCIv5: Security investment can have positive externalities that are not captured by those putting in investment or effort. To address the potential under-investment or effort in cybersecurity, governments can step in, to provide incentives to improve cybersecurity, such as funding, regulation, or other mechanisms. This can increase the level of cybersecurity in a country beyond the level that may have developed without support.

6.1 Are there any government incentive mechanisms in place to encourage capacity development in the field of cybersecurity?

Code-GCIv5: CapDev6.1

Rationale-GCIv5: Government incentive mechanisms can incentivize cybersecurity capacity development, such as undertaking studies, participating in continuing education, or the

development of new capacity development programs, incentive mechanisms such grants, scholarships, fee support, loans, or employment opportunities.

6.2 Are there any government incentive mechanisms in place for the development or further development of the cybersecurity industry?

Code-GCIv5: CapDev6.2

Rationale-GCIv5: Given the nature of information goods like cybersecurity, monopolies can occur.[24] To promote the emergence of new ideas and practices in new and existing organizations, and encourage a diversity of actors and stakeholders to participate in cybersecurity, governments can provide incentives in the form of monetary grants, tax or fee alleviation, reputational benefits, advantages contractual terms, or inducement for companies, organizations, and individuals to participate in a cybersecurity ecosystem.

6.3 Are there government incentive mechanisms within your country to encourage cybersecurity-related R&D activities?

Code-GCIv5: CapDev6.3

Rationale-GCIv5: Government incentive mechanisms are useful when existing market forces are not generating the desired outcomes. As the benefits of cybersecurity-related R&D activities can have positive externalities for society as a whole, governments can encourage cybersecurity-related R&D activities in a variety of ways, such as through grants, loan mechanisms, favorable trade and business environments, contracts, supporting university activities, among others.

[24] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf

Cooperation Measures

Rationale-GCIv5: Cybersecurity requires input from all sectors and disciplines and needs to be tackled from a multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling more comprehensive cybersecurity field of application. Given that cybersecurity spans sectors, geographics, and resource levels, cooperation is needed at the private, public, regional and international levels. Greater cooperative initiatives can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats, and enable better investigation, apprehension, and prosecution of malicious agents.

National and international cooperation can be measured based on the existence and number of partnerships, cooperative frameworks and information sharing networks.

1. Bilateral cybersecurity agreements

Code-GCIv5: Coop1

Rationale-GCIv5: Bilateral agreements (one to one agreements) refer to any officially recognized national partnerships for sharing cybersecurity assets across borders (i.e. the exchange of information, expertise, policy, technology and other resources) by the government with one other foreign government or a regional intergovernmental organization to address the risk of cross-border cyber conflicts. The indicator also measures whether the agreement is legally binding or pending ratification. Assets can designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

1.1 Bilateral cybersecurity agreement(s) with other countries

Code-GCIv5: Coop1.1

Rationale-GCIv5: Bilateral agreements (one to one agreements) refer to any officially recognized national partnerships for sharing cybersecurity assets across borders (i.e. the exchange of information, expertise, policy, technology and other resources) by the government with one other foreign government. Sharing knowledge and expertise between countries can help build strong incident response capabilities, as well as develop proactive measures to deal with cybersecurity risks.

1.1.1 Does your country have cybersecurity information sharing as part of bilateral agreement(s) with other countries?

Code-GCIv5: Coop1.1.1

Rationale-GCIv5: Cybersecurity agreements which address information sharing demonstrate increased cybersecurity commitments by countries, as they facilitate addressing potential risks, carrying out threat assessments, and cooperating on cybersecurity related action.

1.1.2 Does your country have cybersecurity capacity development part of bilateral agreement(s) with other countries?

Code-GCIv5: Coop1.1.2

Rationale-GCIv5: Agreements which promote biliteral cybersecurity capacity development enhance countries' capabilities to proactively address cyber risks through the sharing of best practices, upskilling of personnel, enhancing collaboration, enhancing awareness, and developing and implementing operational procedures related to cybersecurity.

1.2 Cybersecurity agreement(s) with international and regional organizations

Code-GCIv5: Coop1.2

Rationale-GCIv5: Given the importance of regional intergovernmental organizations, countries are increasingly entering into cooperative agreements on cybersecurity for sharing cybersecurity assets across borders, such as the exchange of information, expertise, technology and other resources, as either individual countries or as part of their membership in a regional intergovernmental organization with other regional intergovernmental organizations, such as the European Union, ASEAN, ECOWAS, OAS, AU, among others.

1.2.1 Does your country, or regional intergovernmental organization of which your country is a member, have cybersecurity information sharing as part of bilateral agreement(s) with other regional and international organizations?

Code-GCIv5: Coop1.2.1

Rationale-GCIv5: Cybersecurity agreements which address information sharing demonstrate increased cybersecurity commitments by countries, as they facilitate addressing potential risks, sharing of data on t threat assessments, and cooperating on cybersecurity related action.

1.2.2 Does your country or regional intergovernmental organization of which your country is a member, have cybersecurity capacity development part of bilateral agreement(s) with other regional and international organizations?

Code-GCIv5: Coop1.2.2

Rationale-GCIv5: Bilateral cybersecurity agreements which address cybersecurity capacity development between countries and regional intergovernmental organization can enhance cybersecurity capacity through the sharing of best practices, upskilling of personnel, enhancing collaboration, enhancing awareness, and developing and implementing operational procedures related to cybersecurity.

2. Multilateral cybersecurity agreements with other countries

Code-GCIv5: Coop2

Rationale-GCIv5: Participation in written multilateral agreements requires accord on key definitions and parameters related to cybersecurity and sets forward a common agenda for moving forward on cybersecurity. They can also further confidence building measures as part of creating positive feedback mechanisms to build peaceful relations.

2.1 Is your country part of a multilateral cybersecurity agreement that includes cybersecurity information sharing?

Code-GCIv5: Coop2.1.1

Rationale-GCIv5: Cybersecurity agreements which address information sharing demonstrate increased cybersecurity commitments by countries, as they facilitate addressing potential risks, sharing of data on carrying out threat assessments, and cooperating on cybersecurity related action.

2.2 Is your country part of a multilateral cybersecurity agreement that includes capacity development sharing?

Code-GCIv5: Coop2.1.2

Rationale-GCIv5: Participation in written multilateral agreements that include capacity development can support capacity development in countries with weaker cybersecurity postures, and support confidence building measures

3. Mutual Legal Assistance Treaties (MLATs)[25] related to cybersecurity

Code-GCIv5: Coop3

***Rationale* – GCIv5:** Given the transnational nature of cybersecurity, taking action on threats that impact the sovereignty of another state requires clear mechanisms for cooperation, especially for judicial matters. Mutual legal assistance, such as in the form of Mutual Legal Assistance Treaties (MLATs), can vary between the service of documents and transmittal of evidence, to investigatory assistance, among other forms of assistance.[26]

3.1 Does your country participate in Mutual Legal Assistance Treaties (MLATs) on cybersecurity either through bilateral or multilateral agreement(s) with other countries or regional or intergovernmental organizations?

Code-GCIv5: Coop3.1

Rationale-GCIv5: Given the transnational nature of cybersecurity, taking action on threats that impact the sovereignty of another state requires clear mechanisms for cooperation, especially for judicial matters. Mutual legal assistance, such as in the form of Mutual Legal Assistance Treaties (MLATs), can vary between the service of documents and transmittal of evidence, to investigatory assistance, among other forms of assistance.[27]

4. Public-Private Partnerships (PPPs)

Code-GCIv5: Coop4

Rationale-GCIv5: Public-Private Partnerships have been part of a trend driven by both ideological reasons and in the pursuit of value for money.[28] Especially in cybersecurity, where new innovations often originate in the private sector, engagement in PPPs can help governments more quickly benefit from these new innovations and potentially improved cybersecurity. However, PPPs also carry a number of challenges, such as principal agent problems, management of externalities, complexity of contract negotiation, contract flexibility, and effective assessment.[29]

4.1 Does your government participate in PPPs on cybersecurity with domestic companies?

Code-GCIv5: Coop4.1

Rationale-GCIv5: Because of inherent network effects, PPPs with domestic companies can foster a domestic cybersecurity ecosystem, enabling domestic private sector actors to develop and expand their skill, systems, and services.

---

[25] https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html
[26] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL
[27] https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e966?rskey=XSl5yx&result=1&prd=MPIL
[28] https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page5
[29] https://read.oecd-ilibrary.org/governance/public-private-partnerships_9789264046733-en#page66

4.2 Does your government participate in PPPs on cybersecurity with foreign companies in your country?

Code-GCIv5: Coop4.2

Rationale-GCIv5: Cybersecurity, as an information good, is subject to network effects and expertise gained from scale.[30] International actors who have cybersecurity expertise gained from a variety of national contexts or backgrounds can offer additional benefits to governments seeking to enhance national cybersecurity. Governments that engage in PPPs with foreign actors can leverage this expertise for their own growth and security.

5. Inter-agency partnerships

Code-GCIv5: Coop5

Rationale-GCIv5: Any official domestic partnerships between different government agencies within a country can facilitate government responsiveness to cybersecurity risks. Partnerships could include those for information or asset sharing between ministries, departments, programs, and other public sector institutions. For the purposes of this section, inter-agency partnerships between agencies in different countries or inter-governmental organizations are not considered.

5.1 Within your country, are there specific inter-agency coordination processes on cybersecurity among different national governmental bodies?

Code-GCIv5: Coop5.1

Rationale-GCIv5: Any official domestic partnerships between different government agencies within a country can facilitate government responsiveness to cybersecurity risks. Partnerships could include those for information or asset sharing between ministries, departments, programs, and other public sector institutions. For the purposes of this section, inter-agency partnerships between agencies in different countries or inter-governmental organizations are not considered.

[30] https://www.econstor.eu/bitstream/10419/199018/1/CESifo-Forum-2018-4-p23-28.pdf