Global
Cyber Security
Capacity Centre

Cybersecurity Capacity Maturity Model for Nations (CMM)

2021 EDITION

Executive Summary

The world's economies continue to develop with an ever-increasing dependence on technology. If we do not ensure that cybersecurity capacity exists across the entirety of cyberspace, we will inevitably create cyber-ghettos. In such environments, cyber-harm may become prevalent and cyber-attacks can easily be launched. The ability of countries to respond and grow capacity in the face of changing threats – be they due to trends in technology use, the socio-political climate, or evolution of the threat-actor ecosystem – has never been more important.

The Cybersecurity Capacity Maturity Model for Nations (CMM) helps nations understand what works, what does not work and why, across all areas of cybersecurity capacity. This is important so that governments and enterprises can adopt policies and make investments that have the potential to significantly enhance safety and security in cyberspace, while also respecting human rights, such as privacy and freedom of expression.

Since 2015, the Global Cyber Security Capacity Centre (GCSCC, Capacity Centre) has actively promoted the CMM across sectors, to drive conversation around cybersecurity capacity and to help improve global technology. The resulting adoption of the CMM by various key international stakeholders, and the completion of more than 120 CMM reviews in more than 85 countries around the world, demonstrates the positive impact of the research, supports government self-assessments and informs the development of industry tools and resources.

Prompted by the changing threat landscape and corresponding cybersecurity practice, the GCSCC has led a revision of the CMM, the first to be carried out since the 2016 edition was issued. To produce this 2021 edition, the Capacity Centre undertook a global collaborative exercise aimed at extracting and synthesising the community's latest knowledge. The GCSCC developed change proposals based on lessons learned from CMM deployments, and undertook a series of online and offline consultations with experts, to validate the findings and discuss the changes. Those who were consulted included the GCSCC Expert Advisory Panel, strategic, regional and implementation partners of the GCSCC, and other experts from academia, international and regional organisations, governments, the private sector, and civil society. Based on their input, *indicators* for each *Aspect* have been identified, designed, refined, and validated.

Actors around the world, ranging from individuals to nation states, need to ensure that cyberspace and the systems dependent on it are resilient to increasing attacks. The *CMM 2021 Edition* and its deployment will continue to contribute towards efforts to achieve this resilience, not only by gaining a more profound understanding of international cybersecurity capacity, but also by increasing effective investment into cybersecurity capacity based on a rigorous analysis of data collected from the deployment of the model. Critical gaps in all areas of international cybersecurity will be identified and filled with scalable and effective countermeasures, in co-operation with international partners from the global cybersecurity community.

The enhancement of the CMM is not intended to be a static exercise; a continuous process of refinement will be maintained to ensure the CMM remains applicable to all national contexts and reflects the global state of cybersecurity capacity maturity. However, this evolution will continue to be a considered exercise, stimulated by evidence and practice.

Contents

A National Cybersecurity Assessment with the CMM

The CMM review of a country involves data-gathering by a team of researchers who carry out in-country stakeholder consultation and desk research. The output is an evidence-based report which:

- benchmarks the maturity of a country's cybersecurity capacity;
- details a pragmatic set of actions to contribute to the advancement of cybersecurity capacity maturity gaps; and
- identifies priorities for investment and future capacity-building, based on a country's specific needs.

According to an independent study commissioned by the *UK Foreign, Commonwealth and Development Office*, the benefits of a CMM review for a country are numerous and include:

- increased cybersecurity awareness and capacity building, and greater collaboration within government;
- networking and collaboration with business and wider society;
- the enhancement of the internal credibility of the cybersecurity agenda within governments;
- help in defining roles and responsibilities within governments;
- providing evidence to increase funding for cybersecurity capacity building; and
- a foundation for country strategy and policy development.

It is important that a country can evidence its achievements in cybersecurity capacity and the CMM identifies what that evidence should be, and what it demonstrates. Such evidence gathering is in itself a multi-stakeholder process, involving a wide range of sources and organisations. Discussions can be important to resolve differences of opinion. Whether such discussions can be effective if done remotely (and online), or will necessitate face-to-face meetings, will depend upon the country undertaking a review.

For more information on the CMM review methodology, process and exemplary CMM reports, visit: https://gcscc.ox.ac.uk/the-cmm

The Dimensions of National Cybersecurity Capacity

The CMM considers cybersecurity to comprise five *Dimensions* which together constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity:

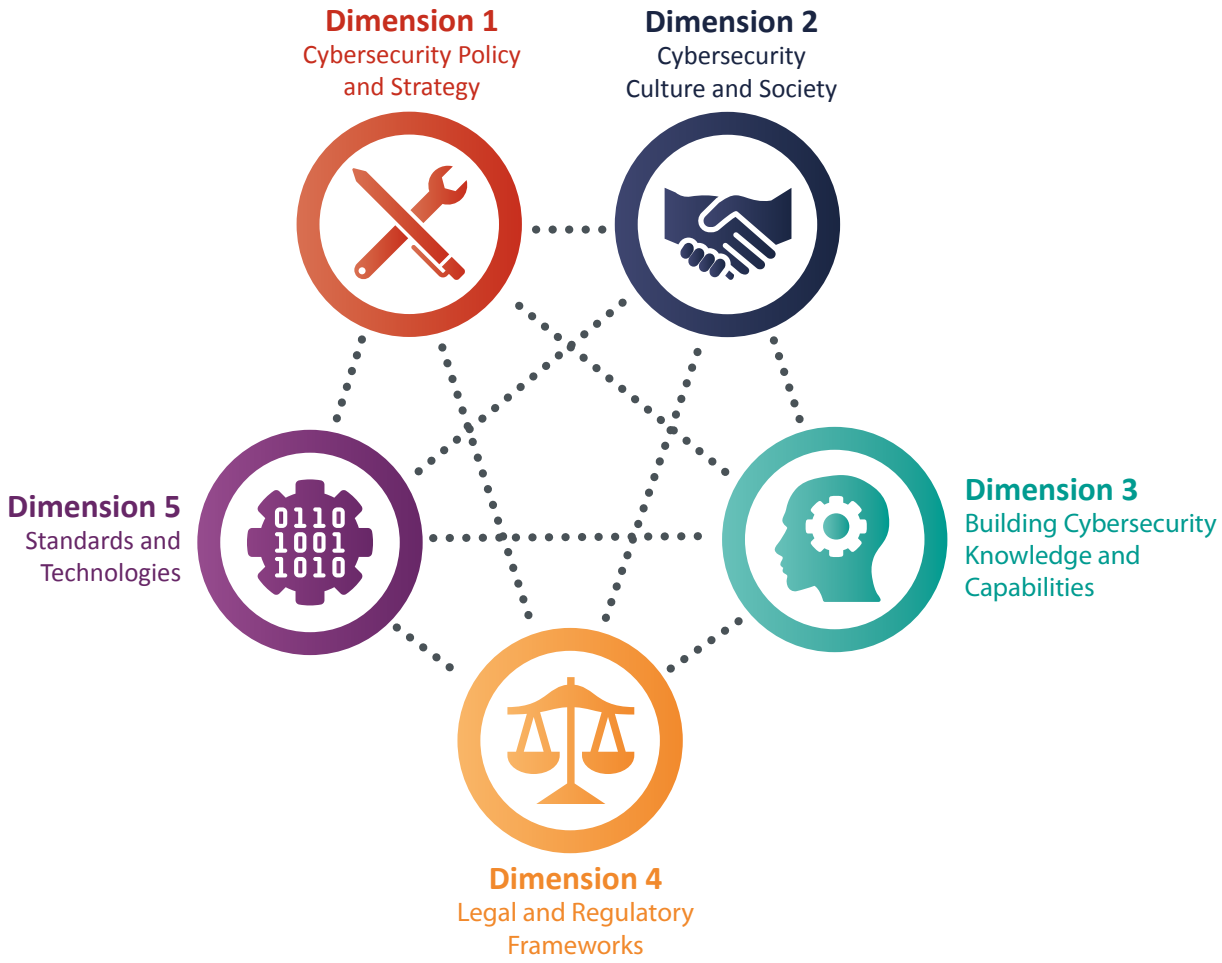
1. Developing cybersecurity policy and strategy;

2. Encouraging responsible cybersecurity culture within society;

3. Building cybersecurity knowledge and capabilities;

4. Creating effective legal and regulatory frameworks; and

5. Controlling risks through standards and technologies.



***Dimension* 1 Cybersecurity Policy and Strategy** explores the country's capacity to develop and deliver cybersecurity strategy, and to enhance its cybersecurity resilience by improving its incident response, cyber defence and critical infrastructure (CI) protection capacities. This *Dimension* considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

***Dimension* 2 Cybersecurity Culture and Society** reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this *Dimension* explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this *Dimension* reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

***Dimension* 3 Building Cybersecurity Knowledge and Capabilities** reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government, private sector and the population as a whole, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.

***Dimension* 4 Legal and Regulatory Frameworks** examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this *Dimension* observes issues such as formal and informal co-operation frameworks to combat cybercrime.

***Dimension* 5 Standards and Technologies** addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. This *Dimension* specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

The CMM defines five *Stages* of maturity for all *Dimensions* being: start-up, formative, established, strategic, and dynamic. These correspond to the following: initial development of capacity, being established, being world-leading, and able to anticipate and prepare for future cybersecurity needs.

It should be noted that there are relationships between the *Dimensions*; for example, to be effective in one area of capacity often places requirements on other areas[1]. It is also the case that resources are limited and priorities for capacity enhancements are likely to require a response which could span multiple *Dimensions*. Therefore, a benchmarking activity reviews a country against the entire CMM and across all *Dimensions*, enabling an holistic consideration of national capacity.

[1] For a country to reach an established level of maturity under the *Aspect* 'Initiatives by Government' in *Factor* 3.1 Building Cybersecurity Awareness, one of the requirements that must be met is that the content of the co-ordinated national cybersecurity awareness-raising programme includes explicit links to national cybersecurity strategy. Similarly, for a country to reach an established level of maturity under the *Aspect* 'Administration' in *Factor* 3.2 Cybersecurity Education, cybersecurity education priorities resulting from the multi-stakeholder consultation process should be reflected in the national cybersecurity strategy.

The Structure of the CMM

Dimension

The five *Dimensions* together cover the breadth of national cybersecurity capacity assessed by the CMM. Each *Dimension* is constituted by a range of *Factors*, which capture the core capacities required to deliver the *Dimension*. Together, they represent the different 'lenses' through which cybersecurity capacity can be evidenced and analysed.

Factor

Within the five *Dimensions*, *Factors* describe what it means to possess cybersecurity capacity. These are the essential elements of national capacity, which are then measured for maturity *Stage*. The complete list of *Factors* seeks to holistically incorporate all of a nation's cybersecurity capacity needs. Most *Factors* are composed of a number of *Aspects* which structure the *Factor's Indicators* into more concise parts (which directly relate to evidence gathering and measurement). However, some *Factors* that are more limited in scope do not have specific *Aspects*.

Aspect

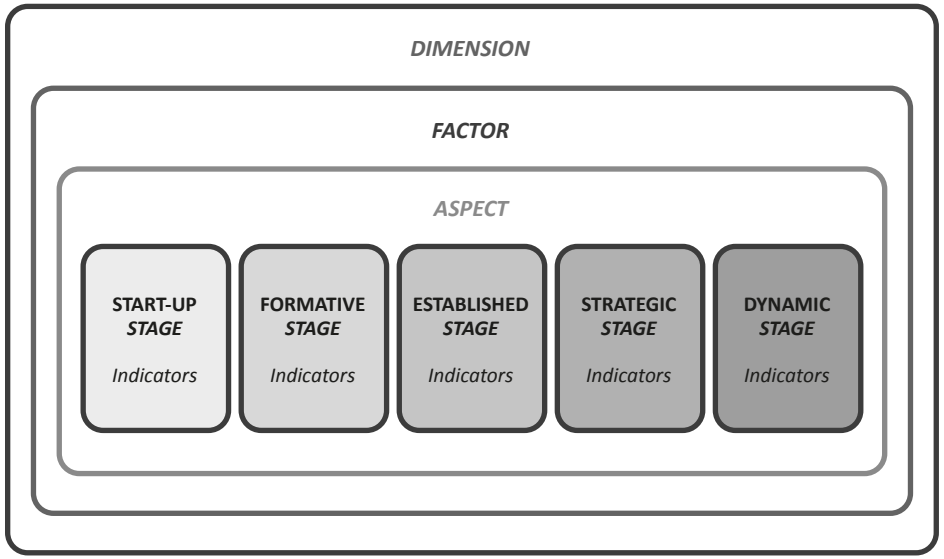
Where a *Factor* possesses multiple components, these are *Aspects*. *Aspects* are an organisational method to divide *Indicators* into smaller clusters that are easier to comprehend. The number of *Aspects* depends on the themes that emerge in the content of the *Factor* and the overall complexity of the *Factor*.

Stage

Stages define the degree to which a country has progressed in relation to a certain *Factor* or *Aspect* of cybersecurity capacity. The CMM consists of five distinct *Stages* of maturity: start-up, formative, established, strategic, dynamic (detailed on page 8). A CMM review will benchmark a country against these *Stages*, capturing existing cybersecurity capacity, from which a country can improve or decline depending on the actions taken (or inaction). Within each *Stage* there are a number of *Indicators* which a country has to fulfil to successfully have reached the *Stage*.

Indicator

Indicators represent the most basic part of CMM's structure. Each *Indicator* describes the steps, actions, or building blocks that are indicative of a specific *Stage* of maturity. To have successfully reached a *Stage* of maturity, a country will need to convince itself that it can evidence each of the *Indicators*. In order to elevate a country's cybersecurity capacity maturity, all of the *Indicators* within a particular *Stage* will need to have been fulfilled. Most of these *Indicators* are binary in nature, i.e., the country can either evidence it has fulfilled the *Indicator* criteria, or it cannot provide such evidence.



The Stages of National Cybersecurity Capacity

Stages define the degree to which a country has progressed in relation to a certain *Factor* or *Aspect* of cybersecurity capacity (see page 7). A CMM review will benchmark a country against these *Stages*, capturing existing cybersecurity capacity.

Start-up

At this *Stage*, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There may be an absence of observable evidence at this *Stage*;

Formative

Some features of the *Aspect* have begun to grow and be formulated, but may be *ad hoc*, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated;

Established

The *Indicators* of the *Aspect* are in place, and evidence shows that they are working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the *Aspect*. But the *Aspect* is functional and defined;

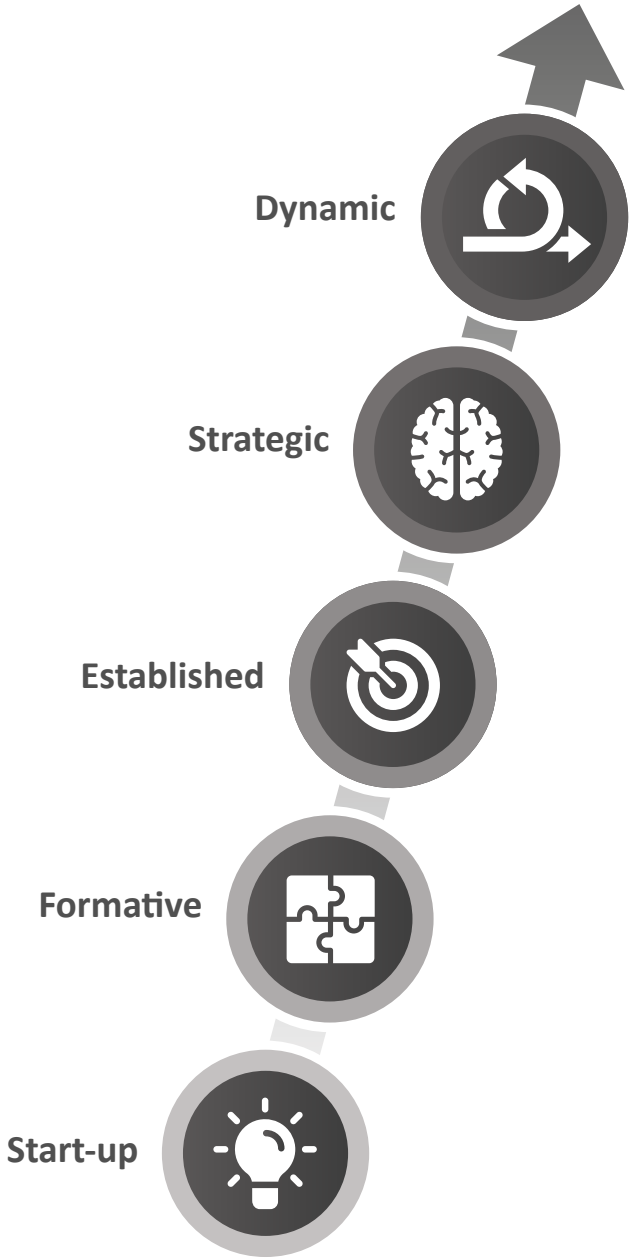
Strategic

Choices have been made about which parts of the *Aspect* are important, and which are less important for the particular organisation or nation. The strategic *Stage* reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and

Dynamic

At this *Stage*, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this *Stage*.

The CMM allows the benchmarking of current national cybersecurity capacity. Understanding the requirements to achieve higher levels of capacity will directly indicate areas for further investment, and how to evidence such capacity levels. The CMM can also be used to build business cases for investment and expected performance enhancements. Combining a CMM review with national risk assessments, social, and economic strategies can further prioritise which capacity enhancements to make.



Dimension 1: Cybersecurity Policy and Strategy

This *Dimension* explores the country's capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, cyber defence and critical infrastructure protection capacities. This *Dimension* considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

Factor
D 1.1: National Cybersecurity Strategy

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

> Navigate to Factor

Aspects

- **Strategy Development:** this *Aspect* addresses the development of a national strategy, allocation of implementation authorities across sectors and civil society, and an understanding of national cybersecurity risks and threats which drive capacity building at a national level;
- **Content:** this *Aspect* addresses the content of the national cybersecurity strategy and whether it is linked explicitly to national risks, priorities and objectives such as national security, public awareness raising, and mitigation of cybercrime, incident response capability and critical national infrastructure protection;
- **Implementation and Review:** this *Aspect* addresses the existence of an over-arching programme for cybersecurity co-ordination, including a departmental owner or co-ordinating body with a consolidated budget; and
- **International Engagement:** this *Aspect* explores to what extent the country is aware of the existence of international discussions on cybersecurity policy, and how the international debates on cybersecurity policy and related issues affect the country's interests and international standing.

Factor
D 1.2: Incident Response and Crisis Management

This *Factor* addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework

> Navigate to Factor

Aspects

- **Identification and Categorisation of Incidents:** this *Aspect* identifies whether internal mechanisms are in place for identifying and categorising incidents;
- **Organisation:** this *Aspect* addresses the existence of a mandated central body designated to collect incident information, and its relationship with the public and private sector for national level incident response; and
- **Integration of Cyber into National Crisis Management:** this *Aspect* explores to what extent cybersecurity is integrated into the national crisis management framework.

Factor

D 1.3: Critical Infrastructure (CI) Protection

This *Factor* studies the government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practice by CI operators
> Navigate to Factor

Aspects

- **Identification:** this *Aspect* addresses the existence of a general list of CI assets, sectors and operators, and an audit of CI assets on a regular basis;
- **Regulatory Requirements:** this *Aspect* addresses the existence of regulatory requirements specific to the cybersecurity of CI; and
- **Operational Practice:** this *Aspect* explores whether CI operators implement recognised industry standards, and the existence of arrangements for collaboration across and within sectors.

Factor

D 1.4: Cybersecurity in Defence and National Security

This *Factor* explores whether the government has the capacity to design and implement a strategy for cybersecurity within national security and defence. It also reviews the level of cybersecurity capability within the national security and defence establishment, and the collaboration arrangements on cybersecurity between civil and defence entities
> Navigate to Factor

Aspects

- **Defence Force Cybersecurity Strategy:** this *Aspect* addresses the existence of a strategy for supporting cybersecurity within national security and defence, and whether it is supported by appropriate legal authorities and relevant operational doctrine and rules of engagement;
- **Defence Force Cybersecurity Capability:** this *Aspect* reviews the level of cybersecurity capability and organisational structures within the national security establishment; and
- **Civil Defence Co-ordination:** this *Aspect* examines the collaboration on cybersecurity between civil and defence entities, and the existence of adequate resources in place.

Factor - D 1.1: National Cybersecurity Strategy

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Strategy Development	No national cybersecurity strategy exists, although planning processes for strategy development may have begun. Advice may have been sought from international partners.	Processes for strategy development have been initiated. An outline/draft national cybersecurity strategy has been articulated. Consultation processes have been agreed for key stakeholder groups, including private sector, civil society and international partners.	A national cybersecurity strategy has been published. An assessment of country-specific national cybersecurity risk has been conducted. The strategy reflects the needs and roles of relevant stakeholders across government (national and sub-national), business and civil society. An implementation programme is in place which covers the scope of the strategy. Mechanisms are in place to enable strategy 'owners' to monitor achievement of outcomes, address implementation issues and maintain strategy alignment.	Strategy review and renewal processes are in place. Emerging cybersecurity risks are regularly assessed and used to update the strategy and implementation plan. The impact of the strategy on risk and harm reduction is understood and is used to inform funding and priority decisions.	The national cybersecurity strategy and implementation plan are both proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental). The country is an acknowledged authority within the international community and is supporting the development of national and global cybersecurity strategies. Cybersecurity considerations are embedded within other relevant national-level strategies and implementation programmes.
Content	Various national policies and strategies may exist that refer to cybersecurity, but these are not comprehensive and there is little evidence that these reflect specific national priorities and circumstances.	Content exists that reflects country-specific priorities and circumstances. Links exist between the strategy (or draft strategy) and priorities such as national security, digital strategy and economic development, but these are generally *ad hoc* and lack detail. The strategy (or draft strategy) defines the key outcomes against which success can be evaluated.	The content of the national cybersecurity strategy is based on a comprehensive risk assessment that includes explicit links to wider national level economic and political policies and strategies. The content includes actions to raise public and business awareness, mitigate cybercrime, establish incident response capability, promote public-private partnership and protect critical infrastructure and the wider economy. Consideration has been given to how the national cybersecurity strategy might incorporate or support wider online policy objectives such as: child protection; the promotion of Human Rights; the promotion of Equality, Diversity and Inclusion; and managing disinformation.	The content takes account of the impact on cybersecurity risk of emerging technologies and their use within critical infrastructure, the wider economy and society. The outcomes defined in the strategy are specific and measurable. Metrics have been defined which enable stakeholders to evaluate the effectiveness of the strategy in reducing harm. Consideration has been given to how the beneficial outcomes of the strategy can be sustained beyond the strategy's lifetime, including how the maintenance of new capabilities will be financed.	The content takes account of the impact of broader developments on cybersecurity risk (political, economic, social, technical, legal and environmental). The content of the national cybersecurity strategy promotes and encourages bilateral and multilateral co-operation between countries to ensure a secure, resilient and trusted cyberspace.

Factor - D 1.1: National Cybersecurity Strategy

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Implementation and Review	No overarching national cybersecurity implementation programme has been developed.	A co-ordinated cybersecurity implementation programme is being developed with relevant stakeholders involved, including the private sector and civil society. Actions within the programme have been assigned to specific 'owners' but the availability of adequate resources has not yet been confirmed. Mechanisms to review processes are limited or *ad hoc*.	A detailed implementation plan has been published including actions, responsible entities and resource budgets. The implementation plan involves relevant stakeholders across government and other sectors. A co-ordinating body has been assigned. The body has sufficient authority to ensure that action 'owners' are held to account. The resources required to deliver the actions of the programme have been identified and are in place. Budget shortfalls are identified and escalated to the relevant authority. Programme review processes and metrics are in place that allow progress to be measured and risks, issues and dependencies to be escalated to the relevant authority. These processes are adequately funded.	Outcome-oriented metrics are being used to monitor the impact that the programme is having on risk reduction (and other relevant strategy goals). There is evidence of these metrics being used to refine action plans. Metrics (both progress and outcome-oriented metrics) are drawn from a wide variety of governmental, non-governmental and international sources. There is independent oversight and/or assurance of the programme.	Mechanisms are in place to make more far-reaching changes to the programme in the event of significant changes in circumstance (political, economic, social, technical, legal and environmental). The programme contributes to the global development of outcome-oriented metrics and their application.
International Engagement	There is limited awareness of the principal international debates relating to cybersecurity policy (such as cybersecurity norms, mutual legal assistance, Internet Governance, data sovereignty, data protection). The country may benefit from regional/ international operational collaboration networks but does not actively engage.	The country is aware of the existence of international discussions on cybersecurity policy and related issues. The country may, on occasion, participate in regional or international discussions on matters related to cybersecurity issues, but does not generally play an active role. The country may participate in relevant operational collaboration and policy bodies (such as FIRST*, regional CERT** bodies, the IGF***, or the UN GGE****), but takes mainly a passive role.	An assessment has been made of how the international debates on cybersecurity policy and related issues affect the country's interests and international standing. Specific engagement objectives have been defined accordingly. Multiple stakeholders have been involved in this process. The country is actively participating in relevant international bodies and forums, either directly or through relevant representative bodies. Their voices are being heard and are having an impact. The country actively contributes to regional/ international operational collaboration and policy bodies.	The country is actively building international communities of interest around specific cybersecurity policy goals and promoting their adoption. The country makes a major contribution to regional/ international operational bodies and is actively involved in building capacity in third-party countries.	The country is a leading actor in building consensus, fostering inclusivity and shaping the international debates on key cybersecurity policy issues. The country is focused on the future, seeing emerging issues (around new technology or new types of threat), and is initiating new international debates around the key issues. The country is actively involved in creating new regional/ international collaboration mechanisms.

* Forum of Incident Response and Security Teams
** Computer Emergency Response Team
*** Internet Governance Forum
**** The United Nations Group of Governmental Experts

Factor - D 1.2: Incident Response and Crisis Management

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Identification and Categorisation of Incidents	No process for identifying and categorising national-level incidents exists.	Some organisations and sectors have internal mechanisms for identifying and categorising incidents within their purview. A process for identifying national-level incidents is under development. There is no central registry in place but *ad-hoc* arrangements exist for dealing with the most significant events.	Most major organisations have internal mechanisms for identifying and categorising incidents. A central registry of national-level cybersecurity incidents exists and a process for timely escalation of incidents, from the organisational to the national level, is in place. Individual national incidents are categorised according to severity and resources are allocated accordingly.	Insights arising from national level incidents are routinely analysed in order to establish lessons and inform broader cybersecurity policy and strategy.	The criteria for categorising incidents are sufficiently flexible to cater for rapidly emerging changes in the underlying technological or threat environment. The country is contributing to international best practice in incident identification and categorisation.
Organisation	No organisation for national-level cyber incident response exists. A few organisations may have internal cybersecurity response mechanisms in place but co-ordination is minimal.	A national CERT* might exist but lacks sufficient resources and skills. Processes for managing incidents are still in development. Some organisations from public and private sectors have internal cybersecurity response mechanisms in place but co-ordination with the national CERT is *ad hoc*. The role of sub-national bodies is unclear. Bilateral co-operation with international partners is limited or *ad hoc*.	A national body for incident response has been established. It has the resources, skills, documented processes and legal authorities required to address the range of cyber incident scenarios that the country is likely to face (including out-of-hours capability, if appropriate). Relationships and protocols are in place to enable incident management co-ordination between the national body and other elements of the public and private sectors. The role of sub-national bodies in incident response is clear and mechanisms are in place to enable co-ordination between the national and sub-national levels. There is regular sharing of threat and vulnerability information, and operational good practices between the national body and a wide range of public and private sector organisations, as well as international partners.	The national body undertakes a wide range of engagement activities such as convening communities of interest, running cross-sector exercises and promoting best cybersecurity practices. The national body innovates to provide a range of additional services that improve the country's ability to prevent, detect, respond and recover from threats. The national body is widely recognised as an authoritative voice on cybersecurity within the country. The effectiveness of the national body in reducing cyber risk and harm is regularly evaluated and benchmarked against international good practice.	The government's overall operational response is adaptive to changes in the underlying technical and threat environment. The country is contributing to international best practice on how to organise operational responses to cybersecurity threats.

* Computer Emergency Response Team

Factor - D 1.2: Incident Response and Crisis Management

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Integration of Cybersecurity into National Crisis Management	No framework exists for national-level crisis management. Cybersecurity has not been considered as a potential national-level crisis scenario. Emergency communication capabilities are limited.	A national crisis management framework is in development and a specific organisation has been allocated responsibility for leading national-level crisis response. Cybersecurity has been recognised as relevant to national crisis management, both as a factor in its own right and as an element of other crisis scenarios. An exercise programme is in development and includes cybersecurity-based scenarios. Emergency communication capabilities are in place but may not be well integrated or lack resilience to cyber disruption.	Cybersecurity is fully integrated into the national crisis management framework and the organisation responsible for crisis management is equipped to deal with a range of cybersecurity-related scenarios. The role of a cyber incident management authority within the crisis management process is well defined and established, and escalation thresholds are fully understood. National crisis management scenarios with cybersecurity components are regularly exercised. Emergency communication systems are regularly tested for cyber resilience against a range of cybersecurity-related scenarios.	Lessons learnt from cyber crisis exercises are used to inform both national crisis management policy and the national cybersecurity strategy and implementation plan. International crisis planning and exercising with partners exists and routinely includes cybersecurity as an element. The resilience of emergency communications has been stress-tested against a wide range of potential scenarios.	The country is contributing to the debate on the integration of cyber into national and international crisis management. Emergency communications capabilities are capable of operating beyond the country's border in order to support third-party countries and global crisis responses.

Factor - D 1.3: Critical Infrastructure (CI) Protection

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Identification	There may be some appreciation of what constitutes a CI asset, but no formal categorisation of CI assets has been produced.	A list of general CI assets, sectors and operators has been created.	The list of CI assets has been formalised and incorporates a range of appropriate public and private sector organisations. Specific operators have been identified and are aware of their status. The list is kept up to date to reflect changes in the country's circumstances. Cross-border dependencies have been identified.	The list of CI assets is adaptive to strategic shifts in the underlying technical, social and economic environment. Interdependencies between sectors are managed. Cross-border dependencies are managed.	There is flexibility in the process for identifying CI assets to cater for rapidly emerging changes in the underlying technological or threat environment. The country is actively involved in the identification and prioritisation of global CI assets. Cross-sector and cross-border dependencies are mitigated.
Regulatory Requirements	There are no existing regulatory requirements specific to the cybersecurity of CI.	The need for baseline standards to govern CI assets is acknowledged but these are not explicitly mandated in regulation. Sector regulators do not routinely assess CI operators for compliance.	CI operators are mandated by regulation to meet appropriate cybersecurity standards (either in the form of specific cyber regulation or as part of broader regulatory requirements). Mandatory breach reporting and vulnerability disclosure requirements are in place. Formal processes are in place to evaluate CI operator compliance with regulatory standards and incident and vulnerability disclosure.	Novel approaches to regulatory supervision are being developed to improve CI cybersecurity while also facilitating effective and efficient CI service delivery. The country is promoting best practice regulatory approaches at an international level.	Regulatory frameworks are sufficiently flexible to cater for rapidly emerging changes in the underlying technological or threat environment. The country is actively involved in establishing regulatory approaches to assuring global CI.
Operational Practice	A few CI operators may be implementing good cybersecurity practices, but this is inconsistent.	Many CI operators are implementing good cybersecurity practice. There is some self-assessment against recognised industry standards. Some informal arrangements exist for collaboration across and within sectors.	CI operators are consistently implementing recognised industry standards and the effectiveness of their cybersecurity controls are regularly assessed. Mechanisms are in place for operators to share threat and vulnerability information, best practices and lessons learned from incidents and near misses. CI operators participate fully in national incident response and crisis management planning and exercising. Mechanisms are in place for public authorities to provide information and other practical support to CI operators, both pre- and post- incident.	There is extensive collaboration among CI operators and with public authorities to develop strategies that enhance collective cybersecurity. The resilience of the critical infrastructure ecosystem as a whole has been assessed against a range of scenarios, and measures are in place to address systemic risks to the economy and society.	The country and its CI operators are contributing to the international debate on global critical infrastructure resilience. Experts from the regulators and CI operators are recognised internationally for their contribution to addressing global infrastructure protection challenges.

Factor - D 1.4: Cybersecurity in Defence and National Security

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Defence Force Cybersecurity Strategy	The potential impact of cybersecurity on national security and defence may have been considered but has not been formally articulated.	The potential impact of cybersecurity on national security and defence has been assessed and a strategy for addressing these risks is under development. This analysis includes risks to the ability of the country's military and other national security assets to operate in a contested cyber environment.	A strategy for cybersecurity for national security and defence has been formally adopted (stand-alone or as part of a wider document). The strategy is supported by appropriate legal authorities and relevant operational doctrine and rules of engagement. These are consistent with international humanitarian law. The dependence of national security and military entities on the cybersecurity of other parts of the critical national infrastructure is understood and is addressed in the defence cybersecurity strategy. Cybersecurity considerations inform other elements of national security and defence strategy, where relevant.	Defence strategy includes appropriate considerations of deterrence. The country's defence and national security establishment (alongside other stakeholders) is actively engaged in the global debate on international humanitarian law and norms of behaviour as they relate to conflict in cyberspace. Declaratory strategy and published doctrine may be part of this.	Strategy and doctrine are not static but are adaptive to changing capabilities and to the geo-political and technical threat environment. The strategy is designed to promote stability in cyberspace. This includes measures to predict and influence the strategies and actions and reactions of potential allies and adversaries.
Defence Force Cybersecurity Capability	Specialist cybersecurity capability within the national security establishment is limited.	Specialist cybersecurity capability requirements are understood, and relevant organisational structures have been defined. Initial steps have been taken to establish these.	Capabilities and organisational structures are in place and have been tested. Resourcing is provided through the national military estimate or equivalent process. Operational doctrine and rules of engagement are fully embedded in training. Specialist intelligence resources are being applied to provide support and are appropriately resourced. Mechanisms to facilitate collaboration with allies are in place and have been tested.	Relevant deterrence and defence/resilience capabilities are in place, forming part of the country's defence cybersecurity strategy. Cybersecurity is embedded in wider operational and command training within the country's military forces.	Defence cybersecurity capabilities are able to support multilateral responses to shared national security challenges.

Factor - D 1.4: Cybersecurity in Defence and National Security

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Civil Defence Co-ordination	Collaboration on cybersecurity between civil and defence entities is limited.	Informal collaboration on cybersecurity between civil and defence entities may exist but has not been formalised. Defence entities have not been formally resourced to undertake this work.	Collaboration on cybersecurity between civil and defence entities exists and has been formalised. Respective roles have been defined within the country's crisis management procedures. The resources required within the defence and national security community, to support civil and CI authorities, have been formally assessed and assigned. Formal mechanisms are in place to determine military/ national security cybersecurity dependencies on civil and CI infrastructure. The ability of civil and CI infrastructure operators to provide these services has been assured.	Civil defence collaboration on cybersecurity is built into the strategic planning of both sectors and designed to address a range of future crisis scenarios. Mechanisms are in place that enable defence and the national security community to draw on the skills and capabilities of the broader economy and society. (For example, via a formal cyber reserve force)	The country is leading the international debate on best practice in cross-governmental, civil-defence cybersecurity collaboration.

Dimension 2: Cybersecurity Culture and Society

This *Dimension* reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this *Dimension* explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this *Dimension* reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

Factor
D 2.1: Cybersecurity Mindset

This *Factor* evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mindset consists of values, attitudes and practices–including habits of individual users, experts, and other actors–in the cybersecurity ecosystem that increase the capacity of users to protect themselves online
> Navigate to Factor

Aspects

- **Awareness of Risks:** this *Aspect* examines the level of awareness of cybersecurity risks within the government, private sector and users;
- **Priority of Security:** this *Aspect* examines the extent to which the government, private sector and users make cybersecurity a priority; and
- **Practices:** this *Aspect* examines whether the government, private sector and users follow safe cybersecurity practices.

Factor
D 2.2: Trust and Confidence in Online Services

This *Factor* reviews critical skills, the management of disinformation, the level of users' trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.
> Navigate to Factor

Aspects

- **Digital Literacy and Skills:** this *Aspect* examines whether Internet users critically assess what they see or receive online;
- **User Trust and Confidence in Online Search and Information:** this *Aspect* examines whether users trust in the secure use of the Internet based on indicators of website legitimacy;
- **Disinformation:** this *Aspect* examines the existence of tools and resources to address online disinformation;
- **User Trust in E-government Services:** this *Aspect* examines whether there are government e-services offered, whether trust exists in the secure provision of such services, and if efforts are in place to promote such trust in the application of security measures; and
- **User Trust in E-commerce Services:** this *Aspect* examines whether e-commerce services are offered and established in a secure environment and trusted by users.

Factor
D 2.3: User Understanding of Personal Information Protection Online

This *Factor* looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights.
> Navigate to Factor

Aspects

- **Personal Information Protection Online:** (as above)

Factor
D 2.4: Reporting Mechanisms

This *Factor* explores the existence of reporting mechanisms that function as channels for users to report Internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.
> Navigate to Factor

Aspects

- **Reporting Mechanisms:** (as above)

Factor
D 2.5: Media and Online Platforms

This *Factor* explores whether cybersecurity is a common subject of discussion across mainstream media, and an issue for broad discussion on social media. Moreover, this *Factor* looks at the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.
> Navigate to Factor

Aspects

- **Media and Social Media:** (as above)

Factor - D 2.1: Cybersecurity Mindset

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Awareness of Risks	The government has minimal or no level of awareness of cybersecurity risks. The private sector has minimal or no level of awareness of cybersecurity risks. Users have minimal or no level of awareness of cybersecurity risks.	Leading government agencies have a minimal level of awareness of cybersecurity risks. Leading private firms have a minimal level of awareness of cybersecurity risks. A limited proportion of Internet users have awareness of cybersecurity risks.	There is widespread awareness of cybersecurity risks within most government agencies. There is widespread awareness of cybersecurity risks within most private firms. A growing number of Internet users within society have awareness of cybersecurity risks.	Government agencies across all levels are aware of cybersecurity risks and proactively anticipating new risks. Private sector actors at all levels are fully aware of cybersecurity risks and are anticipating new risks. Users are fully aware of cybersecurity risks and try to anticipate new risks.	Government agencies at all levels are fully aware of cybersecurity risks and use them to update cybersecurity policies and operational practices. Most private sector actors across all levels mitigate cybersecurity risks and use them to update cybersecurity policies and operational practices. Most users identify and anticipate cybersecurity risks and try to adapt their behaviour.
Priority of Security	The government has minimal or no recognition of the need to prioritise cybersecurity. Private sector actors have minimal or no recognition of the need to prioritise cybersecurity. Users have minimal or no recognition of the need to prioritise cybersecurity. No surveys or metrics exist to document cybersecurity in government, private sector, or across users.	Leading government agencies and private firms recognise the need to prioritise cybersecurity. Private firms recognise the need to prioritise cybersecurity. A limited proportion of Internet users recognise the need to prioritise cybersecurity. Surveys and metrics to assess knowledge of cybersecurity within the nation are limited or *ad hoc*.	Most government agencies at all levels are making cybersecurity a priority. Most private firms at all levels are making cybersecurity a priority. A growing number of Internet users within society make cybersecurity a priority. Surveys and metrics to evaluate knowledge of cybersecurity within the nation are available.	Government agencies across all levels routinely prioritise and reassess cybersecurity priorities in response to changing threats to the population. Most private sector actors across all levels routinely prioritise and reassess cybersecurity priorities in response to changing threats to the population. Most users routinely prioritise cybersecurity and seek to take proactive steps to improve cybersecurity. Surveys and metrics are routinely conducted and publicised in fields of government, business and industry, and among users.	Government agencies at all levels habitually, as a matter of course, prioritise cybersecurity. Private sector actors at all levels habitually prioritise cybersecurity, as a matter of course. Users habitually prioritise cybersecurity and take steps to improve their security online. Survey results and metrics are used to refine cybersecurity policies, inform operational practices and IT-related initiatives within the nation.
Practices	The government agencies do not follow safe cybersecurity practices. Private sector companies do not follow safe cybersecurity practices. In this country, very few Internet users follow safe cybersecurity practices or take protective measures to ensure their security.	Leading government agencies follow safe cybersecurity practices. Leading private firms follow safe cybersecurity practices. A limited but growing proportion of Internet users know or follow safe cybersecurity practices.	Most government agencies at all levels follow safe cybersecurity practices. Most private firms at all levels follow safe cybersecurity practices. Most Internet users within this country know and follow safe cybersecurity practices	Government agencies across all levels routinely follow safe cybersecurity practices. Most private sector actors, (including SMEs) across all levels routinely follow safe cybersecurity practices. Most users know and routinely follow safe cybersecurity practices.	Government agencies at all levels habitually follow and also develop safe cybersecurity practices. Private sector actors at all levels habitually follow and develop safe cybersecurity practices. Nearly all users know and habitually follow safe cybersecurity practices as a matter of course.

Factor - D 2.2: Trust and Confidence in Online Services

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Digital Literacy and Skills	Very few Internet users in this country critically assess what they see or receive online. Internet users generally do not believe or even consider that they have the ability to use the Internet and protect themselves online. No programmes are available to support digital and media literacy skills.	A limited but growing proportion of Internet users critically assess what they see or receive online. A limited proportion believe that they have the ability to use the Internet and protect themselves online. One or more programmes are being developed to support digital and media literacy skills.	Most Internet users critically assess what they see or receive online, based on identifying possible risks. Most Internet users understand how and act to protect themselves from misinformation online, such as performing a search. Programmes have been developed to support digital and media literacy skills.	Most Internet users critically assess what they see or receive online, based on identifying possible risks. Most Internet users recognise questionable information online and take steps to ignore it or check its validity. Efforts are under way to co-ordinate programmes that support Internet, digital, and media literacy skills between Internet platform providers, regulators and civil society.	Nearly all Internet users habitually assess the risk in using online services, including changes in the technical and cybersecurity environment. Internet users continuously adjust their behaviour based on their assessments of the quality of information they receive. Internet platform providers, regulators and civil society are collaboratively developing programmes to support Internet, digital, and media literacy skills.
User Trust and Confidence in Online Search and Information	Most Internet users have no trust or have a blind trust in websites and what they see or receive online. Very few Internet users feel confident in using the Internet. Surveys or other metrics to assess users' trust and confidence online are not available.	Only a limited proportion of users have sufficient trust in their use of the Internet. A limited proportion of Internet users feel confident using it. Surveys and metrics to assess users' trust and confidence online are limited or *ad hoc*.	A growing proportion of users have sufficient trust in using the Internet safely and recognise indicators of legitimate sites and information sources. A growing number of users feel confident using the Internet. Surveys and metrics to assess users' trust and confidence online are in place and adequately funded.	Most users have a learned level of trust in using the Internet safely and recognise indicators of legitimate sites and information sources. Most Internet users feel confident using the Internet, believe they can recognise problematic or non-legitimate websites (including mimicry attempts), and check information using tools such as search options. Surveys and metrics to assess users' trust and confidence online are routinely conducted.	Nearly all users trust that they can safely use of the Internet for a variety of purposes and can help others to use it safely. Nearly all Internet users feel confident using the Internet and sourcing valid content. Surveys and metrics have a strong reputation in the region or globally and are shaping the development of metrics in other nations.

Factor - D 2.2: Trust and Confidence in Online Services

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Disinformation	Internet platform providers are not addressing issues of disinformation such as misinformation, in this nation. Civil society and other non-government actors lack the tools and resources to address online disinformation, such as exposing misinformation campaigns. Government agencies and actors have not addressed online disinformation online.	Internet platform providers are developing approaches to address issues of disinformation in this nation. The development of tools and resources to address disinformation have been initiated by leading civil society and non-governmental actors. Government programmes and initiatives to address disinformation are being developed but entail filtering and limited efforts to inform Internet users.	Internet platform providers have a number of approaches in place to address disinformation; these respect freedom of expression and other human rights online. Civil society stakeholders have developed tools and resources to address online disinformation. Government programmes and initiatives to strengthen the public's preparedness against online disinformation are restricted to awareness raising, but avoid censorship or filtering of information.	Internet platform providers have instituted policies and practices to address disinformation; these respect freedom of expression and other human rights online. The joint efforts of civil society stakeholders are in place and are regularly used to address online disinformation in ways that respect freedom of expression and other human rights online. Outcome-oriented surveys are used to refine programmes and initiatives aimed at empowering users and building the public's understanding of possible online disinformation.	Internet platform providers have instituted policies and practices to address disinformation in some innovative ways that respect freedom of expression and other human rights online. The joint efforts of civil society stakeholders are proactively reviewed to take account of broader strategic developments related to disinformation and awareness raising. The country is supporting the development of national/ regional/ international action plans and guidelines to address disinformation in ways that protect an open Internet and empower users.
User Trust in E-government Services	Government offers a very limited number of e-services, if any, and has not publicly promoted their security. Generally, the public does not use any significant e-government services. No surveys or metrics exist to show how Internet users trust e-government services. There is a lack of information about e-government security and security breaches.	Government has begun to build a core set of e-services, for which they recognise the need to apply security measures in order to establish trust in their use. A limited number of early adopters trust in the secure use of e-government services. Metrics to assess users' trust in e-government services is limited or *ad hoc*. Public authorities are developing information on privacy and security initiatives and breaches in an *ad-hoc* manner.	Key e-government services have been developed and have generated a large number of users. A sizeable and growing number of Internet users trust in the use of e-government services. Surveys and metrics to assess users' trust in e-government services are in place and adequately funded. Public authorities are publishing information and updates of their privacy and security breaches and initiatives such as privacy by default.	E-government services have become the dominant (default) mode of government information service delivery. The majority of Internet users in this country trust in the secure use of e-government services and make use of them. Surveys and metrics to assess users' trust in e-government services are routinely conducted. Public authorities are co-ordinating, publishing and informing users about privacy and security initiatives and breaches.	E-government services in this country are recognised regionally or internationally. Internet users trust that e-government services are proactively reviewed, improved and expanded to enhance their security. Outcome-oriented surveys are used to review e-government services and evaluate the management of online content. The country is a leader in informing users about current and developing privacy and security breaches, initiatives and other issues.

Factor - D 2.2: Trust and Confidence in Online Services

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
User Trust in E-commerce Services	E-commerce services are not offered. Internet users lack the trust to use any available e-commerce services. No surveys or metrics exist to show how Internet users trust e-commerce services. There is little or no recognition of the need for security initiatives for e-commerce services.	E-commerce services are being provided to a limited extent. A limited number of early adopters trust in the secure use of e-commerce services. Metrics to assess users' trust in e-commerce services is limited or *ad hoc*. The private sector recognises the need for the application of security measures to establish trust in e-commerce services.	E-commerce services are fully established by multiple stakeholders in a secure environment. A sizeable and growing number of Internet users trust in the secure use of e-commerce services. Surveys and metrics to assess users' trust in e-commerce services are in place and adequately funded. Reliable security solutions are up to date and available, such as for payment systems. Certification schemes and trust marks for e-commerce services are in place.	E-commerce services have become widely accepted as a safe practice for consumers. The majority of users trust in the secure use of e-commerce services and make use of them. Surveys and metrics to assess users' trust in e-commerce services are routinely conducted. Stakeholders are investing in enhanced service functionality of e-commerce services, protection of personal information and the provision of user feedback mechanisms.	E-commerce services in this country are recognised regionally or internationally. Internet users trust that e-commerce services are proactively reviewed, improved and expanded to enhance their security. Outcome-oriented surveys are used to review and improve e-commerce services in order to promote transparent, trustworthy and secure systems. Terms and conditions provided by e-commerce services are clear and easily comprehensible to all users.

Factor - D 2.3: User Understanding of Personal Information Protection Online

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Personal Information Protection Online	Users and stakeholders within the public and private sectors have no or minimal knowledge about how personal information is handled online, nor do they believe that adequate measures are in place to protect their personal information online. There is no or limited discussion regarding the protection of personal information online. Privacy standards are not in place to shape Internet and social media practices.	Users and stakeholders within the public and private sectors may have general knowledge about how personal information is handled online; and may employ good (proactive) cybersecurity practices to protect their personal information online. Discussions have begun regarding the protection of personal information and about the balance between security and privacy. Concrete actions or privacy policies are being developed.	A growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference, or unwanted access of information by others. There is considerable public debate regarding the protection of personal information and about the balance between security and privacy. Privacy policies have been developed within the public and private sectors.	All stakeholders have the information, confidence and the ability to take steps to protect their personal information online and to maintain control of the distribution of this information. Users and stakeholders within the public and private sectors widely recognise the importance of protection of personal information online and are aware of their privacy rights. Mechanisms are in place in private and public sectors to shape Internet and social media practices and ensure that privacy and security do not compete.	Users have the knowledge and skills necessary to protect their personal information online, adapting their abilities to the changing risk environment. Policies in private and public sectors are proactively reviewed to ensure privacy and security do not compete in a changing environment and are informed by user feedback and public debate. New mechanisms are in place, such as privacy by default, as tools for transparency and are promoted.

Factor - D 2.4: Reporting Mechanisms

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Reporting Mechanisms	There are no official reporting mechanisms available, but discussions might have begun. Users do not use social media channels to raise concerns over any cyber harms and problems. No metrics of reported incidents exist.	The public and/or private sectors are providing some channels for reporting cyber harms (such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents), but these channels are not co-ordinated and are used in an *ad-hoc* manner. Internet users use social media channels to inform other users in an *ad-hoc* manner. Metrics of reported incidents is being developed.	Reporting mechanisms have been established, promoted and are regularly used. Internet users widely use social media channels to inform other users. There are good metrics of reported incidents.	Co-ordinated reporting mechanisms are widely used and promoted within public and private sectors. Internet users routinely use social media channels to inform other users. Cyber harm metrics have been used to inform the revision and promotion of new policies and practices.	Mechanisms have been developed to co-ordinate response to reported incidents between law enforcement and the national incident response capability. Internet users habitually use social media channels to inform other users and share good practice. Metrics are routinely used to inform policy and decision-makers.

Factor - D 2.5: Media and Online Platforms

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Media and Social Media	Mass media rarely, if ever, cover information about cybersecurity or report on issues such as security breaches or cybercrime. There is no, or rarely any discussion on social media about cybersecurity. Any portrayal of whistleblowers is negative, and based on criminal or other negative stereotypes.	It is perceived that there is *ad-hoc* mass media coverage of cybersecurity, with limited information provided and reporting on specific issues that individuals face online, such as protection for children online, or cyber-bullying. It is perceived that there is limited discussion on social media about cybersecurity. There have been positive examples of cases where whistleblowers have had a constructive impact.	It is perceived that cybersecurity is a common subject across mainstream media, and information and reports on a wide range of issues, including security breaches and cybercrime, are widely disseminated. There is broad discussion on social media about cybersecurity. There is acceptance that whistleblowers can play a positive role.	It is perceived that mass media coverage extends beyond threat reporting and can inform the public about proactive and actionable cybersecurity measures, as well economic and social impacts. There is frequent discussion on social media about cybersecurity and individuals regularly use social media to share online experiences. Transparency is encouraged as are whistleblowers.	It is perceived that the broad discussion of personal experiences and personal attitudes of individuals across mainstream and social media inform policy making and facilitate societal change. Social media has become a major component in tracking and addressing cyber harms. Whistleblowing has been encouraged and protected as a means of social accountability.

Dimension 3: Building Cybersecurity Knowledge and Capabilities

This *Dimension* reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government, private sector and the population as a whole, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.

Factor
D 3.1: Building Cybersecurity Awareness

This *Factor* focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats and ways to address them.
> Navigate to Factor

Aspects

- **Awareness-raising Initiatives by Government:** this *Aspect* examines the existence of a national co-ordinated cybersecurity awareness-raising programme driven by the government, covering a wide range of demographics and issues, developed in consultation with stakeholders from various sectors;
- **Awareness-raising Initiatives by Private Sector:** this *Aspect* examines the existence of awareness-raising programmes driven by the private sector and the extent to which they are aligned with government and civil society initiatives;
- **Awareness-raising Initiatives by Civil Society:** this *Aspect* examines the existence of awareness-raising programmes driven by the civil society and the extent to which they are aligned with government and private sector initiatives; and
- **Executive Awareness Raising:** this *Aspect* examines efforts to raise executives' awareness of cybersecurity issues in the public, private, academic and civil society sectors, as well as how cybersecurity risks might be addressed.

Factor
D 3.2: Cybersecurity Education

This *Factor* addresses the availability and provision of high-quality cybersecurity education programmes and sufficient qualified teachers and lecturers. Moreover, this Factor examines the need to enhance cybersecurity education at national and institutional levels and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.
> Navigate to Factor

Aspects

- **Provision:** this *Aspect* explores whether there are educational cybersecurity offerings and educator qualification programmes available that provide an understanding of current risks and skills requirements; and
- **Administration:** this *Aspect* explores the co-ordination of, and resources for developing and enhancing cybersecurity education frameworks with allocated budget and spending based on the national demand.

Factor
D 3.3: Cybersecurity Professional Training

This *Factor* addresses and reviews the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this Factor reviews the uptake of cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organisations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals.
> Navigate to Factor

Aspects

- **Provision:** this *Aspect* examines the development, availability and provision of cybersecurity training programmes for enhancing skills and capabilities; and
- **Uptake:** this *Aspect* examines the uptake and affordability of such programmes to produce a cadre of certified cybersecurity professionals. Issues investigated include initiatives to register for such programmes, initiatives to stay in the country after successful completion, knowledge-sharing after completing a programme, and the existence of a national register of successful and certified students.

Factor
D 3.4: Cybersecurity Research and Innovation

This *Factor* addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges and to advance the building of cybersecurity knowledge and capabilities in the country.
> Navigate to Factor

Aspects

- **Cybersecurity Research and Development:** this *Aspect* investigates the existence of a research and innovation culture in the country, one that is related to a national list of current and completed projects, financial support, incentives and usable research outputs.

Factor - D 3.1: Building Cybersecurity Awareness

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Initiatives by Government	No overarching national cybersecurity awareness-raising programme has been developed by the government. The need for awareness of cybersecurity threats and vulnerabilities in the government is not recognised or is only at initial stages of discussion.	A co-ordinated cybersecurity awareness raising programme with the involvement of the government is under development, with relevant stakeholders involved, including the private sector and civil society. Awareness-raising programmes, courses, seminars and online resources initiated by the government are available but not sufficiently reflected in the national cybersecurity strategy or is in development. The actions within the programmes are led by different 'owners' but they are not yet co-ordinated. The availability of adequate resources has not yet been confirmed. Initial system of mechanisms and metrics to review processes are limited or *ad hoc*.	A co-ordinated national cybersecurity awareness-raising programme with detailed implementation plan is published. The content includes explicit links to national cybersecurity strategy. A co-ordinating body has been assigned with sufficient authority and resources required to deliver the actions of the national programme. A national cybersecurity awareness portal exists to improve the skills and knowledge of the society and is disseminated via that programme. Programme review processes and outcome-oriented metrics are in place, are adequately funded and allow effectiveness to be measured.	The national awareness-raising programme is fully integrated with sector-specific, tailored awareness-raising programmes, such as those focusing on industry, academia, civil society, and/or women and children. Emerging cybersecurity risks are regularly assessed and used to update the national cybersecurity awareness-raising programme. There is evidence of these metrics being used to refine actions within the national awareness-raising programme and national cybersecurity strategy.	The national cybersecurity awareness-raising programme with private and civil society stakeholders is proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental). The country is actively involved in creating new regional/international cybersecurity awareness-raising programmes that contribute toward expanding and enhancing international awareness-raising good practices. The national cybersecurity awareness-raising programme has a measurable impact on the reduction of the overall threat landscape.
Initiatives by Private Sector	The need for awareness of cybersecurity threats and vulnerabilities in the private sector is not recognised or is only at initial stages of discussion.	Awareness-raising programmes, courses, seminars and online resources initiated by the private sector are available but no co-ordination or scaling efforts have been conducted. Initial system of mechanisms and metrics to review processes are limited or *ad hoc*.	Collaborative awareness-raising efforts (e.g.: joint policy and/or advocacy work) with government and civil society stakeholders are made in order to pool resources, information and identify solutions for cyber safety practices. The role of specific 'owners' assigned to actions within private sector initiatives are clear and mechanisms are in place to enable co-ordination between the levels of government, private sector and civil society. Programme review processes and outcome-oriented metrics are in place, well-funded and shared with government and civil society stakeholders.	The effectiveness of joint awareness-raising efforts with government and civil society stakeholders is regularly assessed and used to enhance collaborative processes. Private sector initiatives are fully integrated into the national awareness-raising programme. Evidence from the lessons learnt is fed into the development of future programmes.	The joint awareness-raising efforts with government and civil society stakeholders are proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental). The joint awareness-raising efforts with government and civil society stakeholders have a measurable impact on reduction of the overall threat landscape.

Factor - D 3.1: Building Cybersecurity Awareness

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Initiatives by Civil Society	The need for awareness of cybersecurity threats and vulnerabilities in civil society is not recognised or is only at initial stages of discussion.	There are indications that civil society realises that it can play a role in awareness-raising programmes, courses, seminars and online resources, but no real deliverables are yet evident. Initial system of metrics may exist.	Collaborative awareness-raising efforts (e.g.: joint policy and/or advocacy work) with government and private sector stakeholders are taking place in order to pool resources and information and identify solutions for cyber safety practices. The role of specific 'owners' assigned to actions within civil society initiatives are clear and mechanisms are in place to enable co-ordination between the levels of government, private sector and civil society. Programme review processes and outcome-oriented metrics are in place, well-funded and shared with government and private sector stakeholders.	The effectiveness of joint awareness-raising efforts with government and private sector stakeholders is regularly assessed and used to enhance collaborative processes. Civil society initiatives are fully integrated into the national awareness-raising programme. Evidence from the lessons learnt is fed into the development of future programmes.	The joint awareness-raising efforts with government and private sector stakeholders are proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental). The joint awareness-raising efforts with government and private sector have a measurable impact on reduction of the overall threat landscape.
Executive Awareness Raising	Awareness raising on cybersecurity issues for executives is limited or non-existent. Executives are not yet aware of their responsibilities to shareholders, clients, customers, and employees in relation to cybersecurity.	Executives are made aware of general cybersecurity issues, but not how these issues and threats might affect their organisations. Executives of particular sectors, such as finance and telecommunications, have been made aware of cybersecurity risks in general, and how the organisation deals with cybersecurity issues, but not of strategic implications.	Awareness raising of executives in the public, private, academic and civil society sectors address cybersecurity risks in general, some of the primary methods of attack, and how the organisation deals with cyber issues (usually abdicated to the CIO*). Select executive members are made aware of how cybersecurity risks affect the strategic decision making of the organisation, particularly those in the financial and telecommunications sectors. Awareness-raising efforts of cybersecurity crisis management at the executive level is still reactive in focus.	Executive awareness-raising efforts in nearly all sectors include the identification of strategic assets, specific measures in place to protect them, and the mechanism by which they are protected. Executives are able to alter strategic decision making and allocate specific funding and people to the various elements of cyber risk, contingent on their company's prevailing situation. Executives are made aware of what contingency plans are in place to address various cyber-based attacks and their aftermath. Executive awareness courses in cybersecurity are mandatory for nearly all sectors.	Cybersecurity risks are considered as an agenda item at every executive meeting, and funding and attention is reallocated to address those risks. Executives at regional and international level are regarded as a source of good practice in responsible and accountable corporate cybersecurity governance.

* Chief Information Officer

Factor - D 3.2: Cybersecurity Education

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Provision	Few or no cybersecurity educators are available, and there are no qualification programmes for educators. Computer science courses are offered that may have a security component, but no cybersecurity-related courses are offered. No accreditation in cybersecurity education exists.	Qualification programmes for cybersecurity educators are being explored, with a small cadre of existing qualified educators. Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered. A demand for cybersecurity education is evidenced through course enrolment and feedback.	Qualifications for and supply of educators are readily available in cybersecurity. Specialised courses in cybersecurity are offered and accredited at university level. Cybersecurity risk-awareness modules are offered as part of many university courses. Degrees in cybersecurity-related fields are offered by universities or equivalent educational institutions. Universities and other bodies hold seminars/lectures on cybersecurity issues, aimed at non-specialists. Research and development are leading considerations in cybersecurity education. Cybersecurity education is not limited to universities or equivalent educational institutions, but ranges from primary, secondary and tertiary to post-graduate levels, including vocational education. Steps might have been taken to incorporate STEM* or equivalent education framework with a focus on cybersecurity throughout primary and secondary curricula.	Cybersecurity educators are not only drawn from the academic environment, but incentives are in place so that industry and/or government experts take these positions as well. Accredited cybersecurity courses are embedded in all computer science degrees. Degrees are specifically offered in cybersecurity, and encompass courses and models in various other cybersecurity-related fields, including technical and non-technical elements such as policy implications, and multi-disciplinary education. Cybersecurity educational offerings are weighted and focused on an understanding of current risks and skills requirements. The content of cybersecurity courses covers topics on emerging threats in cybersecurity. National or international cybersecurity frameworks and/or curricular guidelines are taken into consideration by academic institutions when designing cybersecurity courses. Apprenticeship programmes in different industry sectors are offered to combine knowledge and practical skills.	National courses, degrees, and research are at the forefront of cybersecurity education. Cybersecurity education programmes maintain a balance between preserving core components of the curriculum and promoting adaptive processes that respond to rapid changes in the cybersecurity environment. Prevailing cybersecurity requirements are considered in the redevelopment of all general curricula.

* Science, Technology, Engineering, and Mathematics

Factor - D 3.2: Cybersecurity Education

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Administration	The need to enhance national cybersecurity education is not yet considered. A network of national contact points for governmental, regulatory bodies, critical industries and education institutions is not yet established. Discussion of how co-ordinated management of cybersecurity education and research enhances national knowledge development has not or has only just begun.	The need to enhance cybersecurity education in schools and universities or equivalent educational institutions has been identified by leading government, industry, and academic stakeholders. Schools, government and industry collaborate in an *ad-hoc* manner to supply the resources necessary for providing cybersecurity education. A national budget focused on cybersecurity education is not yet established. Initial system of mechanisms and metrics to review the supply and demand for cybersecurity courses are limited or *ad hoc*.	Broad consultation across government, private sector, academia and civil society stakeholders informs cybersecurity education priorities and is reflected in national cybersecurity strategy. National budget is dedicated to national cybersecurity research and laboratories at universities or equivalent educational institutions. Competitions, initiatives and funding schemes for students and employees are promoted by government and/or industry in order to increase the attractiveness of cybersecurity careers. Programme review processes and outcome-oriented metrics to review the supply and demand for cybersecurity courses are in place and well-funded.	Metrics are being used to refine actions within educational investment to create a cadre of cybersecurity experts in the country across, all sectors. Management of the government budget and spending on cybersecurity education is based on national demand. Leading national cybersecurity academic institutions share lessons learnt with other national and international counterparts. Government has established academic centres of excellence in cybersecurity.	International cybersecurity centres of excellence are established through twinning programmes led by world-class institutions. Co-operation between all stakeholders in cybersecurity education is routine and can be proven. Content in cybersecurity education programmes is aligned with practical cybersecurity problems and business challenges and provides a mechanism for enhancing curricula based on the evolving landscape.

Factor - D 3.3: Cybersecurity Professional Training

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Provision	Few or no training programmes in cybersecurity exist.	The need for training professionals in cybersecurity has been documented at the national level. Training for general IT staff is provided on cybersecurity issues so that they can react to incidents as they occur, but no training for dedicated security professionals exists. ICT* professional certification is offered, with some security modules or components. Best practice training and certifications might be accessible via international online sources (e.g.: CISSP**). *Ad-hoc* training courses, seminars and online resources are available for cybersecurity professionals through public or private sources, with limited evidence of take-up.	Structured cybersecurity training programmes exist to develop skills towards building a cadre of cybersecurity-specific professionals. National or international cybersecurity vocational-based frameworks and international best practices are taken into consideration when designing professional training courses. Security professional certification is offered across sectors within the country. The needs of society are well understood, and a list of training requirements is documented. Training programmes for non-cybersecurity professionals are recognised and offered. Government initiatives to stay in the country after the successful completion of cybersecurity training programmes might be in place.	A range of cybersecurity training courses is tailored towards meeting national strategic demand and aligns with international good practice. The training programmes outline the priorities in the national cybersecurity strategy. Training programmes are offered to cybersecurity professionals and focus on the skills necessary to communicate technically complex challenges to non-technical audiences, such as management and general employees. Outcome-oriented metrics drawn from comprehensive supply-and-demand data for cybersecurity professionals are being used to inform the modes, sustainability and procedures of future training programmes.	The public and private sector collaborate to offer training, and constantly adapt and seek to build skillsets drawn from both sectors. Training offerings and education programmes are co-ordinated so that the foundation established in schools can enable training programmes to build a highly skilled workforce. Programmes and incentive structures are in place to ensure the retention of the trained workforce within the country.
Uptake	Training uptake by IT personnel designated to respond to cybersecurity incidents is limited or non-existent. There is no transfer of knowledge from employees trained in cybersecurity to untrained employees.	Metrics that evaluate the take-up of *ad-hoc* training courses, seminars, online resources, and certification offerings are limited in scope or *ad hoc*. The transfer of knowledge from employees trained in cybersecurity to untrained employees in both the public and private sectors is *ad hoc*.	There is an established cadre of certified employees trained in cybersecurity issues, processes, planning and analytics. A national register of successful and certified students and professionals might exist. The transfer of knowledge from employees trained in cybersecurity to untrained employees in both public and private sectors is established. Job creation initiatives for cybersecurity within organisations are established and encourage employers to train staff to become cybersecurity professionals. Programme review processes and metrics are in place to allow progress to be measured and assess the supply and demand for cybersecurity-skilled workers in both public and private environments. These processes are adequately funded.	The uptake of cybersecurity training is used to inform future training programmes. Co-ordination of training across all sectors ensures the national demand for professionals is met.	Cybersecurity professionals not only fulfil national requirements, but domestic professionals overseas are consulted to share lessons learnt and best practice.

* Information and Communications Technology
** Certified Information Systems Security Professional

Factor - D 3.4: Cybersecurity Research and Innovation

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Research and Development	There are limited or no cybersecurity research and development (R&D) activities occurring in the country. There is no access to R&D activities in cybersecurity from other countries.	Some integration of cybersecurity R&D activities occurs within the country, or with a partner country that understands how cyberactivity R&D applies to the local context of the country. The country may participate in relevant regional/ international cybersecurity-related research collaboration networks. Cybersecurity R&D performance metrics are limited in scope, or *ad hoc*.	Cybersecurity R&D activities have been established and are indicated in the national cybersecurity strategy. R&D strategy may be in development. The resources and processes required to deliver the actions of cybersecurity R&D activities have been identified and are in place. Funding is adequate to deliver these actions. There is active regional/ international collaboration with leading practice and developments. The country is actively participating and contributing to regional/ international cybersecurity-related research collaboration networks. Metrics for measuring R&D performance are in place and allow progress to be measured and to improve the cybersecurity R&D capability of the country.	The country is actively building communities of interest around R&D priorities in cybersecurity. R&D strategy is in place and fully implemented. The country makes a major contribution to cybersecurity R&D and is actively involved in building innovation capacity through international R&D consortia and investment. Emerging cybersecurity risks are regularly assessed and used to update the national cybersecurity strategy and the development of future programmes of the R&D strategy. Synergy between academic institutions and industry supports R&D activities and is used to design cyber curricula that cover industry needs.	The country is a leading actor in cybersecurity research and innovation and is shaping international debates on the development of R&D strategic plans. The country is forward looking, seeing emerging issues (around new technology or new types of threat), and uses R&D to prepare a future threat environment. The country is contributing to international best practices in cybersecurity R&D.

Dimension 4: Legal and Regulatory Frameworks

This *Dimension* examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this *Dimension* observes issues such as formal and informal co-operation frameworks to combat cybercrime.

Factor
D 4.1: Legal and Regulatory Provisions

This *Factor* addresses various legislation and regulatory provisions relating to cybersecurity, including legal and regulatory requirements, substantive and procedural cybercrime legislation, and human rights impact assessment.
> Navigate to Factor

Aspects

- **Substantive Cybercrime Legislation:** this *Aspect* explores whether existing legislation criminalises a variety of cybercrimes in specific legislation or general criminal law;
- **Legal and Regulatory Requirements for Cybersecurity:** this *Aspect* reviews the existence of legal and regulatory frameworks on cybersecurity;
- **Procedural Cybercrime Legislation:** this *Aspect* examines whether comprehensive criminal procedural law–with procedural powers for the investigation of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime and crimes involving electronic evidence–is implemented; and
- **Human Rights Impact Assessment:** this *Aspect* examines whether human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations are carried out.

Factor
D 4.2: Related Legislative Frameworks

This *Factor* addresses the legislative frameworks related to cybersecurity including data protection, child protection, consumer protection, and intellectual property.
> Navigate to Factor

Aspects

- **Data Protection Legislation:** this *Aspect* examines the existence and implementation of comprehensive data protection legislation;
- **Child Protection Online:** this *Aspect* focuses on the legislative protection of children online, including the protection of their rights online and the criminalisation of child abuse online;
- **Consumer Protection Legislation:** this *Aspect* addresses the existence and implementation of legislation protecting consumers online from fraud and other forms of business malpractice; and
- **Intellectual Property Legislation:** this *Aspect* is concerned with the existence and implementation of online intellectual property legislation.

Factor

D 4.3. Legal and Regulatory Capability and Capacity

This *Factor* studies the capacity of law enforcement to investigate cybercrime, the prosecution's capacity to present cybercrime and electronic evidence cases, and the court's capacity to preside over cybercrime cases and those involving electronic evidence. Finally, this Factor reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.
> Navigate to Factor

Aspects

- **Law Enforcement:** this *Aspect* examines whether law enforcement officers and agencies have received training in investigating and managing cybercrime cases, and cases involving electronic evidence, and whether there are sufficient human, procedural and technological resources;
- **Prosecution:** this *Aspect* examines whether prosecutors have received training on handling cybercrime cases and cases involving electronic evidence, and whether there are sufficient human, procedural and technological resources;
- **Courts:** this *Aspect* examines whether courts have sufficient resources and training to ensure effective and efficient prosecution of cybercrime cases and cases involving electronic evidence; and
- **Regulatory Bodies:** this *Aspect* reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.

Factor

D 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime

This *Factor* addresses the existence and function of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.
> Navigate to Factor

Aspects

- **Law Enforcement Co-operation with Private Sector:** this *Aspect* examines the information exchange mechanism on cybercrime between domestic public and private sectors, including co-operation with Internet service and other technology providers;
- **Co-operation with Foreign Law Enforcement Counterparts:** this *Aspect* examines the existence of formal mechanisms of international law enforcement co-operation; and
- **Government-Criminal Justice Sector Collaboration:** this *Aspect* reviews the formal communication channels between government and criminal justice actors.

Factor - D 4.1: Legal and Regulatory Provisions

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Substantive Cybercrime Legislation	Specific substantive criminal law on cybercrime does not exist. General criminal law may exist, but its application to cybercrime is unclear.	Partial legislation exists that addresses some aspects of cybercrime, or cybercrime legal provisions are in development.	Substantive cybercrime legal provisions are contained in specific legislation or a general criminal law. The country may have ratified regional or international instruments on cybercrime. The country consistently seeks to implement these measures into domestic law.	Measures are in place to exceed minimal baselines specified in international treaties, where appropriate. The country seeks to adapt its substantive cybercrime legislation to take account of emerging technologies and their use.	Substantive cybercrime law is constructed so that it can cater for dynamic changes in the underlying technology and threat environment, without the need for substantial and lengthy revision. The country is actively contributing to the international promotion of effective cybercrime legislation.
Legal and Regulatory Requirements for Cybersecurity	There are limited cybersecurity requirements set out in regulation or law. The need to create legal and regulatory frameworks on cybersecurity may have been recognised and may have resulted in a gap analysis.	Stakeholders from relevant sectors have been consulted to support the establishment of legal and regulatory frameworks. Draft legislation and regulation may be in place, but this has yet to be adopted and may not cover all relevant sectors.	Comprehensive cybersecurity requirements are set out in relevant regulation and law (including sector-specific requirements, where relevant). These requirements may include mandatory standards, or breach notification requirements and vulnerability disclosure requirements. Relevant civil and criminal liabilities are clearly articulated and understood by regulated entities. Relevant legal and regulatory bodies have the powers needed to enforce these requirements.	The effectiveness of law and regulation in improving cybersecurity practice is regularly assessed and used to inform their future development. Regulations are updated to take account of emerging technologies.	Regulatory frameworks are sufficiently flexible to cater for rapidly emerging changes in the underlying technological or threat environment. The country is promoting best practice legal and regulatory approaches internationally. The country is actively involved in the development of international agreements to promote harmonisation and mutual recognition of cybersecurity laws and regulations.

Factor - D 4.1: Legal and Regulatory Provisions

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Procedural Cybercrime Legislation	Specific procedural criminal law for cybercrime does not exist. It is not clear how general criminal procedural law applies to cybercrime investigations, prosecutions, and electronic evidence.	Development of specific procedural cybercrime legislation, or amendment of general procedural criminal law to adapt to cybercrime cases, has begun.	Comprehensive criminal procedural law containing provisions on the investigation of cybercrime and evidentiary requirements has been adopted and is applied. The country may have ratified regional or international instruments on cybercrime. The country consistently seeks to implement these measures into domestic law. Procedural laws relating to cybercrime permit the exchange of information (and other actions required) to support successful cross-border investigation of cybercrime.	Measures are in place to exceed minimal baselines specified in international treaties, where appropriate. The country seeks to adapt procedural cybercrime legislations to take account of emerging technologies and their use.	Procedural cybercrime law is constructed in a way that it can cater for dynamic changes in the underlying technology and threat environment, without the need for substantial and lengthy revision. The country is actively contributing to the promotion of effective procedural cybercrime legislation and instruments to improve international cybercrime investigations.
Human Rights Impact Assessment	Substantive and procedural cybercrime legislation and cybersecurity regulations may be in development, but no human rights impact assessments have been carried out.	Human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations may have been conducted, including consideration of privacy and freedom of expression implications. Some issues, however, have yet to be resolved. Relevant human rights experts have been consulted in the development of the legislation and regulation.	Full human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations have been completed and international standards are met. Implementation of this legislation is monitored on a regular basis for human rights compliance, and this is independently verified.	Human rights impact assessments are regularly reviewed to ensure that practice remains compatible with human rights requirements, and that the effect of emerging technologies is considered. Consideration has also been given to how cybersecurity can enhance human rights protection within the country and internationally.	The country is actively contributing to the development and promotion of human rights impact assessments as they relate to cybersecurity.

Factor - D 4.2: Related Legislative Frameworks

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Data Protection Legislation	Data protection legislation does not exist.	Data protection legislation is in development. Stakeholders from relevant sectors have been consulted to support the development of this legislation.	Comprehensive data protection legislation in line with international standards and best practice has been adopted and is enforced. A lead agency responsible for data protection has been designated.	The effectiveness of data protection legislation is regularly assessed and used to inform its development. The country seeks to adapt data protection laws to take account of emerging technologies and their use.	Data protection legislation is constructed so that it can cater for dynamic changes in the underlying technology and threat environment, without the need for substantial and lengthy revision. The country is developing and promoting international standards for data protection legislation. The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.
Child Protection Online	Legislation relating to child protection is limited and its application in the online environment is yet to be considered.	Legislation related to child protection is in place and is being adapted to reflect its application in the online environment. Stakeholders from relevant sectors have been consulted to support the development and adaptation of this legislation.	The application of child protection in the online environment is understood and reflected in relevant legislation. Legislation is implemented in line with international standards and best practice.	The effectiveness of online child protection law is regularly assessed and used to inform its development. The country seeks to adapt child protection law to take account of emerging technologies and their use.	Online child protection law is constructed so that it can cater for dynamic changes in the underlying technology and threat environment, without the need for substantial and lengthy revision. The country is developing and promoting international standards for online child protection law. The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.

Factor - D 4.2: Related Legislative Frameworks

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Consumer Protection Legislation	Legislation related to consumer protection is limited and its application in the online environment is yet to be considered.	Legislation related to consumer protection is in place and is being adapted to reflect its application in the online environment. Stakeholders from relevant sectors have been consulted to support the development of this legislation.	The application of consumer protection in the online environment is understood and reflected in relevant legislation. Legislation is implemented in line with international standards and best practice.	The effectiveness of online consumer protection law is regularly assessed and used to inform its development. The country seeks to adapt consumer protection legislation to take account of emerging technologies and their use.	Consumer protection legislation is constructed so that it can cater for dynamic changes in the underlying technology and threat environment, without the need for substantial and lengthy revision. The country is developing and promoting international standards for online consumer protection law. The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.
Intellectual Property Legislation	Legislation related to intellectual property protection is limited and its application in the online environment is yet to be considered.	Legislation related to intellectual property protection is in place and is being adapted to reflect its application in the online environment. Stakeholders from relevant sectors have been consulted to support the development of this legislation.	The application of intellectual property protection in the online environment is understood and reflected in relevant legislation. Legislation is implemented in line with international standards and best practice.	The effectiveness of online intellectual property protection law is regularly assessed and used to inform its development. The country seeks to adapt intellectual property protection legislation to take account of emerging technologies and their use.	Intellectual property legislation is constructed so that it can cater for dynamic changes in the underlying technology and threat environment, without the need for substantial and lengthy revision. The country is developing and promoting international standards for online intellectual protection law. The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.

Factor - D 4.3: Legal and Regulatory Capability and Capacity

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Law Enforcement	Law enforcement officers/ agencies do not have sufficient capacity to prevent and combat cybercrime and do not receive specialised training on cybercrime investigations.	Traditional investigative measures are applied to cybercrime investigations, but digital investigation capacity is limited. Law enforcement officers may receive training on cybercrime and digital evidence, but it is *ad hoc*.	A comprehensive institutional capacity with sufficient human, procedural and technological resources to investigate cybercrime cases has been established. Digital chain of custody and evidence integrity is established, including formal processes, roles and responsibilities. Standards for the training of law enforcement officers on cybercrime and digital evidence exist and are implemented. The respective roles of national and state/local law enforcement agencies are understood and state-/local-level forces are equipped to undertake their role.	Quantified risk assessments are used to allocate resources to operational cybercrime units (at national and state/local levels). Trends and statistics on cybercrime, law enforcement interventions and their impact on harm reduction are collected, analysed and used to inform strategy and long-term resource allocation decision. Law enforcement strategies include crime prevention measures alongside enforcement measures. Intelligence is used to support proactive investigation. Law enforcement agencies have the capabilities to maintain the integrity of data to meet international evidential standards in cross-border investigation.	The country is actively involved in the development of collaborative platforms between national law enforcement authorities. The law enforcement agencies within the country are at the forefront of developing new capabilities and approaches for the prevention and disruption of cybercrime and promoting their use internationally.
Prosecution	Prosecutors do not receive adequate training and resources to review electronic evidence or prosecute cybercrime. Consultation may have begun to consider this capacity in the prosecutor community.	A limited number of prosecutors have the capacity to conduct cybercrime cases and to handle electronic evidence, but this capacity is largely *ad hoc* and is not institutionalised. If prosecutors receive training on cybercrime and digital evidence, it is *ad hoc*.	A comprehensive institutional capacity, including sufficient human and technological resources, to prosecute cybercrime cases and cases involving electronic evidence is established. A specialist cadre of cybercrime prosecutors may have been established.	Institutional structures are in place, with a clear distribution of tasks and obligations within the prosecution services at all levels of the state. A mechanism exists that enables the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.	There is national capacity to prosecute complex domestic and cross-border cybercrime cases.

Factor - D 4.3: Legal and Regulatory Capability and Capacity

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Courts	There is no process to equip judges so they can preside over cybercrime cases or cases involving electronic evidence. Consultation may have begun to consider this capacity in the judicial community.	A limited number of judges have the capacity to preside over a cybercrime case, but this capacity is largely *ad hoc*. If judges receive training on cybercrime and digital evidence, it is *ad hoc*.	Sufficient human and technological resources are available to ensure effective and efficient legal proceedings regarding cybercrime cases and cases involving electronic evidence. Judges receive specialised training about cybercrime and electronic evidence. States/local courts are equipped to deal with cybercrime cases, appropriate to their level. Relevant courts are equipped to process civil litigation relating to cybersecurity liability.	The institutional capacity of the court system to conduct cybercrime cases is frequently reviewed and revised based on an assessment of effectiveness.	The country is actively involved in developing and promoting best practices in the conduct of cybercrime cases.
Regulatory Bodies	Sector-specific regulators have limited understanding of the potential impact of cyber on their regulated entities. There is no cross-sector regulatory body to supervise specific cybersecurity requirements.	Sector-specific regulators have started to establish their cybersecurity roles. A requirement for the establishment of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations may have been considered. Relevant stakeholders have been consulted in this process.	Sector-specific regulators (e.g.: finance, energy, transport) are equipped with the capability and resources required to oversee compliance with cybersecurity requirements within their sector. Where cross-sector regulatory bodies have been established to oversee cybersecurity, they have the necessary capability and resources to undertake their role.	The impact of regulatory actions on organisations' cybersecurity practices are regularly assessed and used to inform supervisory activity and regulation development. Regulatory bodies regularly assess emerging technologies and their potential impact on the cybersecurity of regulated entities. Regulatory interventions and investigations are informed by, and prioritised on the basis of, national assessments of cyber risk.	Regulatory bodies are actively involved in the development and promotion of regulatory best practice internationally.

Factor - D 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Law Enforcement Co-operation with Private Sector	Co-operation between domestic public and private sectors on cybercrime is limited. Specifically, co-operation between Internet service and other technology providers and law enforcement has not been established.	Exchange of information on cybercrime between domestic public and private sectors is *ad hoc* and unregulated. Specifically, *ad-hoc* co-operation between Internet service and other technology providers and law enforcement exists but is not always effective.	Information is regularly exchanged between domestic public and private sectors and is supported by appropriate legislation. Effective co-operation mechanisms between Internet service and other technology providers and law enforcement have been established as part of these broader public–private sector collaboration arrangements.	The effectiveness of public and private co-operation is regularly assessed and used to enhance collaborative processes. Collaboration frameworks are regularly adapted to take account of new technologies and emerging forms of cybercrime.	The country is actively contributing to the promotion of public–private partnership and the development of international public–private partnership platforms.
Co-operation with Foreign Law Enforcement Counterparts	There are minimal or no forms of international co-operation to prevent and combat cybercrime.	Formal mechanisms of international law enforcement co-operation may exist, but their application to cybercrime is *ad hoc* or only possible in some cases. Law enforcement is not formally integrated into regional and international cybercrime networks.	Formal mechanisms of international law enforcement co-operation have been established to facilitate the detection, investigation, and prosecution of cybercrime. Mutual legal assistance, extradition agreements and mechanisms have been established and are applied to cybercrime cases. Domestic law enforcement agencies are integrated with regional and international networks, such as Interpol or 24/7 networks.	Law enforcement agencies work jointly with foreign counterparts, potentially through joint task forces, resulting in successful cross-border cybercrime investigations and prosecutions.	The country actively contributes to the promotion and development of international co-operation mechanisms.
Government-Criminal Justice Sector Collaboration	There is minimal interaction between government and criminal justice actors.	Exchange of information between government and criminal justice actors is limited and *ad hoc*.	Formal relationships between government and criminal justice actors have been established, resulting in the regular exchange of information on cybercrime issues.	The relationship between government actors, prosecutors, judges and law enforcement agencies is regularly assessed and used to enhance their effectiveness.	The country actively contributes to the international promotion of efficient and timely exchange of information between government and criminal justice actors.

Dimension 5: Standards and Technologies

This *Dimension* addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The *Dimension* specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

Factor
D 5.1: Adherence to Standards

This *Factor* reviews the government's capacity to promote, assess implementation of, and monitor compliance with international cybersecurity standards and good practices.
> Navigate to Factor

Aspects

- **ICT Security Standards:** this *Aspect* examines whether cybersecurity-related standards and good practices are being adhered to and implemented widely across the public sector and CI organisations;
- **Standards in Procurement:** this *Aspect* addresses the implementation of standards and good practices in all sectors to guide procurement processes, including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services; and
- **Standards for Provision of Products and Services:** this *Aspect* addresses the use of standards and good practices by local suppliers of goods and services, including software, hardware, managed services, and cloud services.

Factor
D 5.2: Security Controls

This *Factor* reviews evidence regarding the deployment of security controls by users and public and private sectors, and whether the technological cybersecurity control set is based on established cybersecurity frameworks.
> Navigate to Factor

Aspects

- **Technological Security Controls:** this *Aspect* explores to what extent up-to-date technological security controls, including patching and backups, are deployed in all sectors; and
- **Cryptographic Controls:** this *Aspect* reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up to date.

Factor
D 5.3: Software Quality

This *Factor* examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this Factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the critical nature of services.
> Navigate to Factor

Aspects

- **Software Quality and Assurance:** (as above)

Factor
D 5.4: Communications and Internet Infrastructure Resilience

This *Factor* addresses the existence of reliable Internet services and infrastructure in the country, as well as rigorous security processes across private and public sectors. Also, this Factor reviews the control that the government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.
> Navigate to Factor

Aspects

- **Internet Infrastructure Reliability:** this *Aspect* examines the reliability and protection of Internet services and infrastructure in public and private sectors; and
- **Monitoring and Response:** this *Aspect* examines whether mechanisms are in place to conduct risk assessments and monitor network resilience in both public and private sectors.

Factor
D 5.5: Cybersecurity Marketplace

This *Factor* addresses the availability and development of competitive cybersecurity technologies, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.
> Navigate to Factor

Aspects

- **Cybersecurity Technologies:** this *Aspect* examines whether a national market for cybersecurity technologies is in place and supported, and informed by national need;
- **Cybersecurity Services and Expertise:** this *Aspect* explores the availability of cybersecurity consultancy services for private and public organisations;
- **Security Implications of Outsourcing:** this *Aspect* examines whether risk assessments are conducted to determine how to mitigate the risks of outsourcing IT to a third party or cloud services; and
- **Cyber Insurance:** this *Aspect* explores the existence of a market for cyber-insurance, its coverage, and products suitable for various organisations.

Factor
D 5.6: Responsible Disclosure

This *Factor* explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors, and whether there is sufficient capacity to continuously review and update this framework.
> Navigate to Factor

Aspects

- **Sharing Vulnerability Information:** this *Aspect* explores existing information-sharing mechanisms or channels on the technical details of vulnerabilities among the stakeholders; and
- **Policies, Processes and Legislation for Responsible Disclosure of Security Flaws:** this *Aspect* explores the existence of a responsible-disclosure policy or framework in public- and private-sector organisations and the right to legal protections for those disclosing security flaws.

Factor - D 5.1: Adherence to Standards

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
ICT Security Standards	Either no standards or good practices have been identified for use in securing data, technology or infrastructure, by the public and private sectors. Or initial identification of some appropriate standards and good practices has been made by the public and private sectors, and possibly some *ad-hoc* implementation, but no concerted endeavour to implement or change existing practice in a measurable way.	Information risk management standards have been identified for use and there have been some initial signs of promotion and take-up within public and private sectors. There is some evidence of measurable implementation and use of international standards and good practices.	A nationally-agreed baseline of cybersecurity-related standards and good practices have been identified and implemented widely across public and private sectors. An entity within government exists to assess the use of standards across public and private sectors. Government schemes exist to promote continued enhancements, and metrics are being applied to monitor compliance. Consideration is being given as to how standards and best practices can be used to address risk within supply chains within the CI, by both government and CI.	Government and organisations promote use of standards and best practices according to assessment of national risks and budgetary choices. The choice of standards and best practices and their implementation is continuously revised. Emerging cybersecurity risks are regularly assessed and used to re-evaluate the need for additional ICT security standards. There is evidence of debate between government and other stakeholders as to how national and organisational resource decisions should align and drive implementation of standards. Evidence of contribution to international standards' bodies exists and contributes to thought leadership and sharing of experience by organisations.	The country is actively involved in the development and promotion of defined standards internationally. Implementation of standards and non-compliance decisions are made in response to changing threat environments and resource drivers across sectors and CI, through collaborative risk management. Evidence exists of debate within all sectors on compliance to standards and best practices, based on continuous needs assessments.

Factor - D 5.1: Adherence to Standards

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Standards in Procurement	No standards or best practices have been identified for use in guiding procurement processes by the public and private sectors. If they are recognised, implementation is *ad hoc* and un-co-ordinated.	Cybersecurity standards and best practices guiding procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services) have been identified for use. Evidence of promotion and implementation of cybersecurity standards and best practices in defining procurement practices exists within public and private sectors.	Cybersecurity standards and best practices in guiding procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services) are being adhered to widely within public and private sectors. Implementation and compliance of standards in procurement practices within the public and private sectors is evidenced through measurement and assessments of process effectiveness.	Organisations have the ability to monitor and change use of standards and best practices in procurement processes, support deviations and non-compliance decisions as the need arises through risk-based decision-making. Emerging cybersecurity risks are regularly assessed and used to re-evaluate the need for additional standards in procurement. Critical aspects of procurement and supply, such as total lifecycle cost, quality, inter-operability, maintenance, support and other value-adding activities, are continuously improved, and procurement process improvements are made in the context of wider resource planning. Organisations are able to benchmark the skills of their procurement professionals against the competencies outlined in procurement standards and identify any skills and capability gaps.	The country is actively involved in the development and promotion of these standards internationally. Implementation of standards in procurement processes and non-compliance decisions are made in response to changing threat environments.
Standards for Provision of Products and Services	Either no standards or best practices have been identified for use in securing the products and services (in particular, software, hardware, managed services and cloud services) developed or offered by providers in the country. Or there is some identification, but only limited evidence of take-up.	Core activities and methodologies for secure development and lifecycle management for software, hardware and provision of managed services and cloud services are being identified and discussed within professional communities. Government promotes relevant standards in software development, hardware quality assurance, provision of managed services and cloud security but there is no evidence of widespread adoption of these standards yet.	There is evidence of widespread implementation of standards in the software development processes, hardware quality assurance, provision of managed services and cloud services by public and private sector organisations. Government has an established programme for promoting and monitoring standard adoption in software development, hardware quality assurance and cloud security, for public and commercial systems. Evidence that high integrity systems and software development techniques are present within the educational and training offerings in the country.	Security considerations are incorporated in all stages of the development of software, hardware and provision of managed services and cloud services. Core development activities, including configuration and documentation management, security development and lifecycle planning have been adopted into the practices of product and service providers Projects on software development, hardware quality assurance, managed service and cloud security continuously assess the value of standards and reduce or enhance levels of compliance according to risk-based decisions.	The country is actively involved in the development and promotion of these standards internationally. Implementation of these standards and non-compliance decisions are made in response to changing threat environments.

Factor - D 5.2: Security Controls

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Technological Security Controls	There is minimal or no understanding or deployment of the technological security controls available in the marketplace, by users and public and private sectors. Internet service and other technology providers may not offer any upstream controls to their customers.	Technological security controls are deployed by users and public and private sectors, but possibly not consistently across all sectors. The deployment of up-to-date technological security controls is promoted in an *ad-hoc* manner and all sectors are being incentivised to make use of them. Internet service and other technology providers may be offering security services as part of their services but possibly in an *ad-hoc* manner. Internet service and other technology providers recognise a need to establish internal policies for the deployment of technical security controls, to manage identified risks in the products and services they are offering.	Up-to-date technological security controls, including patching and backups, are deployed in all sectors. Physical security controls are used to prevent unauthorised personnel from entering computing facilities in all sectors. Internet service and other technology providers establish internal policies for the deployment of technical security controls, to manage identified risks in the products and services they are offering. The technological cybersecurity control set reflects internationally-established cybersecurity frameworks, standards and good practice.	Widespread adoption of technological security controls leads to effective upstream protection of users and public and private sectors. All sectors have the capacity to continuously assess the security controls deployed, for their effectiveness and suitability according to their changing needs. The understanding of the technological security controls being deployed extends to their impact on organisational operations and budget allocation. The public and private sectors have the capacity to critically assess and upgrade cybersecurity controls according to their appropriateness and suitability for use, and considering emerging risks. There is widespread adoption of multi-factor authentication for online services and privileged accounts. Certificate Authorities are available and digital certificates are widely used. Internet service and other technology providers have the ability to prevent access to non-trusted sites or web addresses in accordance with the requirements of the appropriate regulator.	The application of advanced technological controls within the country is a leading influence internationally. Implementation of advanced technological security controls are made in response to changing threat environments.

Factor - D 5.2: Security Controls

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Cryptographic Controls	Cryptographic techniques (e.g.: encryption and digital signatures) for protection of data at rest and data in transit may be a concern but are not yet deployed within the government or private sector, or by the general public.	Cryptographic controls for protecting data at rest and in transit are recognised and deployed *ad hoc* by multiple stakeholders and within various sectors. Tools, such as TLS*, are deployed *ad hoc* by service providers to secure all communications between servers and users.	Cryptographic techniques are available for all sectors and users for the protection of data at rest or in transit. There is a broad understanding of secure communication services, such as encrypted or signed email. The cryptographic controls deployed meet international standards and guidelines for each sector and are kept up to date. Tools, such as TLS are routinely deployed by service providers to secure all communications between servers and users.	The public and private sectors critically assess the deployment of cryptographic controls, according to their objectives and priorities. The public and private sectors adapt encryption and cryptographic control policies based on the evolution of technological advancement and changing threat environment. The public and private sectors have developed encryption and cryptographic control policies based on the previous assessment, and regularly review the policies for effectiveness. The country has considered implementing digital-identity management. The country has considered whether it requires a national PKI**.	The country is contributing to the international debate around best practice on cryptographic controls. Implementation of cryptographic controls are made in response to changing threat environments.

* Transport Layer Security
** Public Key Infrastructure

Factor - D 5.3: Software Quality

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Software Quality and Assurance	Quality and performance of software used in the country is a concern, but functional requirements are not yet fully monitored. A catalogue of assured software platforms and applications within the public and private sectors does not exist. Policies and processes regarding updates and maintenance (including patch management) of software applications have not yet been formulated.	Software quality and functional requirements in public and private sectors are recognised and identified, but not necessarily in a strategic manner. A catalogue for assured software platforms and applications within the public and private sectors is in development. Policies and processes on software updates and maintenance (including patch management) are now in development. Evidence of software quality deficiencies is being gathered and assessed regarding its impact on usability and performance.	Software quality and functional requirements in public and private sectors are recognised and established. Reliable software applications that adhere to international standards and good practices are being used widely in the public and private sectors. Policies on and processes for software updates and maintenance (including patch management) are established in all sectors. Software applications are characterised as to their reliability, usability and performance in adherence to international standards and good practices.	Quality of software used in public and private sectors is monitored and assessed. Policies and processes on software updates and maintenance (including patch management) are being improved, based on risk assessments and the critical nature of services in all sectors. Benefits to businesses from additional investment in ensuring software quality and maintenance are measured and assessed. Software defects are manageable in a timely manner and service continuity is ensured.	Software applications of high-level performance, reliability and usability are available, with service continuity processes fully automated. Requirements of software quality are being systematically reviewed, updated, and adapted to the changing cybersecurity environment.

Factor - D 5.4: Communications and Internet Infrastructure Resilience

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Internet Infrastructure Reliability	Affordable and reliable Internet services and infrastructure in the country may not have been established; if they have been, adoption rates of those services are a concern. There is little or no national oversight of network infrastructure. If networks and systems are outsourced, the reliability of third-party providers may not have been considered. Network redundancy measures may be considered, but not in a systematic, comprehensive fashion.	Limited Internet services and infrastructure are available, but with low levels of adoption and issues of unreliability. The ability of Internet infrastructure in public and private sectors to withstand incidents with minimum disruption has been discussed by multiple stakeholders but may not have been fully addressed. Support for securing Internet infrastructure may rely on regional assistance.	Reliable Internet services are widely available and used. Internet services are trusted widely for conducting e-commerce and electronic business transactions; appropriate authentication processes are established. Technology deployed and processes used for managing Internet infrastructure meet international standards and follow good practices. National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.	Regular assessments are made of technology, of processes for compliance with international standards, and of guidelines that address the national need in the face of emerging risks, and changes are made as required. There is effective and controlled acquisition of critical technologies, and there are managed strategic planning and service continuity processes in place.	Acquisition of infrastructure technologies is effectively controlled, with flexibility incorporated according to changing market dynamics. Costs for infrastructure technologies are continually assessed and optimised. Scientific, technical, industrial and human capabilities are being systematically maintained, enhanced, and perpetuated in order to maintain the country's independent resilience. Optimised efficiency is in place to mediate extended outages of systems.
Monitoring and Response	No risk assessments are conducted by Internet infrastructure owners to identify vulnerable assets and prioritise protective actions. There is no monitoring in place to detect that incidents have occurred. No incident response plans are in place.	Processes on developing risk assessments for Internet infrastructure owners have been initiated. There is *ad-hoc* monitoring of parts of the Internet infrastructure, but it may not be comprehensive. Incident response plans are in development in some sectors.	Mechanisms are in place in both public and private sectors to conduct risk assessments, monitor and test network resilience, and to respond to incidents. Incident response plans are in place in both public and private sectors and are regularly tested and kept under review. Appropriate resources are allocated to hardware integration, technology stress testing, personnel training, monitoring, response, and drills to test response plans.	Risks related to emerging and converging technologies are regularly assessed by Internet Infrastructure owners. Risks related to emerging and converging technologies are regularly assessed by regulatory agencies responsible for electronic communications networks and this is used to inform funding and priority decisions.	National-level assets can act to work with the international community in the event of a trans-jurisdictional crisis or incident. Lessons learnt from international collaborations are used to evolve monitoring and response capabilities. Evidence exists that sovereign novel monitoring and response capabilities are being developed in anticipation of emerging threats.

Factor - D 5.5: Cybersecurity Marketplace

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Cybersecurity Technologies	If domestic production of cybersecurity technologies exists, it does not follow secure processes. The country has not considered the security implications of using foreign cybersecurity technologies.	If there is domestic production, the need for secure processes is recognised. If there is reliance on foreign technologies, the security implications are considered.	If there is domestic production, secure processes are in place. If there is reliance on foreign technologies, the security implications are identified and mitigated in the context of an international supply chain.	If there is local development of cybersecurity technology, it abides by secure coding guidelines, good practices and adheres to internationally-accepted standards. Risk assessments and market incentives inform the prioritisation of product development and mitigation of identified risks. The security implications of using foreign technologies are routinely analysed and revised based on the assessment of emerging cybersecurity risks.	Security functions in software and computer system configurations are automated in the development and deployment of technologies. Domestic cybersecurity products are exported to other nations and are considered superior products. The country has established a body to assure the security of foreign technologies (devices and software) and supply chains, or to certify entities which can do this.
Cybersecurity Services and Expertise	Cybersecurity consultancy services are not widely on offer in the country. Few if any service providers have professional certification.	There are a growing number of cybersecurity consultancy services available for private and public organisations. A growing number of service providers provide detail of the professional certifications they possess. There may be limited or no guidance to assist organisations with the selection of service providers.	There are widespread cybersecurity consultancy services available for private and public organisations. All service providers provide details of the professional certifications they possess. A national body accredits service providers, to assist organisations in selecting service providers.	Private and public organisations routinely seek advice from cybersecurity consultancy services, including advice about emerging risks. There is an adequate supply of cybersecurity professionals in the country.	The cybersecurity service sector in the country helps shape the international market.

Factor - D 5.5: Cybersecurity Marketplace

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Security Implications of Outsourcing	No risk assessments are conducted to determine how to mitigate the risks of outsourcing IT to a third party or cloud services. There is a lack of understanding of the security measures that the outsourced IT service provider applies.	Some organisations and sectors conduct risk assessments to determine how to mitigate the risks of outsourcing IT to a third party or cloud services. At least some organisations and sectors understand the security measures that the outsourced IT service provider applies. At least some organisations have developed business continuity and disaster recovery processes.	Most major organisations from the public and private sectors conduct risk assessments to determine how to mitigate the risks of outsourcing IT to a third party or cloud services. There is widespread understanding of the security guarantees provided by the outsourced IT service providers. Most organisations have developed and tested processes to support business continuity and disaster recovery.	Insights arising from risk assessments are routinely analysed in order to establish and promote cybersecurity best practices to mitigate the risk of outsourcing IT. Different risk scenarios with the IT service provider are explored and tested, including emerging risks.	The country is contributing to international best practice on how to mitigate the risk of outsourcing IT.
Cyber Insurance	The need for a cyber-insurance market may have been identified, but no products and services are widely available, either domestically or from external providers.	The need for a market in cyber-insurance has been identified through the assessment of financial risks for the public and private sectors, and the appropriateness of available offerings is now being discussed.	A market for cyber-insurance is established and encourages the sharing of threat- information among participants of the market. Products suitable for small and medium-sized enterprises (SMEs) are also on offer.	Cyber-insurance market offers a variety of covers to mitigate consequential losses. Cover is selected by organisations based on strategic planning needs and identified risk. The cyber-insurance market is innovative and adapts to emerging risks, standards and practices, while addressing the full scope of cyber harm. Insurance premium reductions are offered for consistent cyber-secure behaviour.	Cyber-insurance practices in the country help to shape the international market.

Factor - D 5.6: Responsible Disclosure

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Sharing Vulnerability Information	There is no informal way of sharing information among the stakeholders about the technical details of vulnerabilities. Software and service providers generally lack the ability to address bug and vulnerability reports.	Technical details of vulnerabilities are shared informally with other stakeholders which can distribute the information more broadly. Software and service providers are able to address bug and vulnerability reports but there may not be formal protocols for doing so.	There are formal information-sharing mechanisms or channels in place to share the technical details of vulnerabilities with other stakeholders, which can distribute the information more broadly. A substantial proportion of vulnerabilities in products and services are remedied within defined deadlines after their discovery.	Vulnerability information-sharing mechanisms are continuously reviewed and updated based on the needs of all affected stakeholders, and in the light of emerging risks. All affected products and services are routinely updated within defined deadline. Processes are in place to review and reduce deadlines where possible.	The country is contributing to the debate and international best practice on the sharing of vulnerability information.
Policies, Processes and Legislation for Responsible Disclosure of Security Flaws	The need for a responsible-disclosure policy in public and private sector organisations, and the right to legal protections for those disclosing security flaws are not yet acknowledged.	The need for a responsible-disclosure policy in public and private sector organisations is recognised but policies or processes may not be in place, or may only be in development. The right to legal protections for those disclosing security flaws is recognised but legislation may not be in place; or may only be in development. Software and service providers commit to refraining from taking legal action against a party disclosing information responsibly.	A responsible-disclosure policy or framework is in place in public and private sector organisations, and includes a disclosure deadline, scheduled resolution, and the need for acknowledgement. Organisations have established processes to receive and disseminate vulnerability information responsibly. The right to legal protections for those disclosing security flaws responsibly is in place.	Responsible-disclosure policies and processes are continuously reviewed and updated based on the needs of all affected stakeholders and in the light of emerging risks. An analysis of the technical details of vulnerabilities is published and advisory information is disseminated according to individual roles and responsibilities.	The country is contributing to the debate on responsible-disclosure frameworks and legal protections for those disclosing security flaws responsibly.

Evolution of the CMM

This *CMM 2021 Edition* builds on the success of the model over the last six years by considering the changing cyber threat to users, the lessons learned from more than 120 CMM reviews undertaken around the world, and the feedback from cybersecurity experts.

The decision to revise the CMM was informed by two key factors:

- The need to respond to all pertinent aspects of threat, systems vulnerabilities and consequential harm due to changing operational environments and risks; and
- Re-assessment of the changing cybersecurity control landscape and risk management practices available to the community.

To determine whether or not to propose a change to the CMM, or to the evidence required to justify an attainment of capacity maturity, the following decision process was followed.

All potential changes to be included in the *CMM 2021 Edition* had to meet the following criteria:

- Each change must have been proposed by partners, users, or expert advisors. It must be based on experience in deploying the model, feedback from a country which has used the model or from a member of the international stakeholder community with particular insight into changing environments that need be taken into account;
- The change must have been discussed with the GCSCC Expert Advisory Panel, regional, strategic and implementation partners and other experts during the online conference calls and/or one-to-one online meetings. Clear consensus must have been reached amongst the attendees;
- The change must have been discussed at the CMM Revision Workshop in February 2020. Clear consensus must have been reached amongst attendees;
- Global Constellation partners and strategic and implementation partners must have been consulted; and
- Members of the GCSCC Technical Board must agree that the changes are desirable.

Those criteria that did not meet the requirements were documented as requiring further research and consultation.

Acknowledgements

This *CMM 2021 Edition* was developed by the GCSCC with significant contributions by its partners and collaborators:

GCSCC Technical Board

GCSCC Research Team

GCSCC Expert Advisory Panel

Global Constellation Partners

- Cybersecurity Capacity Centre for Southern Africa (C3SA), Cape Town, South Africa
- Oceania Cyber Security Centre (OCSC), Melbourne, Australia

Strategic and Implementation Partners

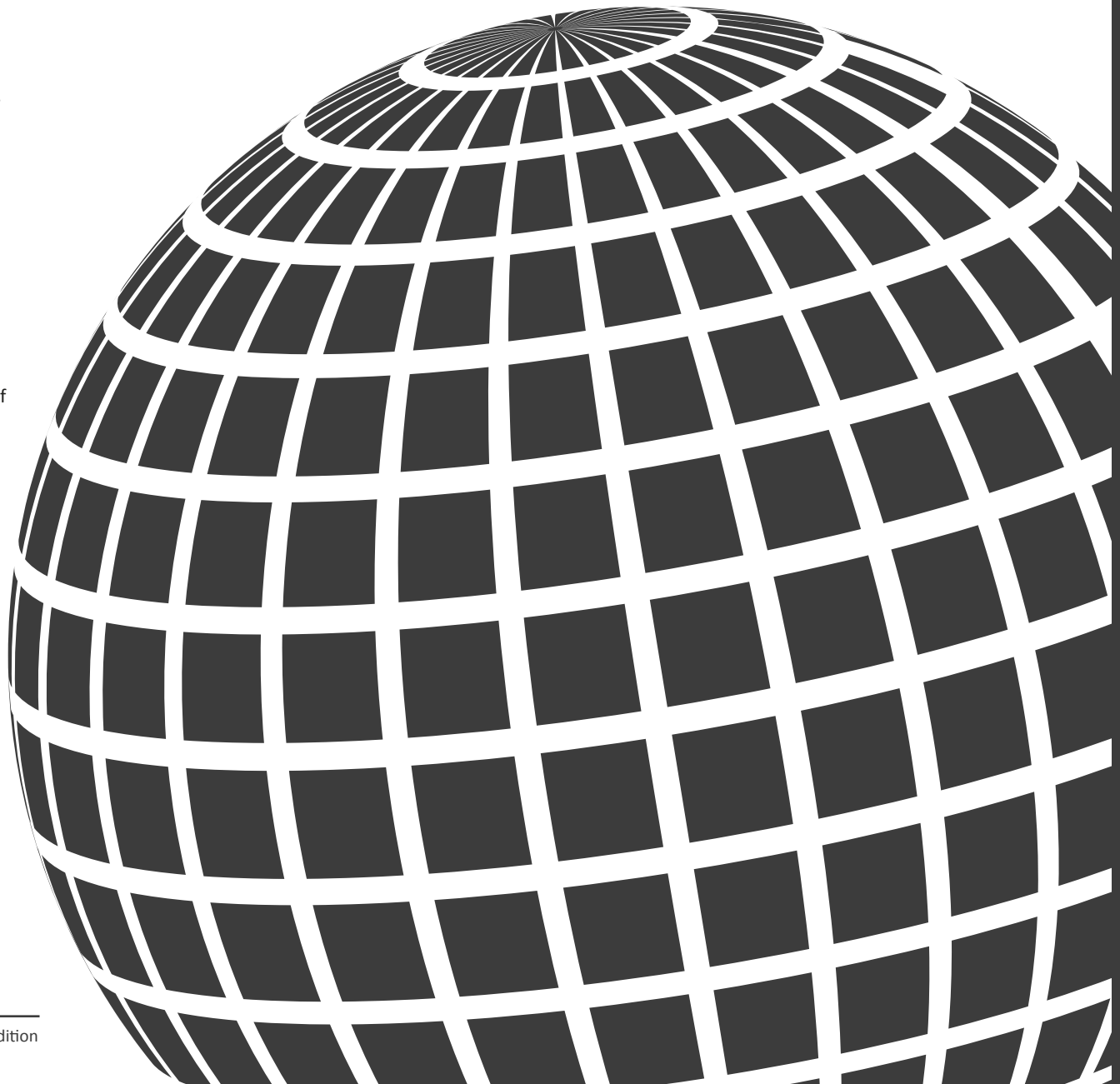
- Commonwealth Telecommunications Organisation (CTO)
- Global Forum on Cyber Expertise (GFCE)
- International Telecommunication Union (ITU)
- NRD Cyber Security
- Organization of American States (OAS)
- World Bank

More than 150 individuals contributed to different steps of the revision process, too many to list them all. We would like to thank all of them.

We also would like to thank our research funders and our partners who provided in-kind support: the UK Foreign, Commonwealth and Development Office (FCDO), State Government of Victoria (Australia), the Organization of American States (OAS), the Inter-American Development Bank (IDB), the World Bank, the International Telecommunications Union (ITU), the Commonwealth Telecommunication Organisation (CTO), the Global Forum on Cyber Expertise (GFCE), the Norwegian Ministry of Foreign Affairs, the Ministry of Foreign Affairs of the Netherlands, GIZ (the German agency for international co-operation), and NRD Cyber Security.

About the GCSCC

The Global Cyber Security Capacity Centre (GCSCC), a programme of the Oxford Martin School and based at the Department of Computer Science of the University of Oxford, is a leading international centre for research on efficient and effective cybersecurity capacity-building. It promotes an increase in the scale, pace, quality and impact of cybersecurity capacity-building initiatives across the world and aims to improve the scale and effectiveness of cybersecurity capacity-building by gaining a more comprehensive and nuanced understanding of the cybersecurity capacity landscape. The goal of the GCSCC is to ensure that the knowledge and research collected and produced by the centre can assist nations to improve their cybersecurity capacities in a systematic and substantive way. By helping in the understanding of national cybersecurity capacity, the GCSCC hopes to help promote an innovative cyberspace in support of well-being, human rights and prosperity for all.



Global
Cyber Security
Capacity Centre

Global Cyber Security Capacity Centre
Department of Computer Science, University of Oxford
Wolfson Building
Parks Road
Oxford
OX1 3QD
United Kingdom

Tel: +44 (0)1865 287430
Email: cybercapacity@cs.ox.ac.uk
Web: https://gcscc.ox.ac.uk/ and https://www.oxfordmartin.ox.ac.uk/cyber-security/

March 2021