Global Cyber Security Capacity Centre

Cybersecurity Capacity Maturity Model for Nations (CMM)

Revised Edition

Global Cyber Security Capacity Centre

University of Oxford

3/31/2016

Executive Summary

The goal of the Global Cyber Security Capacity Centre (Capacity Centre) is to increase the scale and effectiveness of cybersecurity capacity-building, both within the UK and internationally by gaining a more comprehensive and nuanced understanding of the cybersecurity capacity landscape. It is our aim to ensure that the knowledge and research collected and produced by the Capacity Centre can assist nations improve their cybersecurity capacity in a systematic and substantive way. By helping understand national cybersecurity capacity, the Capacity Centre hopes to help promote an innovative cyberspace in support of well-being, human rights and prosperity for all.

In order to achieve this aim, the Capacity Centre developed its prototype National Cybersecurity Capacity Maturity Model in 2014, and deployed it in 2015 during 11 national cybersecurity capacity reviews, as well as a regional assessment of the Latin American and Caribbean Region (led by the Organization of American States in collaboration with the Inter-American Development Bank). The reviews were conducted alongside several international organisations and leading ministries, and convened stakeholders from across all sectors of society in order to gain a comprehensive understanding of the maturity of cybersecurity capacity of the nation. During the reviews, the Capacity Centre was able to gauge whether the content of CMM is consistent with the cybersecurity capacity landscape, as well as determine ways to enhance the overall content, structure and deployment of the CMM through lessons learnt.

Therefore, the Capacity Centre has developed a revised edition of the CMM, based on the lessons learnt through the deployment of the model. The Capacity Centre proposed a series of modifications based on the lessons learnt to a panel of cybersecurity experts from various disciplines. These expert consultations confirmed several proposed amendments, and produced additional inputs for consideration in the revision of the CMM. Once the amended content was curated by senior academics leading the development of the respective cybersecurity capacity dimensions, the revised edition of the CMM was produced.

Most of the alterations that have been made in the revised edition of the CMM are structural rather than substantial. Certain factors and aspects have been combined or reconfigured to improve the clarity and precision of the model as a whole, while ensuring the continuity of the content. For example, in Dimension 3, several review participants expressed confusion regarding the differences between factors, which resulted in a reconfiguration of this dimension in order to more clearly communicate the intention of each factor. Other revisions, such as adding factors to certain dimensions, were made to ensure the essence of the cybersecurity capacity dimensions is more accurately reflected. In Dimension 5, in particular, several new factors were added so that the focus of the dimension is drawn toward technical standards, controls and products rather than the existing ambiguous scope. Finally, some factors were added as a direct result of feedback from the various country reviews, such as the addition of a factor on the role of media in Dimension 2 and a factor on international cooperation in Dimension 4.

This effort to enhance the content of the CMM is not intended to be a static exercise. As the Capacity Centre continues to deploy the model across the world, new lessons will be learnt that can be used to further enhance the CMM. Our aim is to ensure the CMM remains applicable to all national contexts and reflects the global state of cybersecurity capacity maturity.

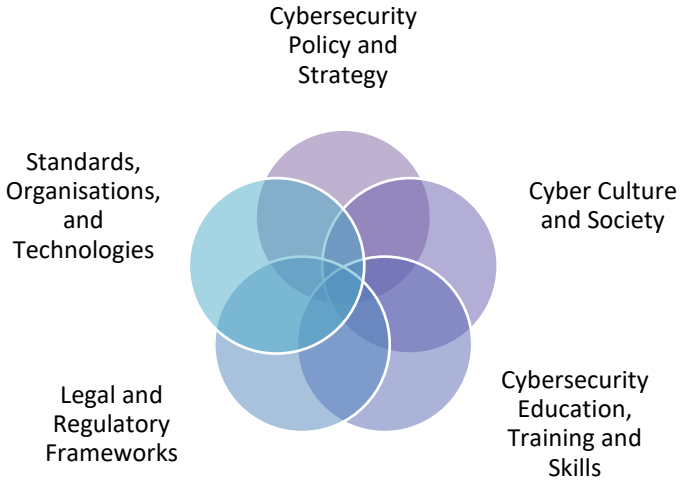
Table of Contents

I. Introduction

The goal of the Global Cyber Security Capacity Centre (Capacity Centre) is to increase the scale and effectiveness of cybersecurity capacity-building, both within the UK and internationally through the deployment of the Cybersecurity Capacity Maturity Model (CMM). The Capacity Centre will make this knowledge available to governments, communities and organisations to help increase their cybersecurity capacity. By helping increasing national cybersecurity capacity the Capacity Centre hopes to help promote an innovative cyberspace in support of well-being, human rights and prosperity for all.

We currently consider cybersecurity capacity to comprise five dimensions:

1. Devising cybersecurity policy and strategy;
2. Encouraging responsible cybersecurity culture within society;
3. Developing cybersecurity knowledge;
4. Creating effective legal and regulatory frameworks; and
5. Controlling risks through standards, organisations and technologies.

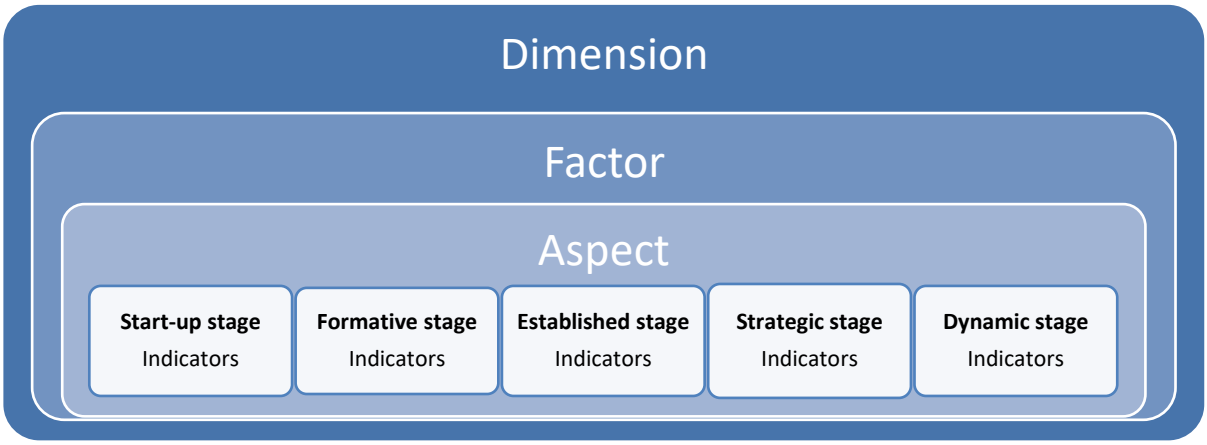


These five dimensions cover the broad expanse of areas that should be considered when seeking to enhance cybersecurity capacity. We recognise that these dimensions may overlap with one another on certain issues, and indeed the Capacity Centre hopes to understand the interdependences between cybersecurity capacities as it conducts more national capacity reviews. Within each dimension, there are several factors, aspects, stages of maturity, and indicators of cybersecurity capacity, each of which is defined as follows:

- **Dimension**: The 5 dimensions represent the clusters of cybersecurity capacity through which the Capacity Centre analyses the nuances of capacity. They represent the different research 'lenses' through which cybersecurity capacity is studied. Accordingly, the most fundamental structure of the CMM is divided into dimensions, which consist of a number of factors.
- **Factor**: Within the 5 dimensions, factors describe what it means to possess cybersecurity capacity. They are elements that contribute to the enhancement of cybersecurity capacity maturity, and the complete list of factors seeks to holistically incorporate all elements of the cybersecurity capacity landscape, though we recognise that this list may need to be adapted based on lessons learnt in reviews. Most factors are composed of a number of aspects that structure the factor's content (indicators) into more concise parts, while some factors that are more limited in scope do not have specific aspects.

- **Aspect**: Each factor is then presented as a number of aspects, which represent different components of the factor. Aspects represent 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. Each aspect is composed of a series of indicators within 5 stages of maturity.
- **Stage**: Stages define to which degree a country has progressed in relation to a certain factor/aspect of cybersecurity capacity. The CMM consists of 5 distinct stages of maturity (defined on page 6), that serve as a snapshot of 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 move towards higher cybersecurity capacity maturity.
- **Indicator**: Indicators represent the most elemental part of CMM's structure. Each indicator describes the steps, actions, or building blocks that are indicative of a specific stage of maturity within a distinct aspect, factor and dimension. 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 they have fulfilled the indicator criteria, or they cannot provide such evidence. In order for a country to enhance its maturity within a given aspect of factor, the fulfilment of every indicator needs to evidenced, otherwise they country cannot progress to the following stage.

The preceding terms are layered as follows:



Below is a template for how the factors, aspects, and indicators are visualised in each dimension of the CMM:

D X.X: Factor Title					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Aspect A	Indicator 1 Indicator 2 Indicator 3	Indicator 4 Indicator 5	Indicator 6 Indicator 7 Indicator 8	Indicator 9 Indicator 10 Indicator 11	Indicator 12 Indicator 13
Aspect B	Indicator 1 Indicator 2	Indicator 3 Indicator 4 Indicator 5	Indicator 6 Indicator 7	Indicator 8 Indicator 9 Indicator 10	Indicator 11 Indicator 12

In order to determine to what stage of maturity particular indicators belong, each stage has been characterised as follows:

- **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 is an absence of observable evidence at this stage.

- **Formative:** Some features of the aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.

- **Established:** The elements of the aspect are in place, and 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 organization's particular circumstances.

- **Dynamic:** At this stage, there are clear mechanisms in place to alter 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). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this stage.

The CMM allows the review of current national cybersecurity capacity maturity. In each case, understanding the requirements to achieve higher levels of capacity should directly indicate areas requiring further investment, and the data required to evidence such capacity levels. This means that the CMM could also be used to build business cases for investment and expected performance enhancements.

II. Development of the Cybersecurity Capacity Maturity Model

a. Selection of Cybersecurity Capacity-Building Factors

In developing the first iteration of the model in 2014, the Capacity Centre began the process of selecting factors contributing to building capacity in cybersecurity through exhaustive exploration into various disciplines. This search sought to gather as much publically available material on cybersecurity capacity-building as possible, in order not to miss relevant material and reduce the risk of duplicating efforts conducted by other institutions. Therefore, the Capacity Centre researched, assessed, and analysed cybersecurity capacity-building factors from several organisations from around the world.

This process sought to ensure that the CMM developed by the Capacity Centre is as scientifically rigorous as possible. Such factors include, but are not limited to, content produced by: the International Telecommunications Union (ITU), the European Network and Information Security Agency (ENISA), Hathaway Global Strategies LLC., the National Institute of Standards and Technologies (NIST), the Economist Intelligence Unit (EIU), the Organization for Economic Co-Operation and Development (OECD), the Australian Strategic Policy Institute (ASPI), and the World Economic Forum (WEF). These organisations (among others) have all conducted significant research into various factors contributing to cybersecurity capacity-building. The Capacity Centre acknowledges the importance of these initiatives in the development of the CMM. In addition, in order to collect as diverse and credible input as possible, the Capacity Centre consulted with various stakeholders with diverse geographic, organisational and disciplinary perspectives. These stakeholders are all regarded as experts in their respective fields, which encompass the five dimensions of cybersecurity capacity identified by the Capacity Centre. Stakeholders routinely contributed to the collection of cybersecurity capacity-building material.

Once the initial broad collection of factors had been completed, the Capacity Centre proceeded to prioritise these factors based on a defined methodology. Prioritisation was deemed necessary in order to prevent an over-abundance of information during the deployment phase. In order to conduct this prioritisation, the Capacity Centre developed a survey which proposed the following questions:

- **CATEGORISATION:** To what extent do you believe that this should be a primary factor within one of the five dimensions (as opposed to a consideration that serves as an aspect of a factor)?
- **EVIDENCE:** To what extent do you believe it is impossible/easy to gather evidence to demonstrate that a nation state or other organisation possesses this capability (i.e. is it measurable or demonstrable in an observable way)?
- **VALIDATION:** How scientifically robust do you believe measures of this factor could be?
- **POTENTIAL:** Do you agree that this factor should be included in the Cybersecurity Capacity Maturity Model, assuming supporting data could be acquired?
- **RELEVANCE:** How important is this factor to the future development of cybersecurity capacity?

This survey was completed by several of the stakeholders previously mentioned. The Capacity Centre collected the responses for all of the participants in the survey in order to create an average score for all results in each dimension of capacity, and then took the average of each factor across all five questions, which produced a single score for every factor. These average scores per factor served as our base for prioritisation. The Capacity Centre decided to use the third quartile as its benchmark for highest priority factors, as this produced both an operational number of factors and is an objective standard for selection. By comparing each score against the baseline, and accounting for overlap between different dimensions, the factors for inclusion were selected.

However, before the CMM could be converted into a tool for national cybersecurity reviews, the CMM was revised to reflect the operational environment. This revision process was crucial to ensuring that the CMM maintains a functional purpose, rather than a theoretical perspective. The Organisation of American States (OAS) provided invaluable insight into several operational environments in which the CMM might be deployed. Finally, the CMM was adapted into a deployment tool, which optimised accessibility to the various stakeholders participating in the cybersecurity review. The adaptation process sought to capture the academic rigour and content behind the development of the CMM, but condense, re-structure, and rephrase the material in such a way as to maximise the impact of the capacity-building exercise.

b. Pilot Phase and Deployment

During the pilot phase of CMM in the first quarter of 2015, the Global Cyber Security Capacity Centre worked alongside the Organisation of American States (OAS) and Inter-American Development Bank (IDB)[1] and the World Bank[2] to conduct national cybersecurity capacity maturity reviews. Further country reviews were conducted over the following year in conjunction with the Commonwealth Telecommunications Organisation (CTO),[3] the government of The Netherlands under the auspices of the Global Forum on Cyber Expertise (GFCE)[4] and individual countries.[5] Throughout the process of deployment, the Capacity Centre has not only gained a unique understanding of the cybersecurity capacities of several countries, but has also learned lessons about cybersecurity capacity-building that can benefit the cybersecurity discipline as an evolving field of work.

As the Capacity Centre does not and cannot have thorough and in-depth understanding of each domestic context in which the model is deployed, it is important to work alongside international organisations or host ministries or organisations within the respective country. Moreover, cooperation with international organisations has sought to enable those organisations to achieve its own cybersecurity capacity-building objectives through a holistic understanding of a country's existing cybersecurity capacity. After engaging with the model deployment a number of times, these organisations will continue to conduct reviews in their own right, with remote Capacity Centre support. In this way, we can increase economies of scale while empowering international organisations to use a single model that is applicable to a variety of objectives and addresses cybersecurity capacity comprehensively.

[1] Colombia, Jamaica, and regional review
[2] Armenia, Bhutan, Kosovo and Montenegro.
[3] Uganda and Fiji.
[4] Senegal.
[5] Indonesia and United Kingdom.

III. Evolution of the Cybersecurity Capacity Maturity Model

This document presents the second iteration of the Capacity Centre's Cybersecurity Capacity Maturity Model. All revisions that have been made are based on lessons learnt in the pilot phase and subsequent post-pilot deployment of the CMM and through expert consultations. However, to validate the results of this revision process and ensure widest stakeholder consultations, this revised edition of the CMM has been disseminated to international cybersecurity experts for review and advice before finalisation.

a. Revision Process

In order to gather feedback and suggestions for the CMM evolution, a series of conference calls with members of the Capacity Centre's Expert Panel was arranged in late 2015. Each conference call focused on one of the five dimensions of the CMM and discussed various enhancements to the existing factors. These calls also introduced potential new factors, as gathered from the lessons learnt of the deployment of the model, a roundtable Expert Panel discussion, and additional preliminary consultations with the respective dimension Chairs. The outcome of the discussion during each of the calls was analysed and fed into the revision of the five CMM dimensions. The revised content was in turn curated by senior academics leading the development of the respective dimensions. Key modifications are described below.

b. Modifications and New Factors of CMM Revised Edition

Dimension One: Cybersecurity Policy and Strategy

An additional aspect was added to the Incident Response factor ('Mode of Operation') to better reflect the operational part of incident response capacity, including processes, tools and training. This was originally a factor in Dimension 5, but the review participants felt this factor was out-of-place without the context of the other aspects of incident response included in Dimension 1.

Furthermore, several aspects within various factors were merged to create a more focused view on each factor. For example, crisis management was condensed from two aspects to one because during the reviews, it became evident that participant responses for the 'Evaluation' aspect of crisis management was dependent on their response to the 'Planning' aspect. By combining these two aspects, the dependent relationship between aspects is removed.

Finally, to avoid further redundancies in this dimension, the word "national" was removed from various factors, aspects and indicators (apart from 'National Cybersecurity Strategy', which was identified as a noun), as the CMM is in itself a national model.

Dimension Two: Cyber Culture and Society

One of the major changes within the second dimension was the clarification of the relationship between cybersecurity awareness raising and cybersecurity mind-set. To ensure coherence within and across dimensions, the factor on initiatives seeking to raise awareness was moved to Dimension Three (Cybersecurity Education, Training and Skills), while the prevailing cybersecurity mind-set and social perception was retained in Dimension Two.

Three new factors were introduced within this dimension, namely: User Understanding of Personal Information Protection Online, Reporting Mechanisms, and Media and Social Media. All of these new factors had been identified as missing or not distinct enough during the deployment of the CMM.

The factor on User Understanding of Personal Information Protection Online refers to the understanding and sensitisation of users to protecting their personal data. This factor was identified as important in the first iteration of the CMM, but was not included due to difficultly of evidence collection. We decided that, since perceptual evidence should be included in the reviews, we are able to include this factor.

The factor on Reporting Mechanisms was identified as an important aspect to be included in the revised edition of the CMM by the various experts we consulted during the revision phase. This factor explores the existence of reporting mechanisms functioning as channels for users to report cybercrime and the possible development of coordinated programmes to promote the use of these mechanisms. The evidence gathered will offer valuable insight in a country's preparedness to control cybersecurity risks and the public ability to recognise and report these.

The role of media was identified as important during the CMM reviews and is now a distinct factor in the revised edition. The factor on Media and Social Media explores whether cybersecurity is a common subject across mainstream media, or an issue for broad discussion on social media, as well as the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Dimension Three: Cybersecurity Education, Training and Skills

Awareness raising was moved to this dimension from the cultural and social dimension, as raising awareness of cybersecurity is crucial to building knowledge. Additionally, the participants in the reviews often claimed that executive awareness of cybersecurity depended on the sector. By re-contextualising this factor into raising executive awareness, this aspect can be more readily applied at the national level.

Additionally, while the content of the third dimension did not change substantially, the deployment of the CMM suggested a broad restructuring of the factors and their aspects, as the previous structure proved to be confusing to country review participants and showed overlaps. For example, there was a conflation of education and training in the first iteration of the model that many participants found confusing. In the new structure, education and training are clearly separated and are defined by the provisional aspect, as well as development/uptake aspect, rather than addressing both education and training in the same factors. Emphasis was further shifted from focusing primarily on businesses and the private sector towards addressing all sectors of society.

Dimension Four: Legal and Regulatory Frameworks

Among the different components of the factor legal and regulatory frameworks, only ICT security legislation was considered unclear during the reviews, as the interpretation varied between ICT security legislation as the legal tool for mandatory standards adoption, or as a unique cybercrime law. As a result, this aspect of the first factor was clarified and the content was made more explicit by referring to the protection of critical information infrastructure, e-transactions, liability of Internet Service Providers and cyber incident reporting obligations.

Additionally, while a distinction was made in the CMM between training prosecutors and judges, review participants commented that it is not only crucial to maintain this distinction in further versions of the model, but also that the need for specialised trainings should be highlighted. This finding was corroborated by experts consulted on this dimension. In fact, one expert even suggested that, if the same training programmes are used for all parts of the criminal justice system, it would signify a lower level of cybersecurity capacity maturity.

The third factor on responsible disclosure was less self-explanatory to participants, as it did not directly relate to the other elements of this dimension and there was disagreement whether responsible disclosure requires a legal response or is rather an issue for policy or standards and good practice. Experts consulted on the various dimensions concluded that the responsible disclosure factor should be moved to the Standards, Organisations, and Technologies Dimension, as its content relates to technical vulnerabilities and the standards that are in place to disclose and address these.

Through expert consultations, several recommendations were gathered to further enhance the structure of Dimension Four. It was discussed that additional aspects on legislation addressing intellectual property, data protection, child protection online and consumer protection should be added to provide a more holistic overview of the legal framework relating to cybersecurity and emphasise these specific subjects that are widely debated at the international arena.

Another recommendation raised during expert consultations was the need to distinguish domestic and international cooperation as its own factor rather than an aspect of the criminal justice system factor. In accordance with expert input, the newly established third factor within this dimension includes both formal legal cooperation mechanisms (such as mutual legal assistance and extradition) and informal mechanisms (such as cooperation between law enforcement and Internet Service Providers), on domestic and international levels.

Dimension Five: Standards, Organisations, and Technologies

The various reviews conducted by the Capacity Centre indicated that the focus of Dimension Five was not as clear or succinct as the other four. Therefore, four new factors were based on recommendations from cybersecurity experts, in order to tailor the focus of this dimension on a clear set of issues.

Two new factors that were added observe the level of deployment and implementation of technical security and cryptographic control measures. These factors will gather evidence on the deployment of up-to-date technical security controls such as anti-malware systems, intrusion detection systems, network firewalls, event-logging and auditing functionality, as well as the deployment of cryptographic controls in all sectors, and whether these controls meet international standards and guidelines.

In addition, software quality was added as a new factor. Experts in cybersecurity have identified that the aspect of quality during deployment of software and the functional requirements as well as the existence and improvement of policies and processes on software updates were missing from the CMM.

The only other substantial change was the combination of the two aspects of National Infrastructure Resilience into one on Internet Infrastructure Resilience which, based on input from the reviews, more accurately reflects the content in the indicators.

IV. National Cybersecurity Capacity Maturity Model

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, crisis management, redundancy, and critical infrastructure protection capacities. Delivering cybersecurity must include capability in early warning, deterrence, resistance and recovery. This dimension considers effective security policy in delivering national defence and resilience capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

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.

- **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 drives capacity building at a national level.
- **Organisation:** This aspect addresses the existence of an overarching programme for cybersecurity coordination, including a departmental owner or coordinating body with a consolidated budget.
- **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 public awareness raising, mitigation of cybercrime, incident response capability and critical national infrastructure protection.

D 1.2: Incident Response

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, coordinate, and operationalise incident response.*

- **Identification of Incidents**: This aspect identifies whether there is a central registry of national level cyber 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.
- **Coordination**: This aspect explores the existence of coordinated national incident response with clear roles and responsibilities as well as lines of communication for crisis situations.
- **Mode of Operation:** This aspect addresses the operational and technical capacity of the incident response organisation, such as services, processes, resources and tools.

D 1.3: Critical Infrastructure (CI) Protection

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

- **Identification**: This aspect addresses the existence of a general list of CI assets, identified risk-based priorities, and an audit of CI assets on a regular basis.
- **Organisation**: This aspect addresses the existence of a formal collaboration mechanism between government ministries and owners of critical assets.
- **Risk Management and Response:** This aspect explores whether cybersecurity is embedded into general risk management practices, and whether security measures are developed to ensure business continuity of CI in the context of the prevailing risk environment. Additionally, this aspect refers to information protection procedures and processes for response planning to an attack on critical assets, supported by adequate technical security solutions.

D 1.4: Crisis Management

This factor addresses crisis management planning addresses conducting specialised needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.

- **Crisis Management:** (as above)

D 1.5: Cyber Defence Consideration

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

- **Strategy**: This aspect addresses the existence of a national cyber Defence strategy.
- **Organisation**: This aspect addresses the existence of a designated organisation within the government responsible for Defence for conflict using cyber means.
- **Coordination**: This aspect addresses coordination in response to malicious attacks on strategic information systems and critical national infrastructure.

D 1.6: Communications Redundancy

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

- **Communications Redundancy:** (as above)

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.	An outline/draft national cybersecurity strategy has been articulated. Processes for strategy development have been initiated. Consultation processes have been agreed for key stakeholder groups, including international partners.	A national cybersecurity strategy has been published. Multi-stakeholder consultation processes have been followed and observations fed back to the identified strategy 'owners'. National cybersecurity strategy is promoted and implemented by multiple stakeholders across government and other sectors.	Strategy review and renewal processes are confirmed. Regular scenario and real-time cyber exercises that provide a concurrent picture of national cyber resilience are considered a strategic priority. Relevant metrics, measurement, and monitoring processes, data, and historic trends are evaluated and inform decision-making. Cybersecurity strategic plans, aligned with national strategic priorities, drive capacity building and investments in security.	Continual revision and refinement of cybersecurity strategy is conducted proactively to adapt to changing socio-political, threat and technology environments. The country is a leader within the international community and the debate shaping the development of global cybersecurity strategy.
Organisation	No overarching national cybersecurity programme has been developed.	A coordinated cybersecurity programme is being developed through a multi-stakeholder consultative process. However, budgets reside in disparate public departments without a discrete cybersecurity budget line.	The single agreed cybersecurity programme has a designated coordinating body with a mandate to consult across public and private sectors, and civil society. The programme is defined according to goals and objectives, using metrics to measure progress. Discrete budget for cybersecurity exists, but is	Evidence exists of iterative application of metrics and resulting refinements to operations and strategy across government, including resource allocation considerations. A consolidated cybersecurity budget has been administered in order to allocate resources.	A singular national cybersecurity posture exists with the ability to reassign tasks and budgets dynamically according to changing risk assessments. A designated national body disseminates and receives feedback on the strategy from wider society to continuously enhance the national cybersecurity posture.

D 1.1: National Cybersecurity Strategy					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			not yet a part of a consolidated budget.		
Content	Various national policies may exist with a reference to cybersecurity, but if so, the content is generic, not necessarily aligned with national goals, and does not provide actionable directives.	Content includes links established between cybersecurity, national risk priorities and business development, but these are generally ad-hoc and lack detail.	The content of the national cybersecurity strategy is linked explicitly and directly to national risks, priorities and objectives, as well as business development. Content at a minimum should seek to raise public awareness, mitigate cybercrime, establish incident response capability and protect critical infrastructure from external and internal threats.	Metrics and measurements are utilised to update national cybersecurity strategy content to help leaders evaluate the success of the various cybersecurity objectives and guide resource investment. Content now also seeks to protect critical infrastructure internal threats.	New content is periodically incorporated in the strategy in response to evolving threat landscapes. Content of the national cybersecurity strategy leads, promotes and encourages national and international cooperation to ensure a secure, resilient and trusted cyberspace.

D 1.2: Incident Response					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Identification of Incidents	No catalogue of national level incidents exists, or is in development.	Certain cybersecurity incidents have been categorised and recorded as national-level threats.	A central registry of national-level cybersecurity incidents is operational.	Regular, systematic updates to the national-level incident registry are made. Resources are allocated for analysing incidents in order to prioritise which incidents are most urgent.	Focus on incident identification and analysis is adapted in response to environmental changes.

D 1.2: Incident Response					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Organisation	No organisation for national cyber incident response exists.	Private sector organisations key to national cybersecurity have been identified, but no formal coordination and information sharing mechanisms exist between public and private sectors. Dispersed public and private sector bodies detect and respond to incidents as they occur but a specific mandate for a national cyber incident response organisation is yet to be agreed.	A funded national body for incident response has been established (such as CSIRTs or CERTs), with specified roles and responsibilities.	Distinct and formal security roles and responsibilities are allocated across government, critical infrastructure, enterprise, and individual systems. Human and financial resources allocated to incident response are adequate to the cybersecurity threat environment and enhance effectiveness of the organisation.	National incident response capability is fully financially sustainable, from a single or multiple sources. An early warning capacity is incorporated into the mission of the incident response organisation, which seeks to shape and manage the threat landscape before responding to specific incidents.
Coordination	Coordination of incident response is informally managed within or between public and private sectors.	Leads for incident response have been designated at the operational level, but national-level coordination has not yet been established.	Routine and coordinated national incident response is established and published between public and private sectors, with lines of communication prepared for times of crisis. International cooperation for incident response between organisations exists to resolve incidents as they occur.	The national incident response organisation coordinates and collaborates with sub-national/sectorial incident-response organisations. Technical capabilities now go beyond coordinating response and include strategically focusing resources in coordinating international incident and threat intelligence analysis/support. A platform for the reporting and sharing of incidents across sectors is promoted.	Multi-level and inclusive national and international coordination between all levels and sectors is internalised as vital for continuous and effective incident response. Regional coordination exists to resolve incidents as they occur.

D 1.2: Incident Response					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Mode of Operation	Key incident response processes (detection, resolution, prevention, etc.) and (digital) tools to support them have not been well defined or documented. There is limited or no sufficient training or understanding of the key concepts of cybersecurity incident response.	Key incident response processes have been identified, but not officially documented or operationalised. Members of CSIRTs receive training in an ad-hoc manner. Incident response is reactive and ad-hoc.	Key incident response processes and tools are defined, documented and functional. Members of CSIRTs receive training regularly in order to understand key concepts of cybersecurity incident response. National-level incident response is limited in scope and still reactive.	Incident response teams have established a training policy for their members; members are being trained in specialised subjects and accredited by internationally recognised bodies on a regular basis. Team members are able to carry out a sophisticated incident analysis investigation quickly and efficiently. Key processes (detection, resolution, prevention, etc.) are being monitored and reviewed in regular basis, and tested with different case scenarios. Forensics services are offered. National incident response teams coordinate with international counterparts.	The results of testing key processes through case scenarios are being analysed and are incorporated into the updating of processes. The benefits of training and accreditation are being evaluated and inform the future training planning. Tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities are embedded in incident response organisation(s). Mechanisms for regional cooperation in incident response have been established.

D 1.3: Critical Infrastructure (CI) Protection					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Identification	Some understanding of what comprises CI assets is acknowledged, but no formal categorisation of assets has been produced.	A list of general CI assets has been created.	A detailed audit of CI assets as it relates to cybersecurity is performed on a regular basis. CI asset audit lists are disseminated to relevant stakeholders.	CI risks and assets have been prioritised according to vulnerability and impact, which guides strategic investment. Vulnerability/asset management processes are in place so that incremental security improvements can be made.	Priority listing of CI assets is regularly re-appraised to capture changes in the threat environment.
Organisation	There is little or no interaction between government ministries and owners of CI assets. No mechanism for collaboration exists.	There is informal and ad-hoc threat and vulnerability disclosure among CI owners as well as between CI and the government, but the scope of reporting requirements has not been specified.	A mechanism is established for regular vulnerability disclosure with defined scope for reporting incidents (either mandatory or voluntary) between CI asset owners and the government. Formal internal and external CI communication strategies have been defined and are consistent across sectors, with clear points of contact. Strategic engagement between government and CI is agreed and promoted.	There is a clear understanding of which threats to CI are managed centrally, and which are managed locally. A public awareness campaign to facilitate the CI communication strategy is established with a point of contact for this information. Cybersecurity requirements and vulnerabilities in CI supply chains are clearly identified, mapped and managed.	Owners of critical infrastructure and assets are able to rapidly respond to the changing threat landscape. Trust has been established between the government and CIs with respect to cybersecurity and exchange of threat information, which is fed into the strategic decision-making process.

Risk Management and Response	Risk management skills and understanding may be incorporated into business practices, but cybersecurity, if recognised, is subsumed into IT and data protection risk and is not recognised as a priority. Response planning and threat awareness may have been broadly discussed, but no formal plan exists.	Physical and virtual access control is implemented. CI has basic capacity to detect, identify, respond to and recover from cyber threats, but such capabilities are uncoordinated and vary in quality. Protection of CI assets includes basic level cybersecurity awareness and data security policies, but no protection processes have been agreed.	Best practices in security measures, guidelines, and standards for CI cybersecurity have been established and adopted. Cybersecurity risk management processes have been established, supported by adequate technical security solutions, communication links, and harm mitigation measures. CI risk management procedures are used to create a national response plan including the participation of all vital entities.	Cybersecurity is firmly embedded into general risk management practice. Assessment of the breadth and severity of harm incurred by CI assets is regularly conducted and response planning is tailored to that assessment to ensure business continuity. Resources are allocated in proportion to the assessed impact of an incident to ensure rapid and effective incident response. Insider threat detection is accounted for.	Audit practices to assess network and system dependencies and vulnerabilities (i.e. unmitigated dependencies) are implemented on a regular basis and inform continuous reassessment of CI risk portfolio, technologies, policies and processes. The impact of cybersecurity risk on the business operations of CI, including direct and opportunity costs, impact on revenue, and hindrance to innovation, are understood and incorporated into future planning and executive decision making.

D 1.4: Crisis Management					
Categories	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Crisis Management	It is understood that general crisis management is necessary for national security, but cybersecurity is not yet considered as a component. Crisis management exercise design and planning authority may have been allocated in principle (either directly or via consultants), but cybersecurity crisis management planning has not been thoroughly outlined.	A preliminary cybersecurity needs assessment of measures and techniques that require testing has been undertaken, but no exercise has been conducted at this point. An exercise planning authority has been designated, and has outlined the steps to be taken in order to conduct the cybersecurity exercise. Key stakeholders and other subject matter experts, such as think tanks, academics, civil leaders and consultants are included in the planning process. Exercise monitors, if designated, are internal and may lack training.	A cybersecurity exercise, with limited size and geographic scope has been conducted involving all relevant stakeholders in all sectors. Appropriate resources have been allocated to the exercises. Planning process includes the engagement of participants, an outline of their role in the exercise, and the articulation of benefits and incentives for participation. Trained internal or external monitors facilitate the exercise. The exercise is evaluated and commentary is provided by participants and stakeholders.	A realistic high-level scenario informs a plan to test information flows, decision-making and resource investment at the national level. Trust is developed well in advance via the recruitment and pre-exercise briefing process and through guaranteed confidentiality control. Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART) objectives and performance key indicators (PKI) inform decisions in crisis management, and evaluation results inform future investment in national cybersecurity capacity. Findings are evaluated against international crisis management good practice. Tailored, sector-specific reports are prepared for each stakeholder, while ensuring sensitive information is secured.	The exercise involves neutral peer stakeholders to observe, and, where appropriate, contribute, and addresses international challenges to produce scalable results for international policy- and decision-making. An evaluation of the crisis management exercise is provided for the international community, so that lessons learnt can contribute toward a global understanding of crisis management. Crisis management is embedded in risk analysis, review and management.

D 1.5: Cyber Defence					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Strategy	National security policy and Defence strategy may be published and may contain a cybersecurity component.	Specific threats to national security in cyberspace have been identified, such as external threat actors (both state and non-state), insider threats, supply chain vulnerabilities, and threats to military operational capacity, but a coherent strategy does not yet exist.	National cyber Defence policy or strategy exists and outlines the country's position in its response to different types and levels of cyber-attacks (for example, cyber-enabled conflict producing a kinetic effect and offensive cyber-attacks aimed to disrupt infrastructure).	Resources dedicated toward Cyber Defence are allocated based on national strategic objectives. The evolving threat landscape in cybersecurity is captured through repeated review in order to ensure that cyber Defence ways and means continue to meet national security objectives.	The policy or strategy drives the international discussion on rules of engagement in cyberspace. Rules of engagement are clearly defined and the military doctrine that applies to cyberspace is fully developed and takes note of significant shifts in the cybersecurity environment.
Organisation	Informal management of cyber Defence may be distributed among the armed forces and/or government organisations, with occasional reference to signals intelligence.	Cyber operations units are incorporated into the different branches of the armed forces, but no central command and control structure exists.	There is a defined organisation within the Defence apparatus responsible for conflict using cyber means.	Highly specialised expertise with advanced capabilities and full situational awareness are integrated into the national defence posture.	The Defence apparatus contributes to the debate in developing a common international understanding of the point at which a cyber-attack might trigger a cross-domain response.
Coordination	No, or limited, capacity for coordinated cyber Defence exists between domestic stakeholders (e.g. law enforcement, public, and enterprise, private) or interstate stakeholders (e.g. allied or neutral states).	Cyber Defence capability requirements are agreed between the public and private sector in order to minimise the threat to national and international security.	The entity in charge of cyber Defence coordinates integration regarding cyber events between government, military and critical infrastructure and identifies clear roles and responsibilities. Defence organisations and critical infrastructure providers have established a mechanism to report threat intelligence.	Analytical capacity exists to support the coordination of resource allocation for national cyber Defence; possibly including a cyber-defence research centre. The understanding of strengths and weaknesses within the coordination mechanism then feeds into the re-evaluation of the national security posture of the nation.	The country is leading the international debate on cyber Defence and systematically shares intelligence with allies.

D 1.6: Communications Redundancy					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Communications Redundancy	Digital redundancy measures may be considered, but not in a systematic, comprehensive fashion. Current emergency response assets may have been identified, but lack any level of integration.	Stakeholders convene to identify gaps and overlaps in emergency response asset communications and authority links. Emergency response assets, priorities and standard operating procedures are mapped and identified in the event of a communications disruption along any node in the emergency response network.	Emergency response assets are hardwired into a national emergency communication network. Communication is distributed across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Appropriate resources are allocated to hardware integration, technology stress testing, personnel training and crisis simulations drills.	Outreach and education of redundant communications protocols is undertaken for key stakeholders and is tailored to their unique roles and responsibilities. Emergency response assets practice interoperability and function effectively under compromised communications scenarios. The results of these scenarios then inform strategic investment in future emergency response assets. Stakeholders contribute to international efforts on redundancy communication planning.	Optimised efficiency is in place to mediate extended outages of systems. National-level assets can act to assist neighbours in the event of an international-level crisis or incident.

Dimension 2: Cyber 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 factor explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this factor reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

D 2.1: Cybersecurity Mind-set

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 mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

- **Government:** This aspect examines whether all agencies across all levels of government have embedded a proactive cybersecurity mind-set.
- **Private sector**: This aspect examines whether all agencies have embedded a proactive cybersecurity mind-set across business and industry.
- **Users**: This aspect examines whether a cybersecurity mind-set is adopted throughout society.

D 2.2: Trust and Confidence on the Internet

This factor reviews the level of user's trust and confidence in the use of online services, in general, and e-government and e-commerce services, in particular.

- **User Trust and Confidence on the Internet**: This aspect examines whether users trust in online services, and whether there is a coordinated programme by operators of Internet infrastructure to promote trust.
- **User Trust in E-government Services**: This aspect examines whether there are government e-services offered, if 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.
- **User Trust in E-commerce Services**: This aspect examines whether e-commerce services are offered and established in a secure environment, trusted by users.

D 2.3: User Understanding of Personal Information Protection Online

This aspect looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

- **User Understanding of Personal Information Protection Online**: (as above)

D 2.4: Reporting Mechanisms

This aspect explores the existence of reporting mechanisms functioning 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.

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

D 2.5: Media and Social Media

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

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

D 2.1: Cybersecurity Mind-set					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Government	Government has no or minimal recognition of the need to prioritise a cybersecurity mind-set. Leading agencies within government may have begun to consider cybersecurity.	Leading agencies have begun to place priority on cybersecurity, by identifying risks and threats.	Most government officials at all levels are aware of cybersecurity good practices.	Agencies across all levels of government have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit. Cybersecurity mind-set informs strategic planning.	The cybersecurity mind-set serves as a foundation for government official's operational practices and is evidenced as global good practice. Cybersecurity mind-set of government officials is related to a reduction of the overall threat landscape of the government.
Private Sector	The private sector has no or minimal recognition of the need to prioritise a cybersecurity mind-set.	Leading firms have begun to place priority on a cybersecurity mind-set by identifying high-risk practices. Programmes and materials have been made available to train and improve cybersecurity practices.	Most private sector actors at all levels are aware of cybersecurity good practices.	Most private sector actors, including SMEs, have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit. Cybersecurity mind-set, informs strategic planning.	The cybersecurity mind-set serves as a foundation for private sector operational practices, informs all IT related initiatives and is evidenced as global good practice. Cybersecurity mind-set of the private sector is related to a reduction of the overall threat landscape of the sector.
Users	Users have no or minimal recognition of the need to prioritise a cybersecurity mind-set and take no proactive steps to improve their cybersecurity.	A limited proportion of Internet users have begun to place priority on cybersecurity, by identifying risks and threats.	A growing number of users feel it is a priority for them to employ good cybersecurity practices and make conscious efforts to securely use online systems.	Most users have routinized a cybersecurity mind-set, employing secure practices as a matter of habit.	Cybersecurity mind-set of users is related to a reduction of the overall threat landscape of the country.

D 2.2: Trust and Confidence on the Internet					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
User Trust and Confidence on the Internet	Most Internet users have blind trust on websites and regarding what they see or receive online. Operators of Internet infrastructure may consider measures promoting trust in online services.	A very limited proportion of Internet users critically assess what they see or receive online and believe that they have the ability to use the Internet and protect themselves online. A limited proportion of users trust in the secure use of the Internet based on indicators of website legitimacy. Operators of Internet infrastructure develop measures to promote trust in online services but have not established them.	A growing proportion of Internet users critically assess what they see or receive online, based on identifying possible risks. A growing proportion of users trust in the secure use of the Internet based on indicators of website legitimacy. Internet infrastructure operators have established programmes to promote trust in online services. User-consent policies are in place designed to notify practices on the collection, use or disclosure of sensitive personal information.	Most Internet users critically assess what they see or receive online, based on identifying possible risks. Most Internet users feel confident while using the Internet, have the ability to recognise non-legitimate websites (including mimicry attempts), and have a sense of control over providing personal data online. Programmes to promote trust in the use of online services are assessed based on measures of effectiveness which informs resource allocation.	Individuals assess the risk in using online services, including changes in the technical and cybersecurity environment and continuously adjust their behaviour based on this assessment. Internet infrastructure operators assess trust promotion services and integrate findings into programme and policy revision.
User Trust in E-government Services	Government offers no or limited e-services, but has not publicly promoted the necessary secure environment. If e-government services are provided, users are unfamiliar with or lack trust in them.	Government continues to increase e-service provision, but also recognises the need for the application of security measures to establish trust in these services. The need for security in e-government services is recognised by stakeholders and users. A limited proportion of users trust in the secure use of e-government services.	E-government services have been fully developed. High-level risks affecting e-government services are prioritised in order to reduce occurrences. The public sector promotes use of e-government services and trust in these services through a coordinated programme, including the compliance to web standards that protect the anonymity of users.	Public authorities are routinely publishing certain information about their activities. Privacy-by-default is promoted as a tool for transparency in e-government services. The majority of users trust in the secure use of e-government services and make use of them.	E-government services and promotion thereof are continuously improved and expanded to enhance transparent/open and secure systems and user trust. Impact assessments on data protection in e-government services are consistently taking place and feed back into strategic planning.

D 2.2: Trust and Confidence on the Internet					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		Some e-government services are informing users of the utility of deployed security solutions.	A growing proportion of users trust in the secure use of e-government services. Possible breaches in e-government services are being identified, acknowledged, and disclosed in an ad-hoc manner.	Processes are employed for gathering user feedback in order to ensure efficient management of online content.	
User Trust in E-commerce Services	E-commerce services are not offered or are offered in an unsecure environment. If e-commerce services are provided, users are unfamiliar with or lack trust in them.	E-commerce services are being provided to a limited extent. The private sector recognises the need for the application of security measures to establish trust in e-commerce services. A limited proportion of users trust in the secure use of e-commerce services. Some e-commerce services are informing users of the utility of deployed security solutions.	E-commerce services are fully established by multiple stakeholders in a secure environment. Security solutions are updated and reliable payment systems have been made available. A growing proportion of users trust in the secure use of e-commerce services. The private sector promotes use of e-commerce services and trust in these services. Terms and conditions of use of e-commerce services are easily accessible.	E-commerce service providers recognise the need for building trust in order to ensure business continuity, and resources are allocated accordingly. The majority of users trust in the secure use of e-commerce services and make use of them. Stakeholders invest in establishing enhanced service functionality of e-commerce services, protection of personal information and the provision of feedback mechanisms for users.	E-commerce services are continuously improved 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. User feedback mechanisms are integrated into e-commerce services in order to enhance trust between users and providers.

D 2.3: User Understanding of Personal Information Protection Online					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
User Understanding of 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. Discussions may have begun and involve multiple stakeholders, but no privacy standards are in place.	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, but this has not resulted in concrete actions or policies.	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 constant public debate regarding the protection of personal information and about the balance between security and privacy, which informs privacy policies within public and private sectors.	All stakeholders have the information, confidence and the ability to take measures 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 sensitised to their privacy rights. Mechanisms are in place in private and public sectors to ensure that privacy and security are not competing. Privacy by default as a tool for transparency is promoted.	Users have the knowledge and skills necessary to protect their personal information online, adapting their abilities to the changing risk environment. There is a wide recognition of the need to ensure security and protection of personal information. Policies are in place in private and public sectors to ensure that privacy and security are not competing in a changing environment and are informed by user feedback and public debate. Assessments of personal information protection in e-services are regularly conducted and feed back into policy revision.

D 2.4: Reporting Mechanisms					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Reporting Mechanisms	There are no reporting mechanisms available, but discussions might have begun.	The public and/or private sectors are providing some channels for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents, but these channels are not coordinated and are used in an ad-hoc manner. Promotion of the existing reporting channels has not yet begun or is ad-hoc.	Reporting mechanisms have been established and are regularly used. Programmes to promote the use of these mechanisms have been established by public and private sectors.	Coordinated reporting mechanisms are widely used. Programmes to promote the use of these mechanisms are prioritised by public and private sectors and are considered as an investment in loss prevention and risk control. Effectiveness metrics of reporting mechanisms are applied and findings inform the revision and promotion of the mechanisms.	All relevant stakeholders actively collaborate and share good practice to enhance existing reporting mechanisms and there is a clear distribution of roles and responsibilities, including regarding the response to reported incidents. Mechanisms have been developed to coordinate response to reported incidents between law enforcement and the national incident response capability.

D 2.5: Media and Social Media					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Media and Social Media	Media and social media rarely, if ever, cover information about cybersecurity or report on issues such as security breaches or cybercrime.	There is ad-hoc media coverage of cybersecurity, with limited information provided and reporting on specific issues that individuals face online, such as online child protection or cyber-bullying. There is limited discussion on social media about cybersecurity.	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.	Media coverage extends beyond threat reporting and can inform the public of proactive and actionable cybersecurity measures, as well economic and social impacts. There is frequent discussion on social media about cybersecurity and individuals regularly exchange experiences online using social media.	The broad discussion of personal experiences and personal attitudes of individuals across mainstream and social media inform policy making and facilitate societal change.

Dimension 3: Cybersecurity Education, Training and Skills

This dimension reviews the availability of cybersecurity awareness raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1: Awareness Raising

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them.

- **Awareness Raising Programmes:** This aspect examines the existence of a national coordinated programme for cybersecurity awareness raising, covering a wide range of demographics and issues, developed based on consultations with stakeholders from various sectors.
- **Executive Awareness Raising:** This aspect examines efforts raising executives' awareness of cybersecurity issues in the public, private, academic and civil society sectors, as well as how cybersecurity risks might be addressed.

D 3.2: Framework for Education

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

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

D 3.3: Framework for Professional Training

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

- **Provision:** This aspects examines the development, availability and provision of cybersecurity training programmes for enhancing skills and capabilities.
- **Uptake:** This aspect examines the existence of certified employees trained in cybersecurity issues, processes, planning and analytics through the uptake of cybersecurity training programmes and knowledge transfer within organisations.

D 3.1: Awareness Raising					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Awareness Raising Programmes	The need for awareness of cybersecurity threats and vulnerabilities across all sectors is not recognised, or is only at initial stages of discussion.	Awareness raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic, and/or civil society sources, but no coordination or scaling efforts have been conducted. Awareness raising programmes may be informed by international initiatives but are not linked to national strategy.	A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) is established, which addresses a wide range of demographics and issues, but no metrics for effectiveness have been applied. Consultation with stakeholders from various sectors informs the creation and utilisation of programmes and materials. A single online portal linking to appropriate cybersecurity information exists and is disseminated via that programme.	The national awareness raising programme is coordinated and integrated with sector-specific, tailored awareness raising programmes, such as those focusing on government, industry, academia, civil society, and/or children. Metrics for effectiveness are established and evidence of application and lessons learnt are fed into future programmes. The evolution of the programme is supported by the adaptation of existing materials and resources, involving clear methods for obtaining a measure of suitability and quality. Programmes contribute toward expanding and enhancing international awareness raising good practice and capacity-building efforts.	Awareness raising programmes are adapted in response to performance evidenced by monitoring which results in the redistribution of resources and future investments. Metrics contribute toward national cybersecurity strategy revision processes. Awareness programme planning gives explicit consideration to national demand from the stakeholder communication (in the widest sense), so that campaigns continue to impact the entire society. The national awareness raising programme has a measurable impact on reduction of the overall threat landscape.

D 3.1: Awareness Raising					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
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 organisation. Executives of particular sectors, such as finance and telecommunications, have been made aware of cybersecurity risk 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 are regarded regionally and internationally as a source of good practice in responsible and accountable corporate cybersecurity governance.

D 3.2: Framework for 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 professional 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 the university level. Degrees in cybersecurity-related fields are offered by universities. Universities and other bodies hold seminars/lectures on cybersecurity issues aimed at non-specialists. Research and development is a leading consideration in cybersecurity education.	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 offered in cybersecurity specifically, which encompasses 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 based on an understanding of current risks and skills requirements. Cybersecurity education is not limited to universities, but ranges from primary to post-graduate levels, including vocational education.	National courses, degrees, and research are at the forefront of cybersecurity education internationally. 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 re-development of all general curricula.

D 3.2: Framework for Education					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Administration	The need for enhancing 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 coordinated management of cybersecurity education and research enhances national knowledge development has not, or only just begun.	The need for enhancing cybersecurity education in schools and universities 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.	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. Competitions and initiatives for students are promoted by government and/or industry in order to increase the attractiveness of cybersecurity careers.	Metrics are developed to ensure that educational investments meet the needs of the cybersecurity environment across all sectors. Government budget and spending on cybersecurity education is managed based on the national demand. Leading national cybersecurity academic institutions share their 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. Routinized cooperation between all stakeholders in cybersecurity education can be evidenced. Content in cybersecurity education programmes is aligned with practical cybersecurity problems and business challenges, and provides a mechanism for enhancing curriculum based on the evolving landscape.

D 3.3: Framework for 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. 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. 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 initially offered.	A range of cybersecurity training courses is tailored toward meeting national strategic demand and aligns with international good practice. The training programme outlines the priorities in the national cybersecurity strategy. Training programmes are offered to cybersecurity professionals that focus on the skills necessary to communicate technically complex challenges to non-technical audiences, such as management and general employees. Metrics of effectiveness assess the modes and procedures of training.	The public and private sector collaborate to offer training, constantly adapting and seeking to build skillsets drawn from both sectors. Training offerings coordinate with education programmes 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 trained workforce within the country.
Uptake	Training uptake by IT personnel designated to respond to cybersecurity incidents is limited or non-existent.	Metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings exist, but are limited in scope. There is no knowledge transfer from employees trained in cybersecurity to untrained employees.	There is an established cadre of certified employees trained in cybersecurity issues, processes, planning and analytics. Knowledge transfer from employees trained in cybersecurity to untrained employees is ad hoc.	The uptake of cybersecurity training is used to inform future training programmes. Coordination of training across all sectors ensures the national demand for professionals is met.	Cybersecurity professionals not only fulfil national requirements, but domestic professionals are consulted internationally to share lessons learnt and good practice.

D 3.3: Framework for Professional Training					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			Job creation initiatives for cybersecurity within organisations are established and encourage employers to train staff to become cybersecurity professionals.		

Dimension 4: Legal and Regulatory Frameworks

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1: Legal Frameworks

This factor addresses various legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks, privacy, freedom of speech, and other human rights online, data protection, child protection, consumer protection, intellectually property, substantive and procedural cybercrime legislation.

- **Legislative Frameworks for ICT Security:** This aspect addresses the existence and implementation of comprehensive ICT security legislative and regulatory frameworks.
- **Privacy, Freedom of Speech & Other Human Rights Online:** This aspect examines to what extent domestic legislation ensures that human rights are protected online, including privacy, freedom of speech, freedom of information, and freedom of assembly and association.
- **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.
- **Intellectual Property Legislation:** This aspect is concerned with the existence and implementation of online intellectual property legislation.
- **Substantive Cybercrime Legislation:** This aspect explores if existing legislation criminalises a variety of cybercrimes in specific legislation or general criminal law.
- **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.

D 4.2: Criminal Justice System

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

- **Law Enforcement:** This aspect examines whether law enforcement have received training on investigating and managing cybercrime cases and cases involving electronic evidence, and have 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.

D 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

- **Formal Cooperation:** This aspect examines the existence and effectivity of formal cooperation mechanisms to combat cybercrime, both between state actors and across borders, including mutual legal assistance and extradition procedures.
- **Informal Cooperation:** This aspect examines the existence and effectivity of informal cooperation mechanisms to combat cybercrime, both domestically and across borders, as well as within the public sector and between public and private sectors.

D 4.1: Legal Frameworks					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Legislative Framework for ICT Security	Legislation relating to ICT security does not yet exist. Efforts to draw attention to the need to create a legal framework on cybersecurity have been made and may have resulted in a gap analysis.	Experienced stakeholders from all sectors may have been consulted to support the establishment of a legal and regulatory framework. Key priorities for creating cybersecurity legal frameworks have been identified through multi-stakeholder consultation, potentially resulting in draft legislation, but legislation has not yet been adopted.	Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been adopted. Laws address the protection of critical information infrastructure, e-transactions, liability of Internet Service Providers and, potentially, cyber incident reporting obligations.	The country reviews existing legal and regulatory mechanisms for ICT security, identifies where gaps and overlaps exist, and amends laws accordingly or enacts new laws. Monitoring of enforcement of legislative frameworks informs resource allocation and legal reform.	Mechanisms are in place for continuously harmonising ICT legal frameworks with national cybersecurity-related ICT policies, international law, standards and good practices. Participation in the development of regional or international cybersecurity cooperation agreements and treaties is a priority. Efforts are in place to exceed minimal baselines specified in these treaties where appropriate.
Privacy, Freedom of Speech & Other Human Rights Online	Domestic law does not recognise fundamental human rights in relation to cybercrime. Discussions of privacy issues online may have begun and include multiple stakeholders, but no privacy legislation or standards are in place.	Domestic legislation partially recognises privacy, freedom of information, freedom of assembly and association, and freedom of expression online. Stakeholders from all key sectors have been consulted for the development of legislation addressing human rights online.	Domestic law recognises fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. Domestic law specifies safeguards to protect the individual's right to privacy during the collection, use and disclosure of personal information in investigations involving electronic evidence. All relevant actors from private sector and civil	International and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and associated resource planning. Research is conducted and measures are in place to exceed minimal baselines specified in international agreements.	In order to meet dynamic changes in the application of technology to human rights, procedures are in place to amend and update legal frameworks as needed. Access to the Internet is recognised and enshrined as a human right. The state is an active contributor in the global discourse on human rights on the Internet. Domestic actors, policies and practices actively shape positive international

D 4.1: Legal Frameworks					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			society are involved in shaping laws and regulations on privacy, freedom of speech, and other human rights online. The country has ratified or acceded to international agreements.		discussions of privacy online.
Data Protection Legislation	Data protection legislation is not yet under development. Public discourse on data protection issues may have begun and includes multiple stakeholders.	Data protection legislation is under development. Stakeholders from all key sectors have been consulted to support the development of legislation.	Comprehensive data protection legislation has been adopted and enforced, which includes conditions for the collection of personal data and protection from misuse.	Legal mechanisms are in place that enable strategic decision making that determines the timeframe in which personal data is no longer required as evidence for investigation and must be deleted. International and regional trends and good practices inform the assessment and amendment of data protection laws and associated resource planning.	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
Child Protection Online	Legislation protecting children online is not yet under development. Public discourse on child protection online may have begun and includes multiple stakeholders.	Legislative provisions protecting children online are under development. Stakeholders from all key sectors have been consulted to support the development of legislation.	Comprehensive legislation on the protection of children online has been adopted and enforced, and ensures that data protection and privacy rules for legal minors apply to the online environment.	The country continuously seeks to improve national child protection online legislation to comply with regional and international law and standards.	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.

D 4.1: Legal Frameworks					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Consumer Protection Legislation	Legislation protecting consumers against online fraud and other forms of cybercrime is not yet under development.	Legislation protecting consumers online is under development. Stakeholders from all key sectors have been consulted to support the development of legislation.	Comprehensive legislation protecting consumers from business malpractice online has been adopted and is enforced. A lead agency responsible for the protection of consumers online has been designated.	The country continuously seeks to improve national consumer protection legislation to address national needs and comply with regional and international consumer protection standards.	In order to meet dynamic changes in the application of technology to consumer protection, procedures are in place to amend and update legal frameworks as needed.
Intellectual Property Legislation	Intellectual property of online products and services might be discussed among multiple stakeholders, but no specific legal provisions are in place. If general law on intellectual property exists, it is not applicable to online products and services yet.	Legislation on intellectual property online is under development, through consultation with key stakeholders.	Comprehensive legislation addressing intellectual property of online products and services has been adopted and is enforced.	Legislation on intellectual property online is regularly reviewed and amended accordingly to reflect changes in national priorities and the international ICT landscape. Legislative amendments are informed by multi-stakeholder consultations and public discourse.	Decisions to update legislation are based on the balance between intellectual property and open access policies, through multi-stakeholder discussion.
Substantive Cybercrime Legislation	Specific substantive criminal law on cybercrime does not exist or general criminal law exists, but its application to cybercrime is unclear Specific substantive criminal provisions on cybercrime might be discussed among lawmakers, but the development of the provisions has not yet commenced.	Partial legislation exists that addresses some aspects of cybercrime or cybercrime legal provisions are under development.	Substantive cybercrime legal provisions are contained in specific legislation or a general criminal law. The country has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law.	Measures are in place to exceed minimal baselines specified in international treaties where appropriate, which includes procedures to amend substantive legal frameworks as needed.	The country is an active contributor in the global discourse on developing and improving international cybercrime treaties. Laws, where needed, are amended to reflect changes in the international ICT environment.

D 4.1: Legal Frameworks					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Procedural Cybercrime Legislation	Specific procedural criminal law for cybercrime does not exist and general criminal procedural law is not applicable to cybercrime investigations, prosecutions, and electronic evidence. Procedural criminal legislation for cybercrime might be discussed among lawmakers, but development of the legislation has not yet begun.	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 enforced. The state has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law.	In the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully investigate cybercrime. Measures are in place to exceed minimal baselines specified in international treaties where appropriate, which includes procedures to amend procedural legal frameworks as needed.	The country is an active contributor in the global discourse on developing and improving international cybercrime treaties. Procedural law, where needed, is amended to adapt to the changing cybercrime landscape and emerging investigative challenges.

D 4.2: Criminal Justice System					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Law Enforcement	Law enforcement does not have sufficient capacity to prevent and combat cybercrime and does not receive specialised training on cybercrime investigations.	Traditional investigative measures are applied to cybercrime investigations, with limited digital forensics capacity. If law enforcement officers receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.	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 exist and are implemented.	Resources dedicated to fully operational cybercrime units have been allocated based on strategic decision making. Advanced investigative capabilities allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators. Law enforcement agencies have the resources to maintain the integrity of data to meet international evidential standards in cross-border investigation. Statistics and trends on cybercrime investigations are collected and analysed.	All law enforcement officers receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes. Law enforcement can utilise sophisticated digital forensic tools, and these technologies are consistently updated. The institutional capacity of law enforcement is frequently reviewed and revised based on an assessment of effectiveness.
Prosecution	Prosecutors do not receive adequate training and resources to review electronic evidence or prosecute cybercrime. There are no specialised cybercrime prosecutors, but consultation may have begun to consider this capacity within the criminal justice community.	A limited number of specialised cybercrime prosecutors have the capacity to build a case based on electronic evidence, but this capacity is largely ad-hoc and un-institutionalised. If prosecutors receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.	A comprehensive institutional capacity, including sufficient human, training and technological resources, to prosecute cybercrime cases and cases involving electronic evidence is established.	Institutional structures are in place, with a clear distribution of tasks and obligations within the prosecution services at all levels of the state. Statistics and trends on cybercrime prosecutions are constantly collected and analysed. A mechanism exists that enables the exchange of information and good	There is national capacity to prosecute complex domestic and cross-border cybercrime cases. A dedicated cybercrime prosecution unit might have been established. All prosecutors receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.

D 4.2: Criminal Justice System					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
				practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.	
Courts	A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence do not exist. 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 and not systematic. If judges receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.	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 on cybercrime and electronic evidence.	The court system has organised itself to ensure a central management of cybercrime cases, with clear distribution of tasks and obligations within the court system at all levels of the state. Statistics and trends on cybercrime convictions are collected and analysed.	Judges receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes. The institutional capacity of the court system is frequently reviewed and revised based on an assessment of effectiveness.

D 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Formal Cooperation	No or minimal forms of international cooperation exist to prevent and combat cybercrime. There is no formal mechanism that promotes the exchange of information between domestic public and private sectors on cybercrime and cooperation is limited.	Formal mechanisms of international cooperation have been established, but the application to cybercrime is ad-hoc or only possible in some cases. Exchange of information on cybercrime between domestic public and private sectors is ad-hoc and unregulated.	Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution. Mutual legal assistance and extradition agreements and mechanisms have been established and are applied to cybercrime cases. Legislative requirements for the exchange of information between domestic public and private sectors have been determined.	Formal international cooperation mechanisms are fully functional, with established communication channels. Strategic decisions are made to expand and enhance formal cooperation mechanisms on cybercrime as needed. Resources are allocated to support the exchange of information between public and private sectors domestically and enhance legislative requirements and communication mechanisms.	Formal international cooperation mechanisms are regularly reviewed to determine effectiveness, and are revised accordingly to reflect the changing cybercrime landscape. Formal and informal international cooperation mechanisms complement each other and are interoperable. Formal mechanisms that enable the exchange of information between domestic public and private sectors are adapted in accordance with identified needs and changing threat environment.
Informal Cooperation	There is minimal interaction between government and criminal justice actors. Cooperation between Internet Service Providers and law enforcement has not been established. Law enforcement cooperation with foreign counterparts is not effective.	Exchange of information between government and criminal justice actors is limited and ad-hoc. Ad-hoc cooperation between Internet Service Providers and law enforcement exists, but is not always effective. Law enforcement cooperates with foreign counterparts on an ad-hoc basis, but is not integrated	Informal relationships between government and criminal justice actors have been established, resulting in the regular exchange of information on cybercrime issues. Effective informal cooperation mechanisms between Internet Service Providers and law enforcement have been established, with clear communication channels.	A strategic relationship between government actors, prosecutors, judges and law enforcement agencies has been established relating to cybercrime. Law enforcement cooperates with domestic and foreign ISPs in combatting cybercrime. Law enforcement agencies work jointly with foreign counterparts, potentially	Government and criminal justice actors exchange information timely and efficiently, and cooperation is adapted to the changing cybercrime environment and associated requirements. A routinized relationship between law enforcement and ISPs, domestically and across borders, has been established and is adaptable to emerging forms of cybercrime.

D 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
		in regional and international networks.	Domestic law enforcement agencies are informally integrated with regional and international counterparts and networks, such as Interpol or 24/7 networks.	through joint task forces, resulting in successful cross-border cybercrime investigations and prosecutions.	Formal and informal international cooperation mechanisms complement each other and are interoperable.

Dimension 5: Standards, Organisations, 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.

D 5.1: Adherence to Standards

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

- **ICT Security Standards:** This aspect examines whether cybersecurity related standards and good practices are being adhered to and adopted widely across the public sector and Critical Infrastructure (CI) organisations.
- **Standards in Procurement:** This aspect addresses the implementation of standards in procurement practices.
- **Standards in Software Development:** This aspect addresses the implementation of standards in software development.

D 5.2: 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 aspect reviews the control that the government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.

- **Internet Infrastructure Resilience:** (as above)

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 criticality of services.

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

D 5.4: Technical Security Controls

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

- **Technical Security Controls:** (as above)

D 5.5: Cryptographic Controls

This factor 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.

- **Cryptographic Controls:** (as above)

D 5.6: Cybersecurity Marketplace

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

- **Cybersecurity Technologies:** This aspect examines whether a national market for cybersecurity technologies is in place and supported, and informed by national need.
- **Cyber Insurance:** This aspect explores the existence of a market for cyber insurance, its coverage and products suitable for various organisations.

D 5.7: Responsible Disclosure

This factor explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors and if there is sufficient capacity to continuously review and update this framework.

- **Responsible Disclosure:** (as above)

D 5.1: Adherence to Standards					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
ICT Security Standards	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, 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 adoption of international standards and good practices.	Nationally agreed baseline of cybersecurity related standards and good practices has been identified, and adopted widely across public and private sectors. Some body within government exists to assess level of adoption across public and private sectors. Government schemes exist to promote continued enhancements, and metrics are being applied to monitor compliance. Consideration is being given to how standards and good practices can be used to address risk within supply chains within the CI, by both government and CI.	Government and organisations promote adoption of standards and good practises according to assessment of national risks and budgetary choices. There is evidence of debate between government and other stakeholders as to how national and organisational resource decisions should align and drive standard adoption. Evidence of contribution to international standards' bodies exists and contributes to thought leadership and sharing of experience by organisations.	The choice of adopted standards and good practices and their implementation is continuously improved. Adoption 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 good practices, based on continuous needs assessments.
Standards in Procurement	No standards or good practices have been identified for use in guiding procurement processes by the public and private sector. If they are recognised, implementation is ad hoc and uncoordinated.	Cybersecurity standards and good practices guiding procurement processes have been identified for use. Evidence of promotion and adoption of cybersecurity standards and good practices in defining procurement practices exists within public sectors and private sectors.	Procurement practices meet international IT guidelines, standards and good practices. Adoption and compliance of standards in procurement practices within the public and private sectors, is evidenced through measurement and assessments of process effectiveness.	Cybersecurity standards and good practices in guiding procurement processes are being adhered to widely within public and private sectors. Critical aspects of procurement and supply, such as prices and costs, quality, timescales and other value adding activities are continuously improved, and procurement process	Organisations have the ability to monitor use of standards and good practices in procurement processes and support deviations and non-compliance decisions in real-time through risk-based decision making and quality assurance.

D 5.1: Adherence to Standards					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
				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. Internal stakeholders have been trained in the secure use of E-sourcing or E-tendering systems and purchase-to-pay systems (P2P) in order to implement these tools in performing key tasks in procurement and supply.	
Standards in Software Development	No standards or good practices for software development have been identified for use relating to integrity and resilience in public and private sectors. Or, there is some identification, but only limited evidence of take-up.	Core activities and methodologies for software development processes focused on integrity and resilience are being discussed within professional communities. Government promotes relevant standards in software development, but there is no widespread use of these standards yet. Some organisations supply or seek to adopt standards in code development.	Government has an established programme for promoting and monitoring standard adoption in software development – both for public and commercial systems. Evidence of public and private sector organisations adopting standards in their software development processes. Evidence that high integrity systems and software development techniques	Security considerations are incorporated in all stages of software development. Core development activities, including configuration and documentation management, security development and lifecycle planning have been adopted. Procurement of software developed according to required standards is considered based on an	Software development projects continuously assess the value of standards and reduce or enhance levels of compliance according to risk-based decisions. Procurement of software includes on-going assessments of the value of standards in delivering software quality – throughout the lifetime of the contract (as opposed to simply initially at procurement stage).

D 5.1: Adherence to Standards					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
			are present within the educational and training offerings in the country.	assessment of risk in investment decisions.	Requirements are built into contracts with suppliers.

D 5.2: Internet Infrastructure Resilience					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Internet Infrastructure Resilience	Affordable and reliable Internet services and infrastructure in the country may have not yet been established; if they have been, adoption rates of those services are a concern. There is little or no national control of network infrastructure; networks and systems are outsourced, with potential adoption from unreliable third-party markets.	Limited Internet services and infrastructure are available, but may not be reliable. Resilience of Internet infrastructure in public and private sectors has been discussed by multiple stakeholders, but has not been fully addressed. There may be regional support to secure Internet infrastructure in the country.	Reliable Internet services and infrastructure have been established. Internet is used for e-commerce and electronic business transactions; authentication processes are established. Technology and processes deployed for Internet infrastructure meet international IT guidelines, standards, and good practices. National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.	Regular assessment of processes according to international standards and guidelines are conducted together with assessment of national information infrastructure security and critical services that drive investment in new technologies.	Acquisition of infrastructure technologies is effectively controlled, with flexibility incorporated according to changing market dynamics. Costs for infrastructure technologies are continually assessed and optimised. There is effectively controlled acquisition of critical technologies with managed strategic planning and service continuity processes in place. Scientific, technical, industrial and human capabilities are being systematically maintained, enhanced and perpetuated in order to maintain the country's independent resilience.

D 5.3: Software Quality					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Software Quality	Quality and performance of software used in the country is a concern, but functional requirements are not yet fully monitored. A catalogue of secure software platforms and applications within the public and private sectors does not exist. Policies and processes regarding updates 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 secure software platforms and applications within the public and private sectors is under development. Policies and processes on software updates and maintenance are now under 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 are established. 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 are being improved based on risk assessments and the criticality of services. 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.

D 5.4: Technical Security Controls					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Technical Security Controls	There is minimal or no understanding or deployment of the technical security controls offered in the market, by users, public and private sectors. Internet Service Providers (ISPs) may not offer any upstream controls to their customers.	Technical security controls are deployed by users, public and private sectors, but inconsistently. The deployment of up-to-date technical security controls is promoted in an ad-hoc manner and all sectors are being incentivised to their use. ISPs may be offering anti-malware software as part of their services but possibly in an ad-hoc manner. ISPs recognise the need to establish policies for technical security control deployment as part of their services. Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed but not necessarily in a consistent manner.	Up-to-date technical security controls, including patching and backups, are deployed in all sectors. Users have an understanding of the importance of anti-malware software and network firewalls across devices. Physical security controls are employed to prevent unauthorized personnel from entering computing facilities. ISPs establish policies for technical security control deployment as part of their services. The technical cybersecurity control set is based on established cybersecurity frameworks, such as the SANS top 20 cybersecurity controls, the CESG 10 steps to cybersecurity, or PAS 55.	Penetration of technical security controls leads to effective upstream protection of users and public/private sectors. Within the public and private sectors, technical security controls are being kept up-to-date, monitored for effectiveness and reviewed on a regular basis. The public and private sector have the capacity to critically assess and upgrade cybersecurity controls according to their appropriateness and suitability for use.	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 technical security controls being deployed extends to its impact on organisational operations and budget allocation. ISPs supplement technical security controls with multi factor authentication, digital certificates and whitelisting to ensure prevention of access of non-trusted sites or web addresses and maintain a safe Internet environment.

D 5.5: Cryptographic 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, private sector or 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. State of the art tools, such as SSL or TLS, are deployed ad-hoc by web service providers to secure all communications between servers and web browsers.	Cryptographic techniques are available for all sectors and users for protection of data at rest or in transit. There is a broad understanding of secure communication services, such as encrypted/signed email. The cryptographic controls deployed meet international standards and guidelines accordingly for each sector and are kept up-to-date. State of the art tools, such as SSL or TLS, are deployed routinely by web service providers to secure all communications between servers and web browsers.	The public and private sectors critically assess the deployment of cryptographic controls, according to their objectives and priorities. 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 relevance of cryptographic controls deployed for securing data at rest and data in transit is continuously assessed through risk assessments. The public and private sector adapt encryption and cryptographic control policies based on the evolution of technological advancement and changing threat environment.

D 5.6: Cybersecurity Marketplace					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Cybersecurity Technologies	Few or no cybersecurity technologies are produced domestically; but international offerings may be available.	The domestic market may provide non-specialised cybersecurity products, but these are not market-driven. Cybersecurity is considered in software and infrastructure development.	Cybersecurity products are now being produced by domestic providers in accordance with market needs. National dependence on foreign cybersecurity technologies is increasingly mitigated through enhanced domestic capacity.	Cybersecurity technology development abides by secure coding guidelines, good practices and adhere to internationally accepted standards. Risk assessments and market incentives inform the prioritisation of product development to mitigate identified 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.
Cyber Insurance	The need for a cyber insurance market may have been identified, but no products and services are available.	The need for a market in cyber insurance has been identified through the assessment of financial risks for public and private sectors, and development of products is now being discussed.	A market for cyber insurance is established and encourages information sharing among participants of the market. First-party insurance typically covers damage to digital assets, business interruptions and, potentially, reputational harm. Third-party insurance covers liability and the costs of forensic investigations, customer notification, credit monitoring, public relations, legal defence, compensation and regulatory fines.	Cyber insurance specifies a variety of coverages to mitigate consequential losses. These coverages are selected based on strategic planning needs and identified risk. Products suitable for SMEs are also on offer.	The cyber insurance market is innovative and adapts to emerging risks, standards and practices, while addressing the full scope of cyber harm. Insurance premiums are offered for consistent cyber-secure behaviour.

D 5.7: Responsible Disclosure					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Responsible Disclosure	The need for a responsible disclosure policy in public and private sector organisations is not yet acknowledged.	Technical details of vulnerabilities are shared informally with other stakeholders who can distribute the information more broadly. Software and service providers are able to address bug and vulnerability reports.	A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and an acknowledgement report. Organisations have established processes to receive and disseminate vulnerability information. Software and service providers commit to refrain from legal action against a party disclosing information responsibly.	Responsible disclosure processes for all involved stakeholders (product vendors, customers, security vendors and public) are set. An analysis of the technical details of vulnerabilities is published and advisory information is disseminated according to individual roles and responsibilities. The large majority of products and services are updated within predetermined deadlines.	Responsible disclosure policies are continuously reviewed and updated based on the needs of all affected stakeholders. Responsible disclosure frameworks are shared internationally, so that best practice in this area can be created. All affected products and services are routinely updated within deadline. Processes are in place to review and reduce deadlines.

Acknowledgements

We would like to acknowledge the contributions of the academic chairs of each dimension, as well as the various working group members that brought their expertise into the development of the CMM.

Director

Professor Sadie Creese (University of Oxford)

Research Team

Dr Maria Bada

Eva Ignatuschtschenko

Lilly Pijnenburg Muller

Taylor Roberts

Technical Board

Professor Ivan Arreguín-Toft (Boston University)

Professor Ian Brown (University of Oxford)

Professor Paul Cornish (Global Cyber Security Capacity Centre, University of Oxford)

Professor William Dutton (Michigan State University)

Professor Michael Goldsmith (University of Oxford)

Lara Pace (University of Oxford)

Professor David Upton (University of Oxford)

Professor Basie Von Solms (University of Johannesburg)

Expert Panel

Professor Gary Blair; Dr Grant Blank; Professor Roger Bradbury; Dr David Bray; Mr Bruno Brunskill; Mr Georgios Chatzichristos; Mr Belisario Contreras; Mr Luc Dandurand; Professor Chris Demchak; Dr Tobias Feakin; Mr Andrew Fitzmaurice; Dr Marco Gercke; Professor Chris Hankin; Mr Robert Hayes; Mr Paul Hopkins; Mr Peter Kahiigi; Ms Gail Kent; Professor Douwe Korff; Ms Vashti Maharaj; Mr Steven Malby; Mr John Mallery; Dr Aaron Martin; Mr Alan Mears; Professor Chris Mitchell; Professor Joseph Nye; Professor Sir David Omand; Dr Wolter Pieters; Mr Steve Purser; Dr Tristram Riley-Smith; Ms Sandra Sargent; Professor Angela Sasse; Mr Mike Steinmetz; Mr Graeme Stewart; Ms Heli Tiimaa-Klaar; Professor Ian Walden; Mr Alex Ward; Mr Graham Wright

The Global Cyber Security Capacity Centre
Oxford Martin School, University of Oxford,
Old Indian Institute, 34 Broad Street, Oxford
OX1 3BD, United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk